

HIPAA Security Policy #1

Administrative Safeguards Security Management Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

The objective of <insert client name> (hereby known as "The Company") in the development and implementation of these HIPAA Security Policies and Procedures, is to create effective administrative, technical and physical safeguards for the protection of the Protected Health Information (PHI) of patients. These policies set forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PHI in all forms.

*The use of the term **employees** will include all of The Company's owners, managers, employees, all independent contractors and temporary employees.*

Purpose of Policy

The purpose of the policy is to develop a risk management process for the selection and implementation of security safeguards to reduce the risks to electronic Protected Health Information (ePHI) to reasonable and manageable levels.

Policy

1 Security Management Policy

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(1)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to prevent, detect, contain and correct security violations."

The Company will protect the confidentiality, integrity, and availability of ePHI by maintaining appropriate safeguards for the networks and systems that handle ePHI. The Company will implement policies and procedures to prevent, detect, contain, and correct security violations.

1.1 Risk Analysis

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(1)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity."

1. The Company acknowledges the potential vulnerabilities associated with storing ePHI, transmitting ePHI locally and transmitting ePHI outside of The Company.
2. To appropriately assess such potential vulnerabilities, The Company shall perform a Risk Assessment which:
 - i. Identify and document all ePHI repositories
 - ii. Identify and document potential threats and vulnerabilities to each repository
 - iii. Assess current security measures
 - iv. Determine the likeliness of threat occurrence
 - v. Determine the potential impact of threat occurrence
 - vi. Determine the level of risk
 - vii. Determine additional security measures needed to lower level of risk
 - viii. Document the findings of the Risk Assessment

Procedure

1. Document all ePHI repositories

- i. Identify and document where ePHI is stored, received, maintained or transmitted.
 1. ePHI may be identified through surveys, questionnaires, interviews, review of documentation, automated scans, or other data gathering methods.
- ii. The output of this process should be documentation of all repositories/systems that contain ePHI in an organization.

2. Identify and document potential threats and vulnerabilities to each repository

- i. Identify and document all reasonably anticipated threats to ePHI. Examples of Threats include:

1. Data entry error
 2. Theft of a laptop
 3. Power outage
- ii. Identify and document all vulnerabilities to each ePHI repository.
- iii. The output of this process should be documentation of all reasonably anticipated threats and vulnerabilities to each repository/system that contains ePHI within an organization.

3. Assess current security measures

- i. Review the current security measures (safeguards / controls) that are currently in place that are used to mitigate identified risks. Examples of current safeguards include:
 1. User awareness training
 2. Backup procedures
 3. Disaster Recovery procedures
 4. Employee termination procedures
- ii. The output of this process should be documentation of current security measures to protect any repositories/systems that contain within an organization.

4. Determine the likeliness of threat occurrence

- i. For each threat and vulnerability to ePHI that has been identified in step 2 of the Risk Assessment procedure, calculate the likelihood of the threat occurring.
- ii. The likeliness or probability of a threat occurring is usually measured in (low, medium or high) or expressed as a number of times a threat is likely to occur in a given year.
- iii. Existing security measures as identified in step 3 of the Risk Assessment procedure may lower the likeliness of a threat.
- iv. Existing vulnerabilities as identified in step 2 of the Risk Assessment procedure may raise the likeliness of a threat.
- v. Examples of a likeliness of a threat includes:

1. If there has been issues with power outages in the past then the threat of a power outage may be assessed as **High**. Additionally, if a backup generator has been previously installed (current security measure) then the likeliness of a threat of a power outage may be reduced to **Medium** or **Low**.
 2. If there have been no issues with flooding in the past 5 years then the threat from flooding may be assessed as **Low**.
- vi. The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI of an organization.

5. Determine the potential impact of threat occurrence

- i. For each threat and vulnerability to ePHI, calculate the associated impact of the threat.
- ii. Examples of threat impact include:
 - i. A fire in the computer room that contains all ePHI repositories / systems would have a **High** impact. The fire may affect the availability of ePHI repositories / systems.
- iii. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of ePHI within an organization.

6. Determine the level of risk

- i. For each threat and vulnerability to ePHI, calculate the level of risk of the associated threat.
- ii. The level of risk is calculated by using the likeliness of a threat, as calculated in step 4 of the Risk Assessment procedure and the resulting impact of a threat, as calculated in step 5 of the Risk Assessment procedure.
- iii. An example of calculating the level of risk for a threat include:
 1. If the threat of a flood has been calculated with a likeliness of **High** and the impact of a flood has been calculated as **High** then the associated level of risk would then be **High**.
 2. If the threat of a power outage has been calculated as **Low** and the impact of a power outage has been calculated as **Medium** then the associated risk level would be **Low**.

- iv. The output of this process should be documentation of the level of risk associated with each threat and impact to the confidentiality, availability and integrity of ePHI within an organization.

7. Determine additional security measures needed to lower the level of risk

- i. Based on the determination of the level of risk as defined in step 6 of the Risk Assessment procedure, additional security measures (safeguards / controls) may be needed to lower the risk.
- ii. Examples of additional security measures needed include:
 - 1. If the threat of a power outage has been calculated as **High** and the impact of a power outage has been calculated as **Medium** then the associate risk level would be **High**. An additional security measure that may be implemented would be the installation of a backup generator to lower the likeliness of a power outage impacting any systems containing ePHI.
- iii. The output of this process should be documentation of any additional security measures that are needed to lower the level of risk associated with each threat and impact to the confidentiality, availability and integrity of ePHI within an organization.

8. Document the findings of the Risk Assessment

- i. The final step in the Risk Assessment process is to document and publish all of the findings in each of the steps of the Risk Assessment procedure.

1.2 Risk Management

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(1)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a) [Risk analysis]."

- 1. The Company shall implement security measures and safeguards for each ePHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The level, complexity and cost of such security measures and safeguards must be commensurate with the risk classification of each such ePHI repository.
- 2. The Company will reassess the potential risks and vulnerabilities of an ePHI repository as part of a periodic review; it must update the security measures and safeguards for such

ePHI repository to reflect any changes in the risks and vulnerabilities assessment. At a minimum the risk management process will include the following:

- i. Assessment and prioritization, on the basis of risks, of each ePHI repository.
- ii. Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.
- iii. Security training and awareness on implemented security measures to workforce members.
- iv. Periodic evaluation and revision, as necessary, of the security measures.

Procedure

1. The Risk Management process will be based on the following steps
 - i. Risk Analysis – A Risk Analysis will be performed based on Risk Analysis policy (1.1).
 - ii. Risk Prioritization - Using information from the risk analysis, risks will be ranked on a scale (from high to low) based on the potential impact to information systems containing ePHI and the probability of occurrence.
 - iii. Cost-benefit analysis – An analysis shall identify and define the costs and benefits of implementing or not implementing the identified security methods.
 - iv. Safeguard selection – Safeguards shall be selected that are the most appropriate security methods to mitigate or manage identified risks to critical information systems and ePHI. Such selections will be based on the nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards.
 - v. Assignment of responsibility – Appropriate workforce members will be identified and assigned responsibility for implementing and managing selected safeguards.
 - vi. Security method evaluation - Selected security safeguards will be regularly evaluated and revised as necessary.
 - vii. The results of each of the above steps will be formally documented.

1.3 Sanctions for Noncompliance

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(1)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.”

1. To ensure that all workforce members fully comply with Security Policies, The Company will appropriately discipline and sanction employees and other workforce members for any violation of the HIPAA Security Policies and Procedures

Procedure

1. Security Violations that Prompt Consideration of Disciplinary Action.
 - i. Human Resources or a department / person with similar responsibilities may discipline a workforce member, who violates the HIPAA Security Rule
 - ii. Human Resources or a department / person with similar responsibilities may also discipline managers or supervisors, if their lack of diligence or lack of supervision contributes to a subordinate's Security Violation.
2. Investigation of Security Violation
 - i. A workforce member who becomes aware of a Security Violation shall promptly communicate the report to the HIPAA Security Officer and his or her supervisor or Human Resources or a department / person with similar responsibilities.
 - ii. After receiving a reported Security Violation, the HIPAA Security Officer or someone designated by him or her shall determine the facts and circumstances surrounding the violation and report the findings to Human Resources or a department / person with similar responsibilities.
3. Imposition of Discipline
 - i. Human Resources or a department / person with similar responsibilities shall impose sanctions for a Security Violation in accordance with Human Resources policies.
4. Reporting of Security Violations
 - i. The failure to report a known Security Violation could lead to discipline because each workforce member has an obligation to report any Security Violation of which the workforce member becomes aware to the HIPAA Security Officer and to his or her supervisor or the Human Resources Department or a department / person with similar responsibilities.

1.4 Information System Activity Review

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(1)(ii)(D)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."

1. Internal audit procedures shall be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
2. To ensure that system activity for all that contain ePHI is appropriately monitored and reviewed, the following procedures outlined below should be followed at a minimum:
 - i. An internal audit procedure should be established and implemented to regularly review records of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity.
 1. Audit logs, activity reports, or other mechanisms to document and manage system activity should be reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on each information system. The interval of the system activity review should not exceed, but may be less than, 90 days.
 - ii. An Audit Control and Review Plan should be created and approved by the HIPAA Security Officer. This plan should include:
 1. Systems and Applications to be logged
 2. Information to be logged for each system
 3. Procedures to review all audit logs and activity reports
 4. Security incidents such as activity exceptions and unauthorized access attempts should be detected, logged and reported immediately to the appropriate system management and HIPAA Security Officer in accordance with the HIPAA Security Policy #6 – Security Incident Procedures
3. A Risk Analysis as defined in Section 1.1 of The Company's HIPAA Security Policy #1 - Security Management Policy should be performed annually but not more than every two years.

Creation Date:

Effective Date:

Last Revision Date:

SAFER Guides Summary

The SAFER Guides were created to optimize EHR/EMR safety. They are a self-assessment tool with nine guides that are separated into three groups. Each guide contains recommended practices involved with EHR/EMR use and can be found below.

We have provided a summary of these nine guides and recommended practices. For an interactive worksheet which helps understand and track each recommendation, please use the links provided in each category. Each worksheet, provided by HealthIT.gov, provides additional information on each recommendation, sections to record notes, and more. These resources can be downloaded, saved, printed, and further edited to aid in attestation.

Table of Contents

Foundational Guides	3
1. High Priority Practices	3
Safe Health IT	3
Using Health IT Safely	3
Monitoring Safety	3
2. Organizational Responsibilities	4
Safe Health IT	4
Using IT Safely	4
Monitoring Safety	5
Infrastructure Guides	6
3. Contingency Planning	6
Safe Health IT	6
Using Health IT Safely	6
Monitoring Safety	6
4. System Configuration	6
Safe Health IT	7
Using Health IT Safely	7
Monitoring Safety	7
5. System Interfaces	7
Safe Health IT	8
Using Health IT Safely	8
Monitoring Safety	9

Clinical Process Guides	9
6. Patient Identification	9
Safe Health IT	9
Using Health IT Safely	9
Monitoring Safely.....	10
7. Computerized Provider Order Entry (CPOE) with Decision Support	10
Safe Health IT	10
Using Health IT Safely	10
Monitoring Safely.....	11
8. Test Results Reporting and Follow-up.....	12
Safe Health IT	12
Using Health IT Safely	12
Monitoring Safely.....	13
9. Clinician Communication	13
Safe Health IT	13
Using Health IT Safely	13
Monitoring Safely.....	14

Foundational Guides

1. High Priority Practices

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_high_priority_practices.pdf

Safe Health IT

- Both data and application configurations are backed up on redundant hardware systems
- EHR/EMR downtime and reactivation policies and procedures are available, complete, and regularly reviewed.
- Coded data elements in the EHR/EMR are used for the entering/storing of allergies, problem list entries, diagnostic test results (including interpretations of results, such as “high” and “normal.”
- Charting templates and evidence-based order sets are available for common procedures, clinical conditions, and services.
- Interactive clinical decision support (CDS) functions and features are available and working correctly. These can include, but are not limited to, info buttons, warnings, and passive suggestions.
- Hardware and software modifications, as well as system-to-system interfaces, are tested to ensure data isn’t lost, incorrectly entered/displayed, or transmitted between (or within) EHR/EMR system components.
- All EHR/EMR-embedded clinical knowledge, logic, and rules are both reviewed and addressed regularly, as well as when changes in the system occur.
- Policies/procedures result in accurate patient identification in all steps of the clinical workflow.

Using Health IT Safely

- Required information to identify patients is clearly displayed on screens and printouts.
- Human-computer interface is designed to ensure all required information is visible/readable/understandable, as well as easy to use.
- The system can be used to track order status.
- When necessary, clinicians can override clinical interventions that are computer generated.
- The EHR/EMR is used to order diagnostic tests, procedures, and medications.
- Knowledgeable staff are available to test/train/provide support to clinical EHS users.
- Common diagnostic and medications have pre-defined orders established in the system.

Monitoring Safety

- Key practice and organization EHR/EMR safety metrics are monitored.
- Patient safety hazards, that are EHR/EMR-related, are reported to all applicable parties and all steps are taken to address said hazards.
- Actions to optimize safety/safe use of EHRs/EMRs include clinician engagement.

2. Organizational Responsibilities

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_organizational_responsibilities.pdf

Safe Health IT

- EHR/EMR software, hardware, internet/network service provider (ISP) safety and performance are regularly monitored and maintained by assigned staff members.
- EHR/EMR software, hardware, and network/ISP performance and safety problems are regularly tested and promptly corrected by designated staff members.
- The responsibility of selection, monitoring, testing, and maintaining clinical decision support (CDS) performance/safety is handled by assigned staff members.
- All IT staff and EHR/EMR users are trained on best practices of data confidentiality and patient privacy maintenance while working with PHI/ePHI.

Using IT Safely

- All parties involved in high-level decision making (e.g. practice owners, board of directors, etc.) are committed to creating and maintaining a “culture of safety” where safety and safe use of EHRs/EMRs is incorporated.
- The management and optimization of the safety/safe use of EHRs/EMRs is based on an existing and effective decision-making structure.
- The management of Clinical Decision Support (CDS) content is the responsibility of designated/assigned staff members.
- All levels of decision-making regarding EHR/EMR that affects clinical use require practicing clinician participation.
- Upon clinicians delegating parts of documentation tasks, order entry, and medication reconciliation, clinician oversight is maintained.
- EHR/EMR users have applicable training and support readily available.
- EHR/EMR training and support are tailored to user needs, is high quality, and provided by high quality trainers.
- To ensure the optimization of complete and safe use, the delivery and content of training for EHRs/EMRs will be assessed regularly.
- The analysis of workflow is used to ensure the EHR/EMR is used safely for delivering care, as well as mapping clinical work.
- Clinical staff are assigned the task of ensuring all CDS content (e.g. protocols and alerts) supports clinical workflow being effective in all settings of practice.
- Policies of the organization facilitate the reporting of EHR/EMR-related hazards/errors and ensures reports are investigated and addressed promptly.
- Records are maintained of all reported/addressed EHR/EMR-related errors and hazards.

Monitoring Safety

- EHR/EMR-related software, hardware, CDS, and network/ISP performance are maintained by assigned staff members who are given the proper oversight and are adequately funded.
- Maintenance of all EHR/EMR-related software, hardware, CDS, and network/ISP performance and safety is regularly monitored by staff members.
- When there are problems with EHR/EMR-related software, hardware, CDs, and network/ISP systems, EHR/EMR users receive timely assistance, as a result of organizational procedures being in place.
- EHR/EMR users are to be made aware of any system changes prior to them being put in place, via communication mechanisms, and are able to provide safety-related feedback concerns both before and after the changes are implemented.
- Employees/staff in positions responsible for EHR/EMR safety are encouraged to communicate with colleagues in similar roles, as well as participate in relevant activities.
- The conducting of self-assessments, including the SAFER Guides are routinely conducted by a designated team, and then risks of delaying/forgoing recommended practices are assessed.
- The organization develops a measurement strategy for high priority safety standards.
- EHR/EMR safety concerns are to be identified by, and are the responsibility of, both EHR/EMR developers and healthcare organizations.

Infrastructure Guides

3. Contingency Planning

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf

Safe Health IT

- All hardware responsible for running critical operation applications is duplicated.
- During an extended power outage, sufficient fuel and an electric generator are available to support the EHR/EMR.
- During downtimes, paper documentation/forms are available to support the functions of the EHR/EMR.
- Both patient data and software configurations that are critical to the operation of the organization are to be backed up.
- Policies/procedures are followed to ensure patient information is accurate when preparing for/during/after downtimes.

Using Health IT Safely

- Staff is trained/tested on both downtime and recovery procedures.
- A communication strategy is in place, that can function outside of the computing infrastructure, exists for use during downtime/recovery periods.
- Policies/procedures are in place to ensure the EHR/EMR downtimes and recover processes facilitate continuity of operations in regard to critical business operations and safe patient care.
- The read-only EHR/EMR system and the locally maintained backup of the user interface are clearly differentiated from the live/production EHR/EMR system.
- All users are trained on strategies to prevent ransomware, including but not limited to identifying malicious emails.

Monitoring Safety

- Strategies for monitoring and comprehensive testing are in place to prevent/manage EHR/EMR downtime occurrences.
- Functional system downtimes (e.g., unreasonable slow response times) are both identified and addressed proactively.
- Root-cause analysis (or other equivalent approaches) are used to review unexpected, greater than 24-hour, extended system downtimes.

4. System Configuration

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_system_configuration.pdf

Safe Health IT

- Clinical areas contain a sufficient number of EHR/EMR access points.
- The EHR/EMR is safely stored in a electronically and physically secure manner.
- Strong authentication mechanisms are used to protect the organization's information assets.
- All system software and hardware (e.g., operating system) that is required to run the EHR/EMR, and their modifications, are individually tested, as-installed before go-live, and after go-live they are closely monitored.
- System interfaces and clinical applications are individually tested, as-installed before go-live, and after go-live they are closely monitored.
- Computers/displays housing identifiable patient data in publicly accessible areas will be configured to ensure said data will be physically and electronically.
- Upon major system changes (e.g., upgrades to browsers, hardware, and operating systems), documented processes ensure integrity during and after these changes.

Using Health IT Safely

- All clinical content is complete, up-to-date, available, and tested. Clinical content includes, but is not limited to, clinical charting templates, content used to create order sets, and to generate reminders in the EHR/EMR.
- A role-based access system being used to make certain all features, functions, patient data, and applications are only accessible to users with role-based appropriate level of authorization.
- The configuration of EHR/EMR ensures EHR/EMR users are working in the live/production environment, and cannot be confused with training/test and/or read-only backup versions
- Any system configuration settings, that can limit clinicians' practice, are minimized, closely monitored, and carefully implemented subsequent to clinician acceptance.
- Human-computer interfaces are configured for ideal use for different clinical contexts and users.

Monitoring Safety

- Processes and methods are in place within the organization to ensure key configuration settings, and the monitoring of their effects, are working as intended.

5. System Interfaces

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_system_interfaces.pdf

Safe Health IT

- Standardized protocols and supports for the exchange of data with the EHR/EMR and other systems are in place.
- The organization uses up-to-date and established versions of the following: operating systems, application software, malware and virus protection software, and interface protocols.
- All system-to-system interfaces use the standard clinical vocabularies that are also used by connected applications.
- Free-text and coded data elements are transmitted without changes or loss to the content of the information, due to proper configuration of the system-to-system interfaces.
- The interface testing (intensity and extent) is congruent with both the interface's technical complexity and the reliability, accuracy, and timeliness of the data that travels through the interface.
- The organization has procedures in place, any time a major system upgrade or change affects the interface, to determine and ensure users on both sides of the interface accurately understand and use the information that traverses the interface.
- Software and hardware changes on any side of the interface are tested before, as well as monitored after, go-live.
- A software and hardware environment exists, that is physically separate from the live/production environment, from the live environment for interface testing.
- Policies/procedures explain, in an orderly manner, the stopping and restarting the exchange of all data across the interface.
- Security procedures, which includes role-based access, are created for monitoring and managing key designated aspects of data exchange and interfaces.

Using Health IT Safely

- Personnel are available and have the skills required to configure, test, and also manage all of the operational system-to-system interfaces.
- Clear documentation indicates financial, administrative, and clinical data exchange needs. It also includes how the organization's data will be used, as well as the designated person responsible for maintaining the interface and its connected systems.
- When any changes are made that result in the content of the data files being affected or allowable values being transmitted via the interface (e.g., charge master or orderable catalog), the organization that is responsible for the management of the clinical content will be certain to notify those involved with the use or maintenance of system interfaces.
- The system interface's operational status is clear and understandable to its users in regard to all clinical use. This includes, but is not limited to, knowing when the interface is unable to transmit/receive alerts, messages, or any crucial information.
- Contextual information can be transmitted by the interface, such as sources of information or units of measure, to allow clinicians to interpret information properly.
- Readily preventable errors are avoided by management of interface problems that are associated with known interface risks and size limits of data fields.

Monitoring Safely

- The use and performance of system interfaces are monitored regularly by the organization. This also includes monitoring the volume of interface transactions and the interface error log.
- Upon the detection of interface errors, they are fixed, reported, and utilized to improve interface testing by constructing new tests with the new error information.

Clinical Process Guides

6. Patient Identification

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_patient_identification.pdf

Safe Health IT

- Patients must be identified before importing data, via a patient index that is organization-wide and includes demographic info and medical record number (or multiple numbers if used by separate parts of the same organization, with the primary number/key).
- Clinicians can facilitate accurate patient identification by having the ability to create electronic lists that are personalized based on multiple criteria (e.g., user, service, time, location).
- All information used to identify patients is clearly displayed on printouts, wristband, and all portions of the EHR/EMR interface.
- The EHR/EMR displays visually distinct patient names when they are on adjacent lines.
- “Check digits” are incorporated into medical record numbers to assist in the prevention of data entry errors.
- Upon attempting to create a new record for a patient or attempting to look for a patient and the search results in multiple options with the same/similar name, users are given an alert/warning.

Using Health IT Safely

- Standardized procedures are used to register all patients in a centralized, common database.
- The EHR/EMR’s test, training, and read-only user interfaces are distinctly different than the production/live version. The purpose being to prevent information being unintentionally entered into the wrong system.
- If a patient is unable to supply required information or the patient registration system is unavailable, the organization has a documented process to assign a temporary unique patient ID that is later merged to a permanent ID.
- Patient identity is verified at key points and or transitions during their care. Examples of this are when being assigned to a room, before surgery/procedures, vital sign recording, during lab work, and during medication administration.

- The EHR/EMR limits that patient records can only be viewed on a computer one at a time.
- Deceased patients are clearly identified as deceased.
- The organization ensures careful monitoring of using test patients in the production/live environment. When these tests occur, they are clearly identifiable as test patients (e.g., different color header for test patients) and have assigned test names that are unambiguous (e.g., includes numbers, multiple Zs, etc).

Monitoring Safely

- The patient database is regularly monitored by the organization for duplicate patients/records and patient identification errors.

7. Computerized Provider Order Entry (CPOE) with Decision Support

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_cpoe.pdf

Safe Health IT

- Prior to order entry, coded reaction and allergen information are entered into the EHR/EMR. This includes “NKA” no known allergies.
- Evidence-based order sets are readily available, and updated regularly, in the EHR/EMR for common tasks.
- User-entered items that are orderable can be looked up from, or matched to, a list of standard terms.
- The EHR/EMR can facilitate acknowledgement and also cancellation of receipt orders. These orders can be from the pharmacy, laboratory, or radiology.
- Relevant clinical context is used for displaying CDS alerts.
- CDS uses guidelines from authoritative sources to incorporate guidelines and best practices. Authoritative sources can be medical specialty professional associations, national organizations, etc.

Using Health IT Safely

- Clinicians are trained and tested on the operations of the CPOE before being given their login credentials.
- Clinicians are engaged in the implementation, reviewing, and updating CDS.
- The CPOE is being used to order all diagnostic tests, medications, and procedures for which the CPOE is available.
- Orders are stored and entered in coded, standardized form. Minimal free-text is used in order entry.

- Order entry information is relayed electronically to those responsible for completing/carrying out the order. Mobile messaging, or messaging through the computer would be examples of how it could be electronically relayed.
- Interruptive alerts/pop ups are only used for high priority and high-risk procedures. These alerts are to be used with discretion.
- Upon entry of new allergies and new orders, drug allergy checking needs to occur.
- All high-risk procedure orders, diagnostic testing, and medication require duplicate order checking. As needed/PRN medications are excluded from this requirement.
- Drug-condition checking occurs for identifying important reactions between selected conditions and drugs.
- Drug-patient age checking occurs to identify any important age-related medication issues.
- The checking of dose range (e.g., maximum daily or daily dose) will occur before orders for medication are submitted for dispensing.
- A procedure/process is in place requiring interactions are reviewed to ensure only the most significant interaction-related alerts are given to clinicians. The organization will determine which interaction-related alerts are the most significant.
- Clinicians must authenticate/sign an order by being required to re-enter their unique PIN or password.
- Consequent/corollary orders are suggested automatically, and then linked with the original order, in a way in which changes would be reflected when/if the original order is renewed, rescheduled, or discontinued.
- All users are able to access authoritative clinical reference materials straight from the EHR/EMR. This would also include organization-specific materials when applicable.
- The functionality of the CDS and CPOE are tested to ensure ideal operation before go-live before clinical use of the production system. Functionality testing also needs to occur with test patients in the production system before go-live/clinical use.
- All CDS and CPOE questions that are presented to the user are unambiguous.
- Usability testing, determined by best practices from human factors engineering, supports CDS and CPOE use an implementation.
- During the process of order entry, critical patient data is visible.
- If additional steps are required to complete an order, the clinician is made aware during the ordering process.
- Use of acronyms and abbreviations are standardized and used minimally.
- Before high-risk medications are prescribed, additional safeguards are implemented in the EHR/EMR. Additional safeguards could include a second qualified staff member double-checking the order.

Monitoring Safely

- Key CDS and CPOE metrics are defined, acted on, and monitored to optimize use and safety.

8. Test Results Reporting and Follow-up

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer_test_results_reporting.pdf

Safe Health IT

- Test values, names and interpretations for lab results are stored within the EHR/EMR. These should be stored using standardized nomenclature and as structured data.
- Reports that are predominantly test-based test reports will have a coded (e.g., normal, abnormal) representation that is associated with them. These include, but are not limited to pathology reports, radiology reports, etc.
- The functionality for both ordering tests and reporting results is tested before and after go-live/production.
- Upon the occurrence of system changes in applications or components related to diagnostic services and CPOE, both data and data presentation are reviewed for completeness and accuracy.

Using Health IT Safely

- The CPOE is used for diagnostic test orders and are transmitted electronically to the diagnostic service provider. Some examples would be radiology, labs, etc.
- The EHR/EMR is able to track all submitted orders, as well as their related procedures. An example would be a blood test was collected, the test was completed, results were reported, and they were acknowledged.
- Both the ordering clinician, as well as the follow-up clinician if applicable, are identified in the EHR/EMR on all ordered tests and test reports.
- Amendments to test results are clearly visible on both the EHR/EMR and the printed reports.
- Electronic notification to ordering and follow-up clinicians occurs when test results are amended or changed. Clinicians are also contacted directly upon any clinically significant changes.
- Reference labs/"send out" tests are electronically traced, and their results are also incorporated into the EHR/EMR. Results in the EHR/EMR will include the coded test name, result value, and the interpretation.
- Written policies are in place that indicate unambiguous responsibility for test result follow-up. There is a shared understanding that there is a responsibility for everyone involved to provide follow-up care.
- Backup procedures are in place to ensure test results are received by someone who is responsible for the patient's care. This should occur for workflows, especially critical ones, that are identified as vulnerable to the mishandling of test results.
- All test results are flagged that are considered to be abnormal or outside of normal range.
- Results should be displayed in a way that they are difficult to overlook, are understandable, clearly visible, and easily accessible.
- Flags/"basket alerts"/automated non-interruptive result notifications are limited to only what is clinically relevant, in an effort to minimize "alert fatigue."

- Result notifications are to remain in clinician inboxes until said clinician takes action to address them.
- There is an EHR/EMR process where clinicians can either assign surrogates to review their notifications or enable them to access the principal clinician's inbox.
- Mechanisms are in place to allow clinicians to forward both results and result notifications to clinician-to-clinician.
- The EHR/EMR has summarization tools available to trend and graph laboratory data.
- The clinician's EHR/EMR inbox can sort test results according to clinically relevant criteria (e.g., severity, date/time, patient name, location, read/unread).
- Clinicians are able to set reminders for themselves and others in the EHR/EMR to facilitate follow-up on test results.

Monitoring Safely

- The organization monitors, as part of Quality Assurance, selected practices related to both test result reporting and follow up. Practices needing to be monitored include, but are not limited to, clinicians following up on test results and test result review.
- The organization monitors and then addresses test results that were never sent to a clinician or were transmitted to the wrong clinician, as part of their Quality Assurance. Examples would be an error due to provider/patient misidentification, an interface error, etc.
- Policies and procedures are in place within the organization to ensure timely patient notification that is monitored. This is to include normal and abnormal test results.

9. Clinician Communication

Interactive Worksheet:

https://www.healthit.gov/sites/default/files/safer/guides/safer_clinician_communication.pdf

Safe Health IT

- Delivery of urgent clinical information is recorded in the EHR/EMR and delivered in a timely manner to clinicians.
- Policies and trainings have been facilitated to ensure messaging systems are used appropriately and limit unnecessary use.
- Clinicians can look up the status (e.g., sent, delivered) of their communications in the electronic messaging system in the EHR/EMR.
- The original sender of electronic messages, as well as the time and date it was sent, is clearly displayed.

Using Health IT Safely

- The EHR/EMR "facilitates provision of all necessary information for referral and consult requests prior to transmission.
- The EHR/EMR allows both forwarding of messages from clinician-to-clinician, as well as accurately routes clinician-to-clinician records.

- A clinician can obtain clinician and patient contact information (e.g., phone, fax, email) electronically. They are also able to access clinicians currently involved in a patient's care.
- Urgency of messages is able to be indicated in the electronic messaging system.
- A copy of clinician-to-clinician communications is documented in the EHR/EMR.
- The EHR/EMR displays time-critical and time-sensitive information more prominently than information that is less urgent.
- Organization and design policies of the EHR/EMR facilitate the clear identification staff/clinicians who are responsible for follow-up/action in response to a message.

Monitoring Safely

- Timeliness of responses and acknowledgement of messages are monitored by existing mechanisms.

HIPAA Security Policy #2

Administrative Safeguards Security Officer Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

Under the HIPAA Security Regulations, The Company is required to designate a security official who is responsible for the development and implementation of its security policies and procedures.

Policy

2.1 Assigned Security Responsibility

SAFEGUARD: Administrative

TYPE: Standard

HIPAA HEADING: REFERENCE: 45 CFR 164.308(a)(2)

SECURITY REGULATION STANDARDS LANGUAGE:

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

1. An individual will be assigned to assume responsibility for developing, implementing, maintaining, and monitoring adherence to The Company security policies and procedures. This role is called the HIPAA Security Officer.

Procedure

1. The HIPAA Security Officer is responsible for:
 - i. Ensuring that appropriate security measures and standards are implemented and enforced with regard to ePHI. The security measures implemented should be based on the criticality, sensitivity, and public or private nature of the data.
 - ii. Review rights of authorized users of ePHI on a regular basis.
 - iii. Review access and system logs for systems that contain ePHI.

- iv. Investigate and report on security problems and issues and refer such matters to the appropriate officials.
- v. Develop conditions of use or authorized use procedures for ePHI.
- vi. Provide training to regularly remind workers about their obligations with respect to information and ePHI security.

Creation Date:

Effective Date:

Last Revision Date:

HIPAA Security Policy #3

Administrative Safeguards
Workforce Security Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to ensure that all workforce members who need access to electronic Protected Health Information (ePHI) have the appropriate access while preventing all others from obtaining access to ePHI.

Policy

3 Workforce Security Policy

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(1)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) [Information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information."

1. The Company will ensure that only properly authorized workforce members shall have access to ePHI Systems. Workforce members shall not attempt to gain access to any ePHI that they are not properly authorized to access. The Company shall train its workforce members on proper and appropriate use of access rights.
2. The Company shall take reasonable and appropriate steps to ensure that workforce members who work with or have the ability to access ePHI are properly authorized and/or supervised.
3. The Company workforce members shall be screened, as appropriate, during the hiring process.
4. The Company shall implement a documented process for terminating access to ePHI when employment of workforce members ends or when access is no longer appropriate.

3.1 Authorization and Supervision

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(3)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."

1. The Company will take reasonable and appropriate steps to ensure that workforce members who have the ability to access ePHI or work in areas where ePHI might be accessed shall be properly authorized and/or supervised. The Company will use a Minimum Necessary Policy, which is one of its HIPAA Privacy policies, and other policies as appropriate, as the basis for the type and extent of authorized access to ePHI.

Procedure

1. The Company will implement procedures to ensure that only workforce members with a need to access ePHI are granted access to ePHI. No unauthorized access to ePHI will be allowed.
2. The Company shall maintain documentation detailing each workforce member's role and responsibilities, why such workforce member requires access to ePHI and the specific levels of ePHI access required by such workforce member.
3. The Company shall ensure that all workforce members who work with ePHI are supervised so that unauthorized access to ePHI is avoided. (See HIPAA Security Policy #4 – Information Access Management).

3.2 Workforce Clearance Procedure

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(3)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures to determine that the access of a workforce member to Electronic Protected Health Information (EPHI) is appropriate."

1. The Company shall develop and implement procedures to ensure that the ePHI access of its workforce members is appropriate when granted and continues to be appropriate on an on-going basis. The Company shall maintain documentation detailing each workforce member's current role and responsibilities and the ePHI access required for such role and responsibilities. (See HIPAA Security Policy #4 -- Information Access Management).

Procedure

1. Each system manager (person who is responsible for the access levels and permissions of a system) shall perform an initial review for each system that uses ePHI to insure that the current user list as well as the level of access for each user is appropriate. Each system manager should perform a subsequent review at least annually.
2. Each supervisor shall advise the appropriate system manager when a workforce member's role changes so that the workforce member's access level can be adjusted promptly.
3. The Company shall review prospective workforce members' backgrounds during the hiring process and, as appropriate, shall perform verification checks on prospective workforce members. The Company shall analyze prospective workforce members'

access to and expected abilities to modify or change ePHI as one of the bases for the type and number of verification checks conducted. Verification checks may include:

- i. Confirmation of claimed academic and professional qualification
- ii. Professional license validation
- iii. Credit check
- iv. Criminal background check
- v. Other state or federal database checks

3.3 Termination Procedure

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(3)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section."

1. The Company shall develop and implement procedures for terminating access to ePHI when the workforce member's employment ends or when the access granted is determined to be no longer appropriate. (See HIPAA Security Policy #4 – Information Access Management).

Procedure

1. The termination procedures should include the following steps:
 - i. A notification mechanism to ensure that the appropriate personnel are made aware that the workforce member's access to ePHI is no longer required.
 - ii. Recovery of all forms of access to PHI and ePHI that was granted or assigned to that workforce member. Examples include, but are not limited to, keys, remote access tokens, and identification badges.
 - iii. Disabling the workforce member's accounts on networks and system.
 - iv. Disabling remote access to networks and systems
 - v. Changing administrative or other shared passwords of which the workforce member has been made aware.

Creation Date:

Effective Date:

Last Revision Date:

Termination Checklist

Physical: Did the employee have any company issued devices like a laptop, smartphone, tablet or USB drive? Was the employee issued any company credit card? Did the employee have any keys or badge access to the office or restricted area within the office? Was there any shared access code to an alarm system or the building itself? The physical realm is an important area to consider when an employee is terminated. Think about what physical access the employee had during their employment. These physical items should be confiscated before or during termination.

Technical: Technical areas that should be considered upon termination include but are not limited to; network level access for workstations and laptops, EHR and Practice Management access, external websites (insurance websites, billing applications) and wireless and remote access capabilities. Technical access is typically the first area where privileges are revoked when a termination occurs but there are often many areas organizations miss when completing this step. Think about all the areas that employee had access to during their time with the organization.

Notification: Notification of termination should be promptly provided to the appropriate individuals prior to termination if possible. If advanced notice isn't available, notice of termination should be provided to the appropriate individuals the day of termination. Individuals who may be notified and involved in employee termination procedures include:

- Security Officer
- Human Resources and Payroll
- IT department or representative

Termination Checklist

Name	Description	Physical or Technical	Responsible Party	Complete?

Upon Final completion

Supervisor Name: _____

Signature: _____

Date: _____

Termination Policy

This policy outlines responsibility and the process for terminating system access for all (company name) employees/workforce members, contractors and others that require such access in support of business needs. The objective of this policy is to promote a high level of information security by providing access to system resources only while performing company business.

Responsibilities: Administrators are responsible for granting/terminating access for all individuals under their span of management control (employees, workforce members, temporaries and contractors). System access includes both internal systems and systems provided by external business partners.

Termination of Access: it is essential that administrators terminate access to agency systems in a timely manner to protect the information, systems and resources. Administrators are required to terminate access immediately upon termination (or even before when possible) of the employee/workforce member or contractor.

Protected Health Information (PHI): All access to PHI must be revoked upon termination.

Responsibilities of terminating access are as follows

In the case of a terminated employee, IT/Administrator should immediately:

- Revoke all computer, network, and data access the former employee has
 - This should be for both internal systems
 - Microsoft Windows Domain
 - Electronic Health Records (EHR)
 - Email
 - Etc.
 - External systems
 - including cloud based systems such as electronic health records, billing systems, picture archiving and communications system [PACS], etc.
- Remote access should be removed
- Wireless access should be removed
- The former employee should be dispossessed of all company-owned property, including technological resources like a notebook computer and intellectual property including all protected health information (PHI)
- All physical access to building should be removed
 - This could be access cards, keys, parking permits, etc.

Just as the granting of access and security clearances should be documented for future reference, the revocation of access should also be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally.

Creation Date: (replace date)

Effective Date: (replace date)

Last Revision Date:

HIPAA Security Policy #4

Administrative Safeguards Information Access Management

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to describe the procedures that The Company should establish and implement to ensure that access to ePHI is assigned and managed in a manner commensurate with the role of each workforce member.

Policy

4. Information Access Management Policy

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(4)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part."

1. This policy ensures that workforce members needing access to ePHI have appropriate access, and provides procedural safeguards to ensure that access to ePHI is properly restricted. Before access to ePHI can be established for a workforce member, that workforce member must be authorized for the appropriate level of access that their position requires. Access to ePHI and systems that store or process ePHI requires a valid and authorized user account and password. Workforce members are required to authenticate themselves to these systems using their unique user accounts.

4.1 Access Authorization

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(4)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

1. The Company shall implement procedures to establish, document, periodically review and modify if appropriate each workforce member's right to access ePHI.

Procedure

1. Procedures for Access Authorization should include the following:
 - i. Each supervisor or manager is responsible for authorizing access to systems and networks containing ePHI for his or her subordinates. Workforce members are not permitted to authorize their own access to ePHI or be granted authorization from another supervisor.
 - ii. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.
 - iii. Each supervisor or manager is responsible for periodically reviewing the access to ePHI granted to each of his or her subordinates and for modifying such access if appropriate.

4.2 Access Establishment and Modification

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(4)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

1. The Company will create a documented process for establishing, documenting, reviewing, and modifying access to ePHI in accordance with The Company's Information Access Management policy (Security Policy #4 – Information Access Management) and as set forth in the Access Authorization operational specification (see Security Policy #4.1 – Information Access Management). All requests for establishing or modifying access will be submitted in writing.

Procedure

1. Procedures for Access Establishment and Modification include:
 - i. System managers shall implement a procedure for establishing and documenting different access levels to ePHI. System managers must define access levels for accessing ePHI. These access levels must be communicated to all supervisors of workforce members.
 - ii. System managers shall implement a procedure for documenting establishment of access to ePHI. All requests for access or modification of access must be done in writing (or electronic) and copies of the request must be kept for at least 6 years
 - iii. System managers shall implement a procedure for reviewing on a regular basis workforce members' access privileges to ePHI.
 - iv. System managers shall implement a procedure for modifying the access privileges of workforce members to ePHI, as appropriate, based on the periodic reviews.

Creation Date: (replace date)
Effective Date: (replace date)
Last Revision Date:

Access Authorization form

(company name)

The HIPAA Security Rule requires both Covered Entities and Business Associates to implement policies and procedures for authorizing access to electronic protected health information (ePHI). Authorization is defined as the act of determining whether a particular user (or computer system) has the right, based on job function or responsibilities, to carry out a certain activity. This activity could include reading a file, running a program or more but the access rights should follow the minimum necessary standard.

Using this form on the following page, (company name) will identify and document each employee's access permissions to a particular program, website or computer system that may have access to ePHI. (Company name) will utilize the separate Access Modification or Establishment form if any changes to access permissions occur. (Company name) will retain this document within the employee's personnel file for the length of their employment.

Access Authorization form

(company name)

Employee Name: _____

Job title: _____

Brief Job Description: _____

System name	Access level	Restrictions	Notes

Security Officer Name: _____

Security Officer Signature: _____

Creation Date: _____

Last Revision Date: _____

Access Modification or Establishment Form

(Company name)

This form will be used when access levels to ePHI are adjusted or established for an employee. Modifications could be due to an increase or decrease in permissions. The minimum amount of access necessary to perform the appropriate job functions will be followed. This form is to be retained by management for at least the length of employment or longer if necessary.

Employee Name: _____

Date: _____

Job title: _____

Reasons for access modifications: _____

System(s) access needed to be modified or established: _____

Access rights modified or established: _____

Name of authorizing individual: _____

Signature: _____

Date: _____

System Audit Review Template

Purpose of Template

The purpose of this policy is to develop a routine audit log process to review the access of critical protected health information (PHI) in an EMR, EHR, PM or other database. Inappropriate access to PHI could be the result of a compromised password, unknown access to the system by a hacker or an employee's malicious intent. Inappropriate access to PHI could negatively impact critical system functionality and could jeopardize patient information. The organization must routinely monitor these logs to seek out inappropriate access of PHI that could indicate malicious/criminal activity.

Responsibilities

The designated HIPAA Security Officer of the organization will be responsible for routinely monitoring the audit logs and further pursue any signs of malicious activity. In addition, the HIPAA Security Officer is responsible for:

- Enabling auditing functions to occur on all critical systems containing PHI.
- Keeping an accurate log of his/her monitoring and results and signing off upon completion.
- Determine an appropriate activity level. All factors, such as job role and skill, should be considered when determining an appropriate average.
- Alert the appropriate parties if malicious intent is suspected.

The review of an audit log will also be conducted for a specific cause upon the request of another member of the organization or appropriate external party. This audit should cover a specific time frame of reference and the nature of the request should be documented.

These logs will be kept in a secure and locked location and should only be reviewed by the appropriate authorities.

Creation Date:

Effective Date:

Last Revision Date:

*By filling in the information in the System Audit Review section of this template, a workforce member attests that they have performed the system audit review and that the information entered is accurate and complete.

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: _____

Name of reviewer: _____

System Reviewed: _____

Reason for review: _____

Date on reviewed audit log: _____

Time frame evaluated (hours): _____

Activity(s) reviewed: _____

What did you find: _____

Resolution Steps Taken: _____

Signature: _____

Today's Date: 7/8/2016 Name of reviewer: Larry Johnson
System Reviewed: Practice Fusion EMR Reason for review: Weekly Checkup
Date on reviewed audit log: 7/6/2016 Time frame evaluated (hours): 24
Activity(s) reviewed: Full day review
What did you find: No inappropriate access was detected

Resolution Steps Taken: No resolution steps needed

Signature: _____

Today's Date: 7/13/2016 Name of reviewer: Larry Johnson
System Reviewed: Practice Fusion EMR Reason for review: Patient inquiry
Date on reviewed audit log: 7/1/2016 Time frame evaluated (hours): 12
Activity(s) reviewed: additions/changes to a patient's record
What did you find: Patient called with a question regarding their record. Investigation shows that

Sally Smith added the wrong diagnosis code during the patient's visit.
Resolution Steps Taken: The proper diagnosis was updated in the patient's record and the patient was notified. Sally apologized for the accident and was given a verbal warning.

Signature: _____

Today's Date: 7/15/2016 Name of reviewer: Larry Johnson
System Reviewed: Practice Fusion EMR Reason for review: Weekly review
Date on reviewed audit log: 7/12/2016 Time frame evaluated (hours): 24
Activity(s) reviewed: Full day review
What did you find: previously terminated employee John Franklin's account was seen logging into the

System at 8:52 PM.
Resolution Steps Taken: IT was notified and John's account was de-activated. An investigation into the Incident has begun to see if John did anything malicious. New termination procedures were updated.

Signature: _____

HIPAA Security Policy #5

Administrative Safeguards Security Awareness and Training

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to develop a security awareness program that will train The Company's workforce members on how to reasonably protect and safeguard ePHI while allowing them to perform their job functions

Policy

5 Security Awareness and Training

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(5)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement a security awareness and training program for all members of its workforce including management."

1. All workforce must receive security training on how to protect the confidentiality, integrity, and availability of ePHI. Workforce members will not be allowed to access ePHI until they are properly trained on how to protect and safeguard the ePHI. The security and awareness program will include the following:
 - i. Security reminders
 - ii. Procedures for guarding against, detecting and reporting malicious software
 - iii. Procedures for monitoring log-in attempts and reporting
 - iv. Procedures for creating, changing and safeguarding passwords
2. The HIPAA Security Officer will advise each existing workforce member (and new workforce members) of the level of training required and the procedure for completing training. The HIPAA Security Officer will keep a log containing the name of the workforce member, job classification, training level required, date the training was completed and date the training log was last reviewed for that employee. The Security Officer will continually track workforce members' training in the log to insure that training is completed in a timely manner and to reevaluate training needs when a workforce member's job function changes.

5.1 Security Reminders

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Periodic security updates."

1. The Company must develop and implement procedures to ensure that periodic security updates are issued to the workforce on reminders of or changes to The Company's HIPAA Security Policies.
2. The Company must develop and implement procedures to ensure that warnings are issued to the workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents. (See HIPAA Security Policy #6 -- Incident Response and Reporting).

Procedure

1. The Company will periodically provide Security updates and reminders to it's workforce on how to protect and safeguard ePHI.
2. Security updates and reminders may be in the form of emails, videos, face to face presentations, posters or other methods to distribute the updates and reminders.
3. The Company will provide Security updates when any of the following occur;
 - i. Significant changes to The Company's HIPAA Security Policies and Procedures.
 - ii. Significant changes to safeguards or controls to protect ePHI.
 - iii. Substantial risks to systems that contain ePHI.

5.2 Protection from Malicious Software

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Procedures for guarding against, detecting, and reporting malicious software."

1. The Company must develop and implement procedures for guarding against, detecting and reporting to the appropriate persons, new and potential threats from malicious software such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

Procedure

1. The Company will ensure that all systems will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions.

2. The Company shall train its workforce members to identify and protect against malicious software. Periodic Security updates will be provided to all workforce members on how to identify and avoid malicious software.
3. The Company shall notify its workforce members of new and potential threats from malicious software designed to interfere with the normal operation of a system or its contents and procedures.
4. The Company's workforce members shall not try to bypass or disable the anti-virus / anti-malware software.

5.3 Log-in Monitoring

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Procedures for monitoring log-in attempts and reporting discrepancies."

1. The Company shall train its workforce members on monitoring Log-in attempts and reporting discrepancies that the workforce member becomes aware of.

Procedure

1. The Company's workforce members should expect that all activity on systems that contain ePHI will be logged and recorded. In addition, all changes made to ePHI will be logged and recorded.
2. The Company's workforce members should be trained on how to identify and report suspicious access activity on their workstations.
3. The Company's workforce members should be trained on any limitations on the number of failed login attempts that are permitted. In addition, workforce members should be trained that failed Log-in attempts will be logged and recorded.

5.4 Password Management

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(D)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Procedures for creating, changing, and safeguarding passwords."

1. The Company must train its workforce members on creating, changing and safeguarding passwords in accordance with HIPAA Security Policy #14 - Access Control.

Procedure

1. The Company's workforce members should receive training on the password policy that is defined in HIPAA Security Policy #14 - Access Control.
2. The Company's workforce members should receive training on how to protect and safeguard passwords.

Creation Date:
Effective Date:
Last Revision Date:

HIPAA Security Policy #6

Administrative Safeguards
Security Incident Procedures

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

Policy

6 Security Incident Procedures

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(6)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to address security incidents."

1. The Company will develop and document a procedure for identifying, responding to and reporting of all security incidents against ePHI or other critical systems.

6.1 Reporting and Response

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(6)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

1. The Company will ensure that all incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI will be reported and responded to.
2. The Company shall have a Security Incident Response Team ("SIRT") charged with the responsibility of identifying, evaluating and responding to security incidents. The HIPAA Security Officer shall oversee the activities of the SIRT.

Procedure

1. The Company's SIRT will be responsible for investigating all known or suspected security incidents to systems containing ePHI or other critical systems.
2. The Company will document a procedure for all workforce members to follow to report security incidents. See **Appendix A – Security Incident Response Log**
3. The Company will ensure that all workforce members receive training on how to identify and report security incidents.
4. All workforce members must follow the documented procedure to report security incidents. In addition, workforce members must report all known or suspected security incidents.
5. All workforce members must assist the SIRT with any security incident investigations.

Creation Date:

Effective Date:

Last Revision Date:

Appendix A – Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Other)	
Response Actions Include Start and Stop times	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	

Assembling your Breach Response Team (Security Policy 6.1)

Assembling a breach response team is an integral part of breach preparation. The members of a breach response team should be identified, each bringing their own skills to the group. In the event of a breach the team will work together to address the situations and take appropriate actions based on the circumstances. The individuals selected and identified below should be made aware and agree to accept the responsibilities that come with this position. The composition of this group may depend of the size of the organization but each critical role should be identified to the best of the organization’s ability. (An alternative Breach Response Team template is available in Appendix A)

Team Leader – The team leader will be responsible for the oversight of the group as a whole. These responsibilities include but are not limited to; developing and overall coordination with the team, updating breach response procedures as necessary and ensuring the team stays on track for timely response.

Name: _____ Email: _____ Phone: _____

Information Technology – A representative from the Information Technology (IT) department should be selected to oversee the technology aspects associated with a breach. This includes but is not limited to; initial breach investigation, mitigation of ongoing harm and implementation of new technologies that can prevent future occurrences.

Name: _____ Email: _____ Phone: _____

Human Resources/PR/Outreach – An individual should be identified to lead the efforts in the communication department. Breaches, depending on size, will often involve notification steps where affected individuals or appropriate government entities are informed of the incident and the remediation steps taken by the organization. This individual will be tasked with producing and sending notifications along with responding to questions or issues raised by affected individuals.

Name: _____ Email: _____ Phone: _____

Legal Counsel – A representative from a legal team is a strong recommendation for a breach response team. Ideally this should be someone knowledgeable and experienced in these situations who can provide guidance from a legal perspective surrounding the actions taken by the team.

Name: _____ Email: _____ Phone: _____

Outside Vendors – Any outside or third-party vendors who may play a role in assisting with a breach should be identified. This could be data forensics companies, law enforcement or data breach resolution companies. If the breach had occurred within a 3rd party system, a representative from that team could play an important role as well.

Breach Response Team (cont.)

	Name	Phone Number	Emergency Phone Number	Email Address
--	------	--------------	------------------------	---------------

Team Leader				
IT Leader				
HR/PR/Outreach				
Legal Counsel				
Additional 3 rd party vendor				
Additional 3 rd party vendor				
Additional 3 rd party vendor				

Sample Breach Response Letter

Dear (affected individual),

This letter is a notification that (organization name) has experienced a recent data security breach that may have affected your sensitive personal and/or sensitive information. (Provide details of the breach. This will include date of incident and discovery date, a brief description of the incident, and the potential categories of PII and Sensitive Data that may have been compromised).

Steps we are taking

We are working diligently to actively investigate this situation. (Describe who you are working with to investigate this incident [local, state or federal authorities, data forensics groups]). (Provide the steps that you the organization are taking to mitigate the harm to the individuals and protect their information against future breaches [this could include; training, updating policies, conducting a thorough risk analysis, etc.]).

(be prepared to potentially offer free credit monitoring services to the affected individuals if necessary)

Steps you should take

We recommend that you call any of these three phone numbers below to place a fraud alert on your credit file. A fraud alert will not allow an individual to open any new accounts unless you are notified first.

<u>Experian</u>	<u>Equifax</u>	<u>TransUnion</u>
1-888-397-3742	1-888-766-0008	1-800-680-7289

By placing a fraud alert with one of these agencies it will automatically inform the other two agencies. You will also have the ability to obtain a free copy of your credit report, which we encourage you to obtain and review for any potentially fraudulent material. Be sure to carefully inspect these reports, looking for items such as accounts you did not create, inquires you did not initiate and any inaccurate personal information.

We recommend that you continue to monitor your credit reports in the future for these inconsistencies. A security freeze can also be implemented on your account which does not allow any new accounts to be created or information to be shared with creditors without your authorization. For more information on a security freeze, you can contact a representative at any of the above agencies.

We sincerely apologize for the inconveniences relating to this situation. (Organization name) takes the protection of your sensitive information seriously. We want to assure you that we are taking all appropriate actions to mitigate future instances.

Please contact us if you have any questions or concerns.

Sincerely,

(Privacy or Security Officer’s name) Contact information (toll free phone number, email, address)

HIPAA Security Policy #7

Administrative Safeguards Contingency Plan

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to plan for operational contingencies in the event of a disaster or emergency and to ensure that ePHI is protected during the disaster or emergency.

Policy

7 Contingency Plan

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(7)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

1. The Company must develop a documented procedure to respond in the event an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:
 - i. Data Backup Plan
 - ii. Disaster Recovery Planning
 - iii. Emergency mode operation plan
 - iv. Testing and Revision Procedures

7.1 Data Backup Plan

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(7)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

1. The Company shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI that is stored on all The Company computer systems.
2. The Data Backup Plan shall apply to all files, records, images, voice or video files that may contain ePHI.
3. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
4. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement shall be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.
5. Data backup procedures outlined in the Data Backup Plan shall be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available.

Procedure

1. The Company will develop and implement a procedure to ensure that daily backups and exact and retrievable copies are made of all systems that contain ePHI.
2. The Company will develop a list of systems that contain ePHI or that contain critical information and ensure that each of the systems are included in the daily backup.
3. The Company will ensure that periodic tests are performed to ensure the daily backups are valid, contain retrievable information and can be restored in the event of a disaster or emergency.
4. The Company will develop and implement a procedure to define restoration steps in the event data needs to be restored from backup.
5. The Company will ensure that any media used for the daily backup will be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
6. Data encryption should be used to safeguard any ePHI on the daily backups.

7.2 Disaster Recovery Plan

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(7)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish procedures to restore any loss of data."

1. To ensure that The Company can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster

effecting systems containing ePHI, The Company shall establish and implement a Disaster Recovery Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.

2. The Disaster Recovery Plan should include training and security reminders to all workforce members.

Procedure

1. The Disaster Recovery Plan should include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
2. The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
3. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all times.

7.3 Emergency Mode Operation Plan

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(7)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

1. The Company shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

Procedure

1. The Company will define what constitutes and triggers an Emergency that would require an Emergency Mode Operation Plan.
2. The Emergency Mode Operation Plan shall include detailed steps on how workforce members will react to emergencies that impact the confidentiality, integrity, and availability of ePHI.
3. The Emergency Mode Operation Plan shall include steps that outline security processes and controls to ensure the confidentiality, integrity, and availability of ePHI.
4. The Emergency Mode Operation Plan shall be documented and easily available to the necessary personnel at all times.
5. The Emergency Mode Operation Plan should include training and security reminders to all workforce members.

7.4 Testing and Revision Procedures

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(7)(ii)(D)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for periodic testing and revision of contingency plans."

1. The Contingency procedures outlined in the Disaster Recovery and Emergency Operations Plans (Contingency Plan) shall be tested on a periodic basis.
2. Any necessary revisions or updates to the Contingency Plans shall be made.

Procedure

1. Testing of Contingency Plan should be performed at least annually.
2. Any necessary revisions that are identified during the Contingency Plan testing will be made to the Contingency Plans.

7.5 Application and Data Criticality Analysis

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(7)(ii)(E)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Assess the relative criticality of specific applications and data in support of other contingency plan components."

1. The Company shall assess the relative criticality of specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
2. The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Procedure

1. The Company will, at least annually, identify the relative criticality of each system that may or may not contain ePHI in relation to patient care.
2. The list of critical systems will be used to prioritize which systems to concentrate on when implementing the Contingency Plan.

Creation Date:

Effective Date:

Last Revision Date:

Data Backup Plan

Client Name

Backup procedure: (describe the backup process that is used)

Backup media/equipment used: (describe the equipment that may be involved in backup, ie NAS, Tapes, USB)

Backup timeframe: (describe when or the frequency at which backups are performed)

Responsible party: (describe who is responsible for the backup procedures)

Recovery testing: (describe how often the backup procedures are tested)

If backup processes differ between systems within the office, the table below can be used to denote differences between the different systems or applications and their backup procedures.

System	Backup Method	Frequency	Notes

Creation Date: (replace date)

Effective Date: (replace date)

Last Revision Date:

Disaster Recovery Plan

Introduction

(company name) has adopted this Disaster Recovery Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope of Policy

The scope of this disaster recovery plan addresses technical recovery only in the event of a significant disruption. All personnel of (company name) must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce. The disaster recovery plan should be tested annually to maintain its integrity.

Considerations

- A disaster may occur at any time, not necessarily during work
- You must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7)
- HIPAA requires (company name) to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information
- hours
- Continuity of patient care requires uninterrupted access to patient information
- Systems that contain patient information can be affected or destroyed in many ways, such as:
 - Flooding
 - Fire
 - Loss of power
 - Acts of God: Tornado, tsunami or hurricane
 - Hackers
 - Unauthorized access or malicious activity

Policy Statement

It is the policy of (company name) to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information.

Disaster Recovery Procedures

Phase 1 - Response

- Contact required personnel (identify team members/roles that will be needed for recovery)
- Determine recovery strategies/options to be taken based on disaster

Phase 2 – Recovery

- Implement recovery procedures/failover
 - Identify restoration procedures
 - Assess risk for each procedure
 - Implement procedures

Phase 3 – Validation

- Validate integrity of restored data and the accessibility of that data
 - Test the recovery and communicate to organization

Pre-disaster measures

- Backup all patient information with accordance to (company name)'s backup policy
- Test integrity of backups (no less than bi-weekly or monthly)
- Protect by uninterruptible power supplies (UPS) all servers and other critical equipment from damage in the event of an electrical outage
- Training in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster (share Emergency Operations Plan with employees)

Disaster Recovery Teams and Responsibilities

In the event of a disaster, different groups will be required to assist in the effort to restore normal functionality to the employees of (company name).

The different groups and their responsibilities could include:

- *Disaster Recovery Lead(s)*
 - *Manage all processes of the disaster recovery plan*
- *Disaster Recovery Team*
 - *Support the DR lead*
 - *Communicate the disaster to workforce members*
- *IT Department*
 - *Handle all IT related processes of the DR plan*
 - *In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility*
 - *If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact*
 - *Install and implement any tools, hardware, and systems required for recovery*
- *Management*
 - *Ensure that the Disaster Recovery Team Lead is held accountable for his/her role*
 - *Assist the Disaster Recovery Team Lead in his/her role as required*
- *Finance Department*
 - *Ensure there is sufficient cash on-hand or accessible to deal with small-scale expenses caused by the disaster*
 - *Ensure there is sufficient credit available or accessible to deal with large-scale expenses caused by the disaster. These can include paying for new equipment, repairs for primary facilities, etc.*
 - *Review and approve Disaster Teams' finances and spending*

Disaster Recovery Lead:

_____ (put DR lead name to the left)

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs.

Role and Responsibilities

- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Be the single point of contact for and oversee all of the DR processes.*
- *Determine what systems and processes have been affected by the disaster.*
- *Communicate the disaster to the other disaster recovery teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Create a detailed report of all the steps undertaken in the disaster recovery process*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DRP test and author all DRP updates.*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored.*

Disaster Recovery Team (list the workforce members that are part of the disaster recovery team)

Name	Role/Title	Work Phone Number	Mobile/Home Phone Number

Add more columns if needed

System and Application Criticality

(company name) provides several critical systems to service its business needs. It is important to note that this DRP attempts to classify and categorize the many systems and applications supported by (company name) for the purpose of offering a tiered approach to the restoration of the services and systems in the event of a disaster. If a disaster does occur, the systems and applications will be restored in tier order as follows:

- Tier A –The system is critically fundamental to the operation of the business and must be restored immediately (less than 4 hours – time can be changed to fit business need).
- Tier B – The system is important to the daily business operations but may be out of service for 1 business day and up to 3 business days in case of a serious catastrophe. (Time can be changed to fit business need)
- Tier C – The system is not required for daily business operations and can run successfully for an extended period of time (3 business day or more) without the system being available. (Time can be changed to fit business need)

Disaster Recovery System Criticality

System / Application	Function	Consequences of Disruption	Workarounds / Alternatives	Primary Contact	Priority Tier
List name of system or application	Describe the function or purpose of the system.	Explain what would happen if the system was unavailable.	List any other method that would allow your business to continue to access the data or use the system during a disruption.	List the primary contact for the listed system.	Assign a priority tier (A, B, or C) based on the definition.

Add more columns if needed

Disaster Recovery Steps

Lists disaster recovery steps below:

Example:

1. Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
2. Determine the extent of the damage and whether additional equipment/supplies are needed
3. Determine how long it will be before service can be restored, and notify required personnel
4. Replace hardware as necessary to restore service
5. Retrieve and upload backup files if necessary to restore service
6. Ensure that backup procedures are followed
7. Verify the integrity of data restored and the ability for workforce members to access
8. Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed
9. Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations
10. Coordinate with administration and others for continuing support and ultimate restoration of normal operations

Recovery Steps (lists steps below for recovery network/systems/servers/etc)

- 1)
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)
- 10)

Add more steps if necessary

Plan Testing

The DRP should be updated every 6 months or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the

entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

(company name) is committed to ensuring that this DRP is functional. The DRP should be tested every year in order to ensure that it is still effective.

Creation Date:

Effective Date:

Last Revision Date:

Emergency Operations

Introduction

(company name) has adopted this Emergency Operations in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

Scope of Policy

This policy governs Emergency Operations for (company name). All employees/workforce members of (company name) must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

The Security Officers responsibilities:

- Employee contact and coordination.
- Patient contact and scheduled appointment coordination.
- Securing, if required, a temporary work location with all necessary equipment (computers, diagnostics, telephones, etc) and coordinating the relocation of equipment and staff to temporary location.
- Contact with IT or software vendor to secure hardware and restoration of systems.

Emergency Locations

An Emergency Location(s) should be established either within the facility or outside the facility. . In most cases, this location will be a larger conference room with the technical abilities for network and telecommunication needs. This location will serve as the on-site command center and provide communication and direction to (company name) essential workforce. It should contain at the minimum:

1. Copies of the Emergency Mode Operations and Disaster Recovery Plans
2. Computers and related supplies
3. Network connectivity
4. Telecommunications connectivity

1. Telecommunications (phone and fax)
2. Operational supplies
3. Internet access
4. Emergency Resources

Staffing

1. Technical support
2. Internal and external security
3. Administrative/individual support

Temporary manual processes for mission critical activities

1. Copies of vital records required for business continuity
2. Documented manual procedures
 - a. Capturing patient information via paper when electronic health records (EHR) systems are not functional
 - b. Other manual procedures
3. Check-off lists
4. Call sheets with critical contact information

Emergency Operations

Use this check-off list to ensure you have all the supplies you need in the event of a disaster.

	Need	Have
NOAA Weather Radio		
First Aid Kit		
Flashlights/Batteries		
Waterproof Plastic Bags		
Camera		
Pens/Pencils/Paper		
Water/Food supplies		
Generator		
Mops/Pails		
Tool kit (basic tools, gloves, etc.)		
Contact sheets		

Other:		

Emergency Contact List

This contact list should be available to all employees in the event of a disaster or emergency.

Emergency Contact References:

Contact	Contact name	Contact Information (Address, Phone, Fax, Email, Contact Name, Account #)
Police department (local)		
Fire department (local)		
Building manager/security		
Electric company		
Gas/Heat company		
Hospital (local)		
Insurance companies (List Type of Insurance, Deductibles, Policy Limits, Coverage (General Description))		
Lawyer		
Software vendors (EMR, Practice Management, Billing, etc.)		
IT Company		
Cable, Phone, Internet companies		
Banking Institutions		
Other:		

Employee Contact List:

Smaller organizations can list employee contact information below. Larger organizations may want to attach an appendix with employee contact list.

Employee name	Home phone/Cell phone	Email address (work and personal)	Address

Creation Date: (replace date)

Effective Date: (replace date)

Last Revision Date:

HIPAA Security Policy #8

Administrative Safeguards Evaluation of Security Policies and Procedures

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the procedures that will ensure that each Security Policy adopted by The Company is periodically evaluated for technical and non-technical viability.

Policy

8 Evaluation

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(8)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

1. The Company's Security Policies initially should be evaluated to determine their compliance with the HIPAA Security Rule. Once compliance with the HIPAA Security Rule is established, The Company's Security Policies should be evaluated on a periodic basis to assure continued viability in light of technological, environmental, operational or regulatory changes that could affect the security of ePHI.

Procedure

1. The Company HIPAA Security Officer shall periodically (at least annually) evaluate its HIPAA Security Procedures to ensure that such Procedures maintain their technical and non-technical viability and continue to comply with any Regulatory Policies
2. The results of the periodic security evaluation shall be documented and retained.
3. In the event that one or more of the following events occur, the policy evaluation process should be triggered:
 - i. Changes in the HIPAA Security Regulations or Privacy Regulations.

- ii. New federal, state, or local laws or regulations affecting the privacy or security of PHI or ePHI.
 - iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures.
 - iv. A serious security violation, breach, or other security incident occurs
4. Any changes to Security Policies or Procedures shall be communicated to all workforce members.

Creation Date:

Effective Date:

Last Revision Date:

HIPAA Security Policy #9

Administrative Safeguards
Business Associate Contracts

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to cover all Business Associates that create, receive, maintain, or transmit ePHI on The Company's behalf. The Company will develop and implement contracts that ensure the Business Associate will appropriately safeguard the information in compliance with the HIPAA Security Rule.

Policy

9 Business Associate Contracts

TYPE: Standard

REFERENCE: 45 CFR 164.308(b)(1); 45 CFR 164.308(b)(4)

SECURITY REGULATION STANDARDS LANGUAGE:

"A covered entity, in accordance with § 164.306 [Security standard: General rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a)[Business Associate contracts and other arrangements] that the business associate will appropriately safeguard the information."

1. At times ePHI may be disclosed to and used by Business Associates (BA) as necessary to allow the BA to carry out a healthcare related function or activity on behalf of The Company or to provide services to The Company. A BA must sign a Business Associates Agreement (BAA) with The Company, in order to access, use or disclose ePHI. The BAA must be in writing and must contain the requirements of the Security Rule and authorized signatures.

Procedure

1. The HIPAA Security Officer shall ensure that all Business Associates enter into Business Associate Agreements that contain the requirements of the Security Rule.
2. Each Business Associate Agreement shall state that the Business Associate will:

- i. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on The Company' behalf.
- ii. Ensure that any agent, including a subcontractor to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it.
- iii. Report to The Company any security incident of which it becomes aware.
- iv. Authorize the termination of the Business Associate Agreement by The Company if The Company determines that the Business Associate has violated a material term of the contract.

Creation Date:

Effective Date:

Last Revision Date:

What Is a “Business Associate?”

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity or another business associate. A member of the covered entity’s workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. HIPAA regulations lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

The Department of Health and Human Services has provided more guidance on Business Associates at:

http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html#businessassociate

Examples of Business Associates.

- A third party administrator that assists a health care provider with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health care provider involve access to PHI.
- A consultant that performs utilization reviews for a hospital or health care provider.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.
- Companies involved in claims processing, repricing or collections (e.g., medical billing companies)
- Health information exchanges (HIEs), e-prescribing gateways and other HIOs
- Data conversion, de-identification and data analysis service providers
- Utilization review and management companies

Additional examples *may* be Business Associates:

- An Email provider (Microsoft, Google, Yahoo)
- Cloud providers where PHI may be stored (Amazon, Dropbox, Rackspace, Google Drive)
- Hosted phone vendors where PHI in the form of voicemails may be stored on the vendors systems
- IT service providers
- EHR/EMR vendors
- Answering services
- Document storage or disposal (shredding) companies
- Collections agencies
- Research firms (if performing HIPAA functions for a covered entity)
- Auditors

- Companies providing personal health records (business associate if providing personal health records on behalf of a covered entity)

Exceptions (who is *typically* not considered a Business Associate)

- An individual who performs services as part of the workforce of a covered entity (employee)
- A health care provider, to the extent that disclosures of PHI by another covered entity concern the treatment of the individual
- A plan sponsor (such as an employer), with respect to various disclosures from its group health plan
- Financial and banking institutions when performing only payment processing activities
- A janitorial service performing traditional functions where there would be no use or disclosure of PHI and any access to PHI would be incidental, if at all.
- Maintenance and repair personnel (other than working on systems holding PHI)
- Conduits (e.g., U.S. Postal Service and its electronic equivalents such as an Internet Service Provider/ISP i.e. Verizon, AT&T, etc.)

[Covered Entity Name]
[Covered Entity Contact Name]
[Covered Entity Title]
[Covered Entity Address]

[Date]

[Business Associate Name]
[Business Associate Contact Name]
[Business Associate Title]

Dear [Business Associate Contact First Name],

[Covered Entity Name] is serious about protecting patient information and ensuring that appropriate security measures are in place to comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations. As a Business Associate of [Covered Entity Name] we would like to ensure that [Business Associate Name] is protecting and safeguarding patient information with the same diligence as [Covered Entity Name].

What is a Business Associate?

A "Business Associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

What the HITECH Act did for Business Associates?

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR/EMR) systems among providers.

Under the HITECH Act, Business Associates are now required to comply with the safeguards contained in the HIPAA Security Rule and use and disclosure provisions of the HIPAA Privacy Rule.

Compliance verification

We are respectfully asking you to complete the below section and answer the questions regarding how [Business Associate Name] is currently protecting electronic protected health information and complying with the HIPAA and HITECH regulations. We would appreciate your response on or before [Date of Questionnaire to be Returned].

Please fill in the following information and answer the following questions:

Organization's name: [Business Associate Name]

Name of organization's HIPAA security officer: _____

Organization's Email: _____

Organization's Phone number: _____

Organization's Address: _____

Does your organization have a HIPAA security officer? If yes please fill in above section.

YES	NO	OTHER

Has the HIPAA security officer gone through formal HIPAA training?

YES	NO	OTHER

Have you performed a Risk Assessment on how the organization is protecting electronic protected health information in the past year?

YES	NO	OTHER

Name of organization that performed the Risk Assessment? If the Risk Assessment was performed internally please put "Internal Risk Assessment" below.

--

Do you have HIPAA Policies and Procedures?

YES	NO	OTHER

Have your employees been informed about your HIPAA policies?

YES	NO	OTHER

Have your employees been trained on HIPAA security in the past year? (This includes, full and part-time employees, contractors, temporary employees, etc)

YES	NO	OTHER

Do you use encryption to protect electronic protected health information?

YES	NO	OTHER

Do you have a documented data backup plan?

YES	NO	OTHER

Organization's compliance officer signature:

Name [Print]: _____ Title: _____

Date: _____ Signature: _____

Sincerely;

[Covered Entity Contact Signature]

[Covered Entity Contact Name]

[Covered Entity Name]

[Covered Entity Contact Title]

Business Associate Compliance Check For Cloud Vendors

Dear Business Associate,

[Covered Entity Name] is serious about protecting patient information and ensuring that appropriate security measures are in place to comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations. As a Business Associate, we would like to ensure that you are complying with HIPAA regulations, protecting and safeguarding patient information and have proper procedures to minimize the chance of a data breach.

What is a Business Associate?

A "Business Associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

What does the HIPAA Omnibus Rule do for Business Associates?

The HIPAA Omnibus Rule (Final Rule) has a significant effect on Business Associates. The Health Information Technology for Economic and Clinical Health (HITECH) Act made the portions of the HIPAA Privacy rule and the Security Rule directly applicable to Business Associates. The Final Rule sets forth in detail the manner in which some of the HITECH Act's provisions will be applied.

Under the HIPAA Omnibus Rule (Final Rule), Business Associates are now required to comply with the safeguards contained in the HIPAA Security Rule and use and disclosure provisions of the HIPAA Privacy Rule. In addition, subcontractors of Business Associates must also comply with HIPAA Regulations.

Compliance verification

We are respectfully asking you to complete the below section and answer the questions regarding how you are currently protecting electronic protected health information (ePHI) and complying with the HIPAA regulations. We will share this information with our client and it will be incorporated as part of their HIPAA compliance program.

We would appreciate your response on or before [Date of Questionnaire to be Returned].

Please fill in the following information and answer the following questions:

Organization's name: _____

Name of Organization's Contact: _____

Organization's Contact Email: _____

Organization's Contact Phone number: _____

Organization's Address: _____

Have you performed a HIPAA Security Risk Assessment within the past year?

YES	NO	More Information

Is there a process to conduct periodic vulnerability scans and penetration tests?

YES	NO	More Information

What kinds of certifications do you have (HITRUST, SSAE 16)?

YES	NO	More Information

What measures are used to protect the data from loss, theft and hacking?

YES	NO	More Information

Does the system back up an exact copy of the ePHI?

YES	NO	More Information

If so, are these backup files kept in a different location, well protected, and easily restored?

YES	NO	More Information

Is the information encrypted while at rest? In transit?

YES	NO	More Information

Do you offer the ability to activate emergency access to the information in the event of a disaster?

YES	NO	More Information

Can you provide a written copy of your Disaster Recovery procedures?

YES	NO	More Information

Are your staff members required to complete periodic training on HIPAA Security and overall data protection?

YES	NO	More Information

Is there a procedure in place for evaluating and responding to a security incident/breach?

YES	NO	More Information

Please provide any additional notes that you feel may be applicable :

Notes	
-------	--

Sample Business Associate Contract For Subcontractors

Introduction

This sample agreement is intended for use by Business Associates who may use or share protected health information with other downstream subcontractors. The form is derived from the sample documents available on the US Department of Health & Human Services' website, but by providing this form HIPAA_Secure Now is not providing legal advice. You should consult with your own legal counsel to confirm that this document will adequately address your organization's needs.

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A business associate also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure the appropriate use, disclosure, and safeguarding of protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate or a business associate and a subcontractor must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate or subcontractor; (2) provide that the business associate or subcontractor will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate or subcontractor to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate or subcontractor to report to the covered entity or business associate any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate or subcontractor to disclose protected health information as specified in its contract to satisfy a covered entity's or business associate's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate or subcontractor is to carry out a covered

entity's or business associate's obligation under the Privacy Rule, require the business associate or subcontractor to comply with the requirements applicable to the obligation; (7) require the business associate or subcontractor to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate or subcontractor on behalf of, the covered entity or business associate for purposes of HHS determining the covered entity's or business associate's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate or subcontractor to return or destroy all protected health information received from, or created or received by the business associate or subcontractor on behalf of, the covered entity or business associate; (9) require the business associate or subcontractor to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate or subcontractor with respect to such information; and (10) authorize termination of the contract by the covered entity or business associate if the business associate or subcontractor violates a material term of the contract.

This document includes sample business associate agreement provisions to help business associates and subcontractors more easily comply with the business associate contract requirements.

These are only sample provisions and use of all such sample provisions may not be required for compliance with the HIPAA Rules. Certain language may be changed to more accurately reflect specific business arrangements between a covered entity and business associate or between a business associate and subcontractor. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

This HIPAA Business Associate Agreement ("BAA"), dated as of _____ ("Effective Date"), is by and between _____, a _____ corporation ("Business Associate") and _____, a _____ corporation ("Subcontractor"). To the extent that Business Associate discloses Protected Health Information to Subcontractor, or Subcontractor handles Protected Health Information on Business Associate's behalf, in connection with services or products provided to Business Associate, or as otherwise required by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, codified at 42 U.S.C. § 1320d through d-9, as amended, ("HIPAA"), Subcontractor and Business Associate agree to the following terms and conditions, which are intended to comply with HIPAA, the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and their implementing regulations. The privacy and security provisions of this BAA shall be applicable to Subcontractor only in the event and to the extent Subcontractor meets, with respect to Business Associate, the definition of a Business Associate set forth at 45 C.F.R. §160.103, or applicable successor provisions. Now, therefore, in consideration of the foregoing and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the parties agree as follows:

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103

(c) Subcontractor. "Subcontractor" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of subcontractor]. A Subcontractor can be viewed as a Business Associate to another Business Associate.

(d) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160, Part 164, and 42 CFR Part 2.

(e) "Service Agreement" shall mean the separate agreement(s) between the parties in which Subcontractor performs functions or activities on behalf of Business Associate.

Obligations and Activities of Subcontractor

Subcontractor agrees to:

- (a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
- (b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 and 42 CFR Part 2 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
- (c) Report to business associate any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410 and 42 CFR Part 2, and any security incident of which it becomes aware;
- (d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the subcontractor agree to the same restrictions, conditions, and requirements that apply to the subcontractor with respect to such information;
- (e) Make available protected health information in a designated record set to the business associate as necessary to satisfy obligations under 45 CFR 164.524 and 42 CFR Part 2;
- (f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the business associate pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy obligations under 45 CFR 164.526;
- (g) Maintain and make available the information required to provide an accounting of disclosures to the business associate as necessary to satisfy obligations under 45 CFR 164.528 and 42 CFR Part 2;
- (h) To the extent the subcontractor is to carry out one or more of business associate's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the business associate in the performance of such obligation(s); and
- (i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.(j) [Use only when applicable] Data Use Agreement: With respect to Limited Data Sets Used or Disclosed by Business Associate in a manner permitted by the HIPAA Rules, Business Associate will:

(i) Not Use or further Disclose the Limited Data Set other than as provided for in this subsection (Data Use Agreement), which includes purposes consistent with the HIPAA Rules, including those related to research, public health or health care operations or as otherwise required by law;

(ii) Use appropriate safeguards to prevent Use or Disclosure of the Limited Data Set other than as provided for in this Data Use Agreement;

(iii) Report to Covered Entity any Use or Disclosure of the Limited Data Set not provided for by this Data Use Agreement of which it becomes aware;

(iv) Ensure that any agents to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and

(v) Not identify the individuals who are the subject of the Limited Data Set, or contact the individuals.

Permitted Uses and Disclosures by Subcontractor

(a) Subcontractor may Use and Disclose Protected Health Information as necessary to perform the services set forth in the Service Agreement, as permitted in this BAA or the Service Agreement, and as otherwise permitted by the HIPAA Rules, including for purposes related to treatment, payment, and health care operations and for public health purposes.

(b) Subcontractor may use or disclose protected health information as required by law, but will make certain they are also complying with 42 CFR Part 2.

(c) Subcontractor agrees to make uses and disclosures and requests for protected health information consistent with business associate's minimum necessary policies and procedures.

(d) Subcontractor may not use or disclose protected health information in a manner that would violate 42 CFR Part 2 Subpart E of 45 CFR Part 164.

(e) Subcontractor may disclose protected health information for the proper management and administration of subcontractor or to carry out the legal responsibilities of the subcontractor, provided the disclosures are required by law, or subcontractor obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies subcontractor of any instances of which it is aware in which the confidentiality of the information has been breached. The exception being when a disclosure does not adhere to 42 CFR Part 2. This would require additional consent from Substance Abuse Disorder (SUD) patients to provide additional consent for management and administration, legal responsibilities, and when records are required by law.

Provisions for Business Associate to Inform Subcontractor of Privacy Practices and Restrictions

(a) Business associate shall notify subcontractor of any restriction on the use or disclosure of protected health information that business associate has agreed to or is required to abide by under 45 CFR 164.522 and 42 CFR Part 2, to the extent that such restriction may affect subcontractor's use or disclosure of protected health information.

Permissible Requests by Covered Entity

Business associate shall not request subcontractor to use or disclose protected health information in any manner that would not be permissible under 42 CFR Part 2 and Subpart E of 45 CFR Part 164..

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date business associate terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Subcontractor authorizes termination of this Agreement by business associate, if business associate determines subcontractor has violated a material term of the Agreement.

(c) Obligations of Subcontractor Upon Termination.

Upon termination of this Agreement for any reason, subcontractor shall return to business associate or, if agreed to by business associate, destroy all protected health information received from business associate, or created, maintained, or received by subcontractor on behalf of business associate, that the subcontractor still maintains in any form. Subcontractor shall retain no copies of the protected health information.

(d) Survival. The obligations of subcontractor under this Section shall survive the termination of this Agreement.

IN WITNESS WHEREOF, the Business Associate and Subcontractor have executed the Agreement as of the day and year written above.

BUSINESS ASSOCIATE:

SUBCONTRACTOR:

By: _____

By: _____

Title: _____

Title: _____

Sample Business Associate Contract for Covered Entities

Introduction

This sample agreement is intended for use by Covered Entities who may use or share protected health information with Business Associates. By providing this form HIPAA Secure Now is not providing legal advice. You should consult with your own legal counsel to confirm that this document will adequately address your organization's needs.

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A business associate also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure the appropriate use, disclosure, and safeguarding of protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate or a business associate and a subcontractor must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate or subcontractor; (2) provide that the business associate or subcontractor will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate or subcontractor to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate or subcontractor to report to the covered entity or business associate any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate or subcontractor to disclose protected health information as specified in its contract to satisfy a covered entity's or business associate's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate or subcontractor is to carry out a covered entity's or business associate's obligation under the Privacy Rule, require the business associate or subcontractor to comply with the requirements applicable to the obligation; (7) require the

business associate or subcontractor to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate or subcontractor on behalf of, the covered entity or business associate for purposes of HHS determining the covered entity's or business associate's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate or subcontractor to return or destroy all protected health information received from, or created or received by the business associate or subcontractor on behalf of, the covered entity or business associate; (9) require the business associate or subcontractor to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate or subcontractor with respect to such information; and (10) authorize termination of the contract by the covered entity or business associate if the business associate or subcontractor violates a material term of the contract.

This document includes sample business associate agreement provisions to help covered entities, business associates, and subcontractors more easily comply with the business associate contract requirements.

These are only sample provisions and use of all such sample provisions may not be required for compliance with the HIPAA Rules. Certain language may be changed to more accurately reflect specific business arrangements between a covered entity and business associate or between a business associate and subcontractor. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement ("BAA"), effective as of _____ ("Effective Date"), is by and between _____, a _____ corporation ("Covered Entity") and _____, _____ corporation ("Business Associate") (each a "party" and, collectively, the "parties.") To the extent that Covered Entity discloses Protected Health Information to Business Associate in connection with services or products provided to Covered Entity, or as otherwise required by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, codified at 42 U.S.C. §1320d through d-9, as amended ("HIPAA"), Covered Entity and Business Associate agree to the following terms and conditions, which are intended to comply with HIPAA, the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and their implementing regulations, as amended. Now, therefore, in consideration of the mutual promises contained herein, the exchange of information pursuant to this BAA, and other good and valuable consideration, the sufficiency and receipt of which are hereby acknowledged, the parties agree as follows:

1. General Terms, Conditions, and Definitions

(a) "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. §160.103, and in reference to the party to this BAA, shall mean the entity defined as such above.

(b) "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. §160.103, and in reference to the party to this BAA, shall mean the entity defined as such above.

(c) "HIPAA Rules" shall mean the privacy, security, breach notification, administrative, and enforcement rules at 45 C.F.R. Parts 160, 162 and 164, as amended from time to time.

(d) "Service Agreement" shall mean the separate agreement(s) between the parties in which Business Associate performs functions or activities on behalf of Covered Entity.

(e) Other Definitions: The following terms used in this BAA shall have the same meaning as those in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Limited Data Set, Notice of Privacy Practices, Protected Health Information (limited to the information created, received, maintained or transmitted by Business Associate on behalf of Covered Entity), Reproductive Health Care, Required By Law, Secretary, Security Incident, Standard, Subcontractor, Transaction, Unsecured Protected Health Information, and Use. Additional definitions are as set forth in this BAA.

(f) Notification by Covered Entity. Covered Entity agrees to notify Business Associate of any restrictions on the use or disclosure of Protected Health Information to which Covered Entity has agreed that may affect Business Associate's use or disclosure of Protected Health Information pursuant to this BAA.

2. Obligations and Activities of Business Associate

(a) Business Associate may not use or disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law. Business Associate (i) acknowledges that in receiving, storing, processing, or otherwise dealing with any Protected Health Information subject to protection under the substance use disorder program regulations under 42 C.F.R. Part 2 or comparable state laws ("Part 2 Regulations" and "Part 2 Records"), it is bound by the provisions of the Part 2 Regulations applicable to Business Associate as a recipient of Part 2 Records; and (ii) if necessary, agrees to resist in judicial proceedings any effort to obtain access to information pertaining to such patients otherwise than as expressly provided for in the Part 2 Regulations. With regard to Part 2 Records, Business Associate must maintain on or with such records the Part 2 notice and a copy or description of patients' Part 2 consent affixed to or noted on such Part 2 Records upon receipt of such Part 2 Records from Covered Entity, and must not re-disclose such Part 2 Records without such notice and consent affixed.

(b) Business Associate agrees to use appropriate safeguards and implement recognized security practices to prevent use or disclosure of Protected Health Information other than as provided for by this BAA, and to comply with Subpart C of 45 C.F.R. part 164 with respect to electronic Protected Health Information.

(c) Business Associate agrees to report, in writing, to Covered Entity's Privacy Official, within seventy-two (72) hours of discovery, or such shorter time required by applicable law, any use or disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including Breaches of Unsecured Protected Health Information as required by 45 C.F.R. §164.410, and any Security Incident of which it becomes aware. All reports must include Business Associate's name and point of contact information; a description of what happened including the date of the incident and the date of discovery of the incident, if known; the types of Protected Health Information involved in the incident, if applicable; a description of what Business Associate is doing to investigate the incident and protect against further incidents; and other information reasonably requested by Covered Entity. For reports of incidents that would be a Breach but for the fact that there is a low probability that Protected Health Information was compromised, Business Associate must provide to Covered Entity, as soon as possible, a detailed written analysis of at least the four factors listed in 45 C.F.R. §164.402 demonstrating that there is a low probability that Protected Health Information has been compromised. For reports of incidents constituting a Breach, the report must include, to the extent available, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during a Breach of Unsecured Protected Health Information, and any other available information that a Covered Entity is required to include in a notification to the Individual under 45 C.F.R. §164.404 and applicable state law, and any other information reasonably requested by Covered Entity. Additional information must be reported by Business Associate immediately as it becomes available. Without limiting any other indemnification obligations of Business Associate, at Covered Entity's election, Business Associate must reimburse Covered Entity for the cost of outside forensic investigators if Covered Entity determines an outside investigation of the Breach or Security Incident is necessary.

(d) Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate agree in

writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

(e) Business Associate agrees to make available Protected Health Information to Covered Entity in the manner, time and format reasonably requested by Covered Entity. Business Associate also agrees to make available Protected Health Information in a Designated Record Set to Covered Entity or the Individual as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.524 and other applicable state and federal regulations, including requirements for timely provision of access to Protected Health Information.

(f) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set as agreed to or directed by Covered Entity pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.526.

(g) Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.528 and the HITECH Act. Business Associate agrees to provide to Covered Entity, within fifteen (15) days and in a secure manner, information collected in accordance with this Section 2(g) of this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528, the HITECH Act, and applicable state law and Business Associate must retain such accounting records for at least the length of time required by the HIPAA Rules and the HITECH Act.

(h) To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164 of the HIPAA Rules, Business Associate agrees to comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

(i) Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules. Unless otherwise prohibited by law or by the Secretary, Business Associate must notify Covered Entity immediately upon receipt by Business Associate of any such request, and must provide Covered Entity with copies of all materials provided to the Secretary.

(j) Business Associate agrees to, subject to subsection 4(c) below, return to the Covered Entity or Covered Entity's designee or, with Covered Entity's written permission destroy, within fifteen (15) days of the termination of this BAA, the Protected Health Information in its possession and retain no copies. All permitted destruction of Protected Health Information must be done in accordance with federal Department of Health and Human Services guidance regarding rendering Protected Health Information unusable, unreadable, or indecipherable.

(k) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to either party of a use or disclosure of Protected Health Information in violation of this BAA.

(l) Notwithstanding anything in this BAA or the Service Agreement to the contrary, Business Associate agrees to indemnify and hold harmless Covered Entity and Covered Entity's employees, affiliates, customers, directors, partners, shareholders, officers, subcontractors, and agents (each of the foregoing hereinafter referred to as an "Indemnified Party") from, and at Indemnified Party's option, defend against any and all losses, liabilities, claims, fines, damages, penalties, costs, and expenses, including, but not limited to, reasonable attorneys' fees, consultants' fees, court costs, Breach notification costs, and credit monitoring and identity theft protection fees (collectively, "Losses") to the extent that such Losses arise from, or may be in any way attributable to, any act or omission by Business Associate or Business Associate's employees, contractors, Subcontractors, agents, or representatives that constitutes or that is otherwise asserted by any regulatory agency or third party to be (i) a breach of this BAA, (ii) negligence, gross negligence, bad faith, or intentional or willful misconduct, (iii) a violation of the HIPAA Rules, HIPAA, the HITECH Act and/or any state data privacy or security law; and/or (iv) any Security Incident or Breach involving Protected Health Information in Business Associate's possession, custody or control, or for which Business Associate is otherwise responsible. The provisions of this paragraph shall survive the expiration or termination of this BAA for any reason.

(m) Except as otherwise allowed in this BAA and the HIPAA Rules, Business Associate must not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual unless the Individual has provided a valid authorization compliant with the HIPAA Rules and state law.

(n) Covered Entity, in its sole and absolute discretion, may elect to delegate to Business Associate any requirement to notify affected Individuals of a Breach of Unsecured Protected Health Information if such Breach results from, or is related to, an act or omission of Business Associate or the subcontractors, agents or representatives of Business Associate. If Covered Entity elects to make such delegation, Business Associate must perform such notifications and any other reasonable remediation services (i) at Business Associate's sole cost and expense, and (ii) in compliance with all applicable laws including HIPAA and the HITECH Act. Business Associate must also provide Covered Entity with the opportunity to review and approve of the form and content of any Breach notification that Business Associate provides to Individuals, the government, including the Secretary, and/or the media.

(o) To the extent that Business Associate submits Standard Transactions on behalf of Covered Entity, or assists Covered Entity with submission of Standard Transactions, Business Associate must comply with HIPAA's Transaction and code set Standards for such Transactions, must require any agent or subcontractor to comply with the applicable requirements for such Transactions, and must provide documentation of such compliance upon request of Covered Entity.

(p) Unless Covered Entity agrees, in writing, that this requirement is infeasible with respect to particular data, Business Associate must secure all Protected Health Information at rest or in transmission by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed in accordance with Department of Health and Human Services' applicable guidance and other applicable laws and regulations.

(q) Business Associate agrees to respond to and accommodate a request for confidential communications by an Individual, including requests to communicate or correspond with an Individual by alternative means or at alternative locations, or a request for, changes in, or a revocation of, permission by an Individual to restrict Business Associate's use or disclosure of Protected Health Information, in a timely manner in accordance with the requirements under 45 C.F.R. §164.522, and to make changes to Business Associate's processes to the extent that such request, if approved, may affect Business Associate's use or disclosure of Protected Health Information.

(r) Business Associate must not engage in information blocking, agrees to communicate with and provide access to Protected Health Information orally and in writing to authorized employees, workforce members, agents, and business associates of Covered Entity, and must comply with the Information Blocking Rule set forth in the 21st Century Cures Act regulations, 45 C.F.R. Parts 170 and 171 and any amendments (also known as the "Information Blocking Rule"). Business Associate must transmit Protected Health Information to Covered Entity's authorized employees, workforce members, agents and business associates at the request of and in the format required by Covered Entity, to the extent permitted by and in accordance with the HIPAA Rules.

(s) Business Associate must make itself, and any of its employees, agents, and subcontractors assisting Business Associate in the performance of its obligations under this BAA, available to Covered Entity at no cost to Covered Entity to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against Covered Entity, its customers, directors, officers, agents, Workforce members, or employees based upon a claimed violation of HIPAA, the HIPAA Rules, the HITECH Act, or other laws relating to security or privacy.

(t) If Business Associate is required by subpoena, civil investigative demand or similar legal process to disclose Protected Health Information, Business Associate will notify Covered Entity in advance of any disclosure of Protected Health Information that Business Associate is required by law to make, to the extent such notice is not legally prohibited, and will obtain any legally required attestations or other privacy assurances from the recipient, obtain a protective order or, if required by HIPAA or Part 2 Regulations, oppose such disclosure in the absence of a valid court order or order of an administrative tribunal requiring disclosure.

(u) With regard to Protected Health Information potentially related to Reproductive Health Care ("RHI"), Business Associate may not use or disclose RHI without an Individual's express Authorization, when the request for use or disclosure is to conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided or to identify any person for such a purpose. To the extent that Business Associate receives a request for RHI for health oversight activities, judicial and administrative proceedings, from law enforcement, or from coroners or medical examiners, Business Associate must require execution of an attestation as required by the HIPAA Rules.

3. Permitted Uses and Disclosures of Protected Health Information by Business Associate

(a) Business Associate may only use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this BAA and the Service Agreement, provided that such use or disclosure complies with the HIPAA Rules. Business Associate acknowledges and agrees that it acquires no title or ownership rights to the Protected Health Information, including any de-identified information, as a result of this BAA.

(b) Business Associate may use or disclose Protected Health Information as Required By Law.

(c) Business Associate agrees to use and disclose only a Limited Data Set when practicable and make uses of and disclosures and requests for Protected Health Information consistent with HIPAA and any of Covered Entity's policies and procedures provided to Business Associate regarding the use and disclosure of the minimum necessary Protected Health Information and consistent with Covered Entity's Notice of Privacy Practices. Covered Entity asserts that its policies and procedures regarding minimum necessary uses and disclosures are consistent with 45 C.F.R. §164.514(d) and Business Associate agrees to comply with the provisions of that rule.

(d) Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.

(e) Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(f) Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [ADD ONLY IF NECESSARY] Data Use Agreement: With respect to Limited Data Sets created or used by Business Associate on behalf of Covered Entity, Business Associate will:

(i) Not use or further disclose the Limited Data Set other than as provided for in this subsection (Data Use Agreement), which includes purposes consistent with the HIPAA Rules, including those related to research, public health or health care operations or as otherwise required by law;

(ii) Use appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided for in this Data Use Agreement;

(iii) Report to Covered Entity any use or disclosure of the Limited Data Set not provided for by this Data Use Agreement of which it becomes aware;

(iv) Ensure that any agents to whom it provides the limited data set agree in writing to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and

(v) Not identify the individuals who are the subject of the Limited Data Set, or contact the individuals.

4. Survival, Term and Termination

(a) Term.

Except as otherwise provided herein, the term of this BAA shall coincide with the Service Agreement, including any renewals, and shall be terminable in accordance with the termination provisions of the Service Agreement, or the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause

Business Associate authorizes termination of this BAA and the Service Agreement by Covered Entity if Covered Entity determines Business Associate has violated a material term of this BAA that is, in Covered Entity's sole judgment, incapable of cure or is not cured within the time specified by Covered Entity.

(c) Effect of Termination

Upon termination of this BAA, for any reason, Business Associate must return to Covered Entity or Covered Entity's designee or, with Covered Entity's prior written permission, destroy, all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate must retain no copies of the Protected Health Information. If termination or permitted destruction is infeasible, Business Associate must provide Covered Entity with written notice and, upon Covered Entity's agreement that return or permitted destruction is infeasible, Business Associate must:

- i. Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
- ii. Return to Covered Entity or, if agreed to in writing by Covered Entity, destroy the remaining Protected Health Information that Business Associate still maintains in any form;

- iii. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section, for as long as Business Associate retains the electronic Protected Health Information;
- iv. Not use or disclose the Protected Health Information retained by Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set forth in this BAA, related to Use and Disclosure for Business Associate's proper management and administration or to fulfill its legal responsibilities, and Subpart E of 45 C.F.R. Part 164, which applied prior to termination; and
- v. Return to Covered Entity or, if agreed to in writing by Covered Entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

(d) Survival

Business Associate's obligations under this BAA will survive the expiration or other termination of this BAA to the fullest extent necessary for their enforcement and for the realization of the benefit thereby by Covered Entity.

5. Interpretation and Amendment of this BAA

A regulatory reference in this BAA to a section of the HIPAA Rules means such section as in effect or as amended. Any ambiguity or inconsistency in this BAA shall be interpreted to permit compliance with the HIPAA Rules. This BAA supersedes any and all prior representations, understandings, or agreements, written or oral, concerning the subject matter herein, including conflicting provisions in the Service Agreement. In the event of a conflict between the Service Agreement and this BAA, the BAA shall control. If Covered Entity determines it is necessary to amend this BAA from time to time to comply with the requirements of any HIPAA Rules or applicable state law, Covered Entity shall provide Business Associate with written notice of the amendment. If Business Associate disagrees with any such amendment proposed by Covered Entity, Business Associate must so notify Covered Entity in writing no later than fifteen (15) days after receipt of Covered Entity's notice of amendment, or the amendment will be deemed to be incorporated by reference into this BAA. If Business Associate provides Covered Entity with notice of disagreement within the fifteen (15) days, the parties shall negotiate in good faith to amend this BAA. If the parties are unable to agree on an amendment, Covered Entity may, at its option, terminate this BAA and the Service Agreement.

6. No Third Party Rights/Independent Contractors

The parties to this BAA do not intend to create any rights in any third parties, except as expressly set forth in subsection 2(l) of this BAA. The parties agree that they are independent contractors and not agents of each other, except nothing herein affects whether Business Associate is an "agent" for purposes of compliance with 42 C.F.R. §1001.952.

7. Notices

Any notice required or permitted by this BAA to be given or delivered shall be in writing and shall be deemed given or delivered if delivered in person, or delivered by courier or expedited delivery service, or delivered by registered or certified mail, postage prepaid, return receipt requested, to the address set forth below. Each party may change its address for purposes of this BAA by written notice to the other party. Notices must be directed to the signators to this BAA and pursuant to the Service Agreement notice provisions.

8. Severability

Whenever possible, each provision of this BAA shall be interpreted so as to be effective and valid under applicable law. If any provision of this BAA should be prohibited or found invalid under applicable law, such provision shall be ineffective to the extent of such prohibition or invalidity without invalidating the other of such provision or the remaining provisions of this BAA.

9. State Law

Business Associate acknowledges and agrees that it has implemented and will maintain appropriate privacy and security measures to protect personal information consistent with state laws and regulations to the extent those state laws and regulations are applicable to the Protected Health Information, and Business Associate must comply with any applicable laws that provide access, correction, deletion and/or portability rights to individuals, as appropriate. The obligations hereunder are independent of and do not limit or otherwise affect the parties' other obligations under this BAA.

10. Governing Law; Dispute Resolution

To the extent not preempted by federal law, the BAA shall be governed and construed in accordance with the state laws governing the Service Agreement, without regard to conflicts of law principles that would require application of the law of another state. Disputes shall be resolved as provided for in the Service Agreement, to the extent applicable.

11. Assignment, Binding Nature and Benefits

This BAA binds and benefits the parties, and their respective successors, and their permitted assigns. Business Associate may not assign or subcontract rights or obligations under this BAA without the express written consent of Covered Entity.

12. Injunction

Business Associate hereby recognizes that irreparable harm may result to Covered Entity, and to the business of Covered Entity, in the event of a breach by Business Associate of any of the covenants and assurances contained in this BAA. As such, in the event of a material breach of any material covenants and assurances contained herein, Covered Entity shall be entitled to seek an injunction to enjoin and restrain Business Associate from any continued violation of such covenants and assurances. Such right shall be in addition to the remedies otherwise available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a

remedy in damages will be adequate and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.

13. Legal Privileges

Nothing in this BAA is intended to or shall be deemed to constitute or require any waiver of any privilege or other legal protection (such as the attorney-client privilege, the work product doctrine and the quality assurance privilege) applicable to, relating to or arising out of (i) the relationship between Covered Entity and Business Associate, (ii) the Protected Health Information, or (iii) any summaries, analyses, reports and the like related thereto. The provisions of this section shall survive the termination or expiration of this BAA.

14. Counterparts

This BAA may be executed in multiple counterparts, which shall constitute a single agreement, and by facsimile, pdf or electronic signatures, which shall be treated as originals.

IN WITNESS WHEREOF, the parties, through their duly authorized representatives, have executed this BAA as of the Effective Date.

Covered Entity:

By: _____

Title: _____

Address: _____

Date: _____

Business Associate:

By: _____

Title: _____

Address: _____

Date: _____

Non-Disclosure and Confidentiality Agreement

This is a non-disclosure and confidentiality agreement between [Party A] and [Party B]. This agreement goes into effect on [Date of Agreement]. To perform regular operations [Party A] must handle confidential patient information on a day-to-day basis. Due to the relationship between [Party A] and [Party B], it is necessary to ensure that [Party B] maintains the confidentiality of the patient information handled by [Party A].

A. Definition of "Confidential Information"

- a. Confidential Information in this context will refer to "patient information"
- b. Patient information can include one or a combination of the following identifiers
 - Patient name
 - Address
 - Date of birth
 - Photograph
 - Fingerprints
 - Social security number
 - Driver's license number
 - Diagnosis/treatment information
 - Email address
 - Phone number
 - Any other unique patient identifier

B. Statement of Obligation

I understand that by working with, or encountering [Party A] puts me at a higher risk of being exposed to patient information. I understand that [Party A] holds patient information in the highest confidence. I will not in any way disclose, neither verbally, electronically or by any other means, patient information to any unauthorized party. I agree to abide by all of [Party A]'s policies and procedures that are in place to protect the confidentiality of patient information. I understand that if the terms of this agreement are violated, [punishment] may be levied against myself and my organization

Signature [Party A] _____

Signature [Party B] _____

Effective Date _____

HIPAA Security Policy #10

Physical Safeguards Facility Access Controls

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the procedures that will limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Policy

10 Facility Access Controls

TYPE: Standard

REFERENCE: 45 CFR 164.310(a)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

1. The Company shall create and maintain a Facility Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store ePHI against unauthorized physical access, tampering, or theft. The Facility Security Plan will include:
 - i. Contingency Operations Plans
 - ii. Facility Security Plans
 - iii. Access Control and Validation Plans
 - iv. Maintenance Records

10.1 Contingency Operations

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."

1. The Company will create procedures that ensure access to facilities by appropriate personnel during Disasters or Emergency Operations. These procedures will be incorporated into the respective Contingency Operations Plan (See HIPAA Security Policy#7 – Contingency Plan)

Procedure

1. The Company shall implement the following procedures to allow facility access in the event of an emergency, disaster, or other occurrence resulting in lost data:
 - i. The Company will take reasonable and appropriate steps to secure any location that contains PHI or ePHI. The Company workforce members will take reasonable and appropriate steps to continue to protect PHI and ePHI.
 - ii. The Company will permit access to all workforce members involved in the repair of electronic information systems and in the restoration of lost data in accordance with the Emergency Mode Operation Procedures and Disaster Recovery Procedures (see HIPAA Security Policy #7 -Contingency Plan)
 - iii. The Company Management and/or HIPAA Security Officer shall see that The Company' workforce members involved in Emergency Mode Operation Procedures and Disaster Recovery Procedures (see HIPAA Security Policy #7 -Contingency Plan) have access to rooms and areas containing any back-up data stored on-site or off-site.

10.2 Facility Security Plan

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

1. The Company will implement procedures to safeguard facilities and equipment from unauthorized physical access, tampering, and theft.

Procedure

1. The Company shall ensure that all network servers, application servers, routers, database systems, device management system hardware, and other servers are located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.
2. The Company will ensure that only appropriate and authorized personnel have access to facilities housing operations related systems.
3. Any other workforce members requiring access to facilities housing The Company operations-related electronic information systems shall request and receive permission from the HIPAA Security Officer.
 - i. Such access shall only be granted on a need-to-know basis.

- ii. The HIPAA Security Officer shall log the names of personnel who have requested and been granted access to the facilities containing The Company electronic information systems.

10.3 Access Control and Validation Procedures

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(iii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

1. The Company will take reasonable and appropriate steps to control and validate physical access to facilities containing ePHI Systems.

Procedure

1. The Company will implement the following procedures to control and validate a person's access to facilities based on their role or function:
 - i. Access to highly sensitive areas that contain ePHI will only be granted on a need to know basis and based on a legitimate business need.
 - ii. All access to areas that house systems that contain ePHI will be tracked and logged. Logs will contain at a minimum: person's name, company, date of entry, time of entry, duration and reason for entry.
 - iii. Guests of The Company should not be given access to areas that house systems that contain ePHI.
 - iv. Patients should only be permitted in common areas and should not be given access to areas that house systems that contain ePHI.

10.4 Maintenance Records

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(iv)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)."

1. The Company management will be responsible for overseeing that repairs and modifications to the physical components of the facility, which are related to security (for example, hardware, walls, doors and locks), are completed and logged. At a minimum, the log shall contain the following information:
 - i. The equipment or component where maintenance has been performed
 - ii. The date maintenance was performed
 - iii. A description of the maintenance performed

- iv. The Company's workforce member(s) or contractor who performed the maintenance.

Creation Date:

Effective Date:

Last Revision Date:

Date	Time	Name (Full)	Reason for Access	Additional Notes	Signature

Organization name: _____

Server room location: _____

Security Officer: _____

Signature of Security Officer for approval _____ Date: _____

Request for Access to the Secured Server Location

(Company name)

(company name) takes the privacy and security of Protected Health Information it possesses very seriously. By utilizing this form (company name) is attempting to limit the access to the secured server location to only those who are deemed necessary for access. If ongoing access is permitted, (company name) should record these permissions in Appendix A on the following page.

Name: _____

Job title: _____

Organization (if external): _____

Reasons for access: _____

Permissions Granted (one time access or ongoing access): _____

- ☐ I understand that the equipment held within the secured server location may contain highly sensitive information. By achieving permission to access this area I certify that I will protect the integrity and security of the information within.

Name (Printed): _____

Signature: _____

Date: _____

Security Officer Signature: _____

Appendix A: Current list of Individuals with Access to Secured Server location
(Company name)

[illegible]

Facility Maintenance Record

(company name)

(company name) management will be responsible for overseeing that repairs and modifications to the physical components of the facility, which are related to security (for example, hardware, walls, doors and locks), are completed and logged. The security officer will use this log to record when important maintenance is performed at the facility. All completed forms should be saved and retained.

Equipment serviced: _____

Date of maintenance: _____

Description of maintenance performed: _____

Name of individual performing maintenance: _____

Company name performing maintenance (if applicable): _____

Security Officer's Name: _____

Security Officer's Signature: _____

Date: _____

HIPAA Security Policy #11

Physical Safeguards Workstation Use

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to provide policies and specifications on workstation use that include documented instructions and procedures defining the proper functions to be performed and the manner in which those functions are to be performed in order to maximize the security of ePHI

Policy

11 Workstation Use

TYPE: Standard

REFERENCE: 45 CFR 164.310(b)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information."

1. To ensure that workstations and other computer systems that may be used to send, receive, store or access ePHI are only used in a secure and legitimate manner, all workforce members' must comply with The Company Computer Use Policy, a copy of which is attached as Exhibit A.
2. The Company may provide workstations and other computer systems to workforce members for the purpose of performing their job functions for The Company. Workforce members shall be responsible for using workstations appropriately in conformance with this Policy.
3. The Company may remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.
4. Workforce members must be assigned and use a unique User Identification and Password (See HIPAA Security Policy #14 - Access Control)
5. Workforce members that use The Company information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, The Company may log, review, or

monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.

Creation Date: (replace date)

Effective Date: (replace date)

Last Revision Date:

Appendix A

The Company Computer Use Policy

Introduction

This document provides guidelines for appropriate use of computer facilities and services at The Company. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide The Company's employees, and specific policy statements serve as a reference point. It will be modified as new questions and situations arise.

Computers, the Internet and electronic mail (e-mail) are powerful research, communication, commerce and time-saving tools that are made available to The Company employees. The use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and e-mail have the potential to be used for inappropriate purposes.

The Company will provide workstations and other computer systems to The Company employees for the purpose of performing their job functions for The Company. The Company employees shall be responsible for using workstations appropriately in conformance with this Policy.

Policy

The following policies on computer, the Internet and electronic mail usage shall be observed by all The Company employees.

- Users of the Internet and e-mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.
- Primary purpose of the Internet and e-mail is to conduct official business.
- Users should identify themselves properly when using the Internet and e-mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all The Company's employees.
- Each user is individually responsible for the content of any communication sent over or placed on the Internet and e-mail.
- All employees have a responsibility to ensure a respectful workplace. The Company equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.
- Exceptions to this policy are only allowed when pre-approved by the department head and deemed necessary for official The Company business, research or investigatory work.

The following actions are prohibited. It is unacceptable for The Company employees to:

- Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.

- Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.
- View or distribute obscene, pornographic, profane, or sexually oriented material.
- Violate laws, rules, and regulations prohibiting sexual harassment.
- Engage in any unauthorized activities for personal financial gain.
- Place advertisements for commercial enterprises, including but not limited to, goods, services or property.
- Download, disseminate, store or print materials including articles and software, in violation of copyright laws.
- Download any software, including but not limited to games, screen savers, toolbars or any other browsing tools without the permission of Information Services.
- Violate or infringe on the rights of others.
- Conduct business unauthorized by The Company.
- Restrict or inhibit other users from using the system or the efficiency of the computer systems.
- Cause congestion or disruption of networks or systems, including distribution of chain letters.
- Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.
- Use the system for any illegal purpose or contrary to The Company policy or business interests.
- Connect a personal computer to The Company network without having the computer checked by Information Services to ensure no threatening viruses / programs infect The Company network.
- Monitor or intercept the files or electronic communications of other employees or third parties.
- Hack or obtain access to systems or accounts they are not authorized to use.
- To disclose a Login ID(s) or password to anyone nor allow anyone to access any information system with someone else's Login ID(s) or passwords
- Use other people's Login ID(s) or passwords to access any information system for any reason.
- Will not post any patient information on social network sites, public forums, etc.
- Users shall not remove from The Company's facilities electronic media that contains Protected Health Information (PHI) or confidential or proprietary The Company information unless such removal is authorized by a user's supervisor and the user signs out the media in accordance with The Company HIPAA Security Device and Media Controls Policy.

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Any employee will immediately report to The Company Security Coordinator any activity that violates this agreement.

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of The Company computer and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that Internet and e-mail may be subject to monitoring. I am aware that violations of this guideline on appropriate use of the e-mail and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the e-mail and Internet may reflect on the image of The Company to our patients, competitors and suppliers and that I have responsibility to maintain a positive representation of The Company. Furthermore, I understand that this policy can be amended at any time.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. The Company may deny access to information systems if this Agreement is not returned signed and dated.

Signature

Date

Requestor's Immediate Supervisor Signature

Date

Access Agreement Approved by (printed name)

Date

Sanction Policy

Introduction

Client name has adopted this Sanction Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

Scope of Policy

This policy governs Workforce Sanctions and disciplinary actions for client name. All employees/workforce members of client name must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Policy Statement

- Client name must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).
- It is the Policy of client name to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established policies and procedures, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- It is the Policy of client name to fully document all workforce sanctions and their dispositions, according to HIPAA requirements.

Based on the severity of the violation, develop varying levels of disciplinary action such as:

- Verbal warning
- Written warning
- Education – training/retraining
- Removal of system privileges
- Suspension without pay
- Termination of employment

Procedures

- Inadvertent release of PHI will be investigated and the punishment will be determined by management and the extent of harm to individual involved.
- Accessing patient records in client name files that they do not have a reason to be in is a privacy violation that may result in immediate termination. At the very least, they will lose patient information access and be placed on written warning for 90 days.
- Blatant disregard for client name HIPAA Policies and Procedures may result in immediate termination.
- Intentional release of PHI to someone who does not meet criteria to access WILL result in immediate termination and possible prosecution.

Optional Signature Line

Name [Print]: _____

Signature: _____

(Use the same signature as in the Workstation Use Policy)

Creation Date:

Effective Date:

Last Revision Date:

Sanction Records

(company name)

This document should be completed by management to record the sanctions that were enforced for an employee who violated policies and procedures in accordance with the Sanction Policy set forth. This record shall be retained in the employee's file for the length of their employment with (company name).

Employee name: _____

Description of violation: _____

Is this the first violation for the employee?: _____

If no, please explain prior violation(s): _____

Describe the disciplinary action taken for the recent violation: _____

Security Officer name: _____

Security Officer Signature: _____

Date: _____

Remote Work Guidelines

Purpose

The purpose of this policy is to address vulnerabilities associated with staff working remotely. The goal of this policy is to provide a safe and functional work environment that will allow staff to work remotely. A focus of concern with remote work is staff-owned devices (laptops, PCs, smartphones, etc.) entering your network, as these devices may not have the same controls as company-owned devices, and if compromised, could infect your data network.

Scope

This policy covers all Company name's employees who have remote work capabilities.

Statement of Policy

Company name will implement, to the fullest extent possible, all necessary security controls to ensure staff can remotely work in a safe and functional environment.

Technology and procedure requirements for remote work

- Transmission security and integrity
 - Company name has ensured their firewall is capable of VPN traffic and that employees working remotely are provided with VPN licenses
 - Company name has tested Unified Communication strategy and technology necessary for remote work: VOIP phones, softphone technology that transfers to mobile phones from the office number, and employees' use of internal chat technology and video conferencing.
 - Data sharing through external cloud applications (OneDrive, etc.) is restricted to only company approved applications
 - Staff can securely exchange files and information externally and internally (*i.e., office-365 encryption option enabled, on-premises solution, etc.*)
 - Multifactor Authentication will be implemented for remote connectivity
 - Ensure remote connectivity sessions are set to expire after 4-8 hours
- Device and media controls for remote work
 - Devices used to connect remotely (laptops and PCs) will utilize encryption
 - These devices should not have admin privileges. If they do, then strong passwords must be used
 - Mobile Device Management software will be implemented on all devices
 - A Bring Your Own Device (BYOD) policy will be developed to define proper security for personal devices
 - Remote endpoint security tools that can be centrally reviewed and monitored for company and employee-owned devices will be reviewed and implemented

- Access to Sensitive Company Information, Personally Identifiable Information (PII), and electronic Protected Health Information (ePHI) will be restricted/limited when an employee is not using a secure workspace or device
- Incident Response procedures will include response to incidents originating from or affecting employees working remotely
- Remote workers will be trained on common social engineering and phishing scams

Controls for remote work environment

- Secure workspace
 - Remote work staff must have the ability to lock laptops, devices, and any business relevant information (i.e., paper documents) when not in use. Cable locks for laptops should be used when necessary. Laptops and devices should be locked out of sight and/or in the trunk if it must be left in a vehicle unattended. Any other business relevant information (i.e., paper documents with sensitive information) should be stored securely
 - Remote work staff should be aware of their environment and who is around them. Safely perform conversations without visitors eavesdropping or shoulder surfing. Use screen protectors when necessary
 - Restrict the use of devices containing business-relevant information. Employees will not let family members, friends, or anyone but themselves use company-owned devices or personal devices used for business purposes
- Remote network security
 - Wireless security
 - Always change default Wi-Fi Router passwords
 - Enable WPA-2 or higher encryption
 - Ensure your local router firmware is up to date
 - The use of public Wi-Fi should be limited. Always use a VPN when connecting to public Wi-Fi. Never use public Wi-Fi to send sensitive information without a VPN
 - Ensure all personal devices are secure with company-provided or personally owned antivirus and antimalware software
 - Update IOT Device firmware (smart thermostats, surveillance cameras, etc.)
 - Ensure default passwords are changed
 - Update software on all devices within your home network (Corporate laptop, IOT devices such as cameras and smart thermostats, personal laptops/tablets, etc.)
 - Review and follow corporate Bring Your Own Device (BYOD) and other relevant policies and procedures
- Remote Work Employee Awareness
 - Be extremely cautious of email phishing scams
 - Limit social media use

- Don't reveal business itineraries, corporate info, daily routines, etc.

Guidelines & Tips for Employees Working Remotely

Working remotely, whether short-term or permanent comes with many perks, but it also poses many new risks for the security of your organization's data. For example, if an employee-owned device (laptop, PC, etc.) is connected to the company's network and contains a virus or malware, they could be spread to your company's network. Additionally, it becomes more of a challenge to verify the legitimacy of emails (for example, you're no longer right down the hall from your CEO who requested an unusual wire transfer), you may be unfamiliar with policies and procedures as they pertain to a work from home environment, and the list goes on.

We've developed a list of guidelines and tips to assist you as you prepare to work from home in a safe, functional work environment. Note, this list is intended for guidance and information purposes only. If you have any questions regarding these tips, please reach out to your supervisor or IT provider for additional information.

Guidelines & Tips

- Secure workspace
 - Ensure you have the ability to lock your devices (laptop, PC, etc.) and any business relevant information when not in use. Cable locks for laptops should be used when necessary. Laptops and devices should be locked out of sight and/or in the trunk if it must be left in a vehicle unattended
 - Avoid using your personal devices for work-related business
 - Safely perform conversations without visitors eavesdropping or shoulder surfing, especially while working in a mobile setting, such as a coffee shop
 - Protect the data you are accessing by using a VPN to log into the company network, and ensure you are protecting data visible on your screen with a screen protector. This is especially critical for employees who are required to be HIPAA compliant, PCI compliant, etc.
 - Restrict the use of devices containing business-relevant information. Do not let family members, friends, or anyone but yourself use company-owned devices or personal devices used for business purposes
 - Use strong unique passwords on all your devices and accounts to prevent unauthorized access
- Wireless Security
 - Change default Wi-Fi Router passwords
 - Enable WPA-2 or higher encryption
 - Ensure your local router firmware is up to date
 - Limit the use of public Wi-Fi. Always use a VPN when connecting to public Wi-Fi. Never use public Wi-Fi to send sensitive information without a VPN
- Ensure all personal devices are secure with company-provided or personally owned antivirus and antimalware software company
- Updated IOT Device firmware (smart thermostats, surveillance cameras, etc.)
 - Ensure default passwords are changed
- Ensure the software on all devices within your home network is kept up to date (corporate laptop, IOT devices such as cameras and smart thermostats, personal laptops/tablets, etc.)

- Review and follow corporate Bring Your Own Device (BYOD) and other relevant policies and procedures

AWARENESS

- Remote Work Employee Awareness
 - Be extremely cautious of email phishing scams
 - Limit social media use
 - Don't reveal business itineraries, corporate info, daily routines, etc.

Guidelines & Tips for IT Providers

Transitioning Your Clients to a Remote Work from Home Environment

As an IT provider, we know that your clients rely on your assistance when transitioning to a remote, work from home environment. Whether that transition is short-term or permanent, remote working poses many new risks for the security of your client's data. Concerns that arise in a remote work environment include employee-owned devices (laptops, PCs, etc.) entering your client's network and spreading viruses or malware, employees not knowing how to use a VPN to access the network, employees letting their guard down when it comes to verifying the legitimacy of emails, and the list goes on. As their trusted security advisor, we strongly recommend assisting your clients in the development of remote work from home policies and procedures that will enforce strong guidelines to help protect their organization.

We've developed a list of guidelines and tips to assist you in ensuring your clients and their employees are prepared to work from home in a safe, functional work environment. Note, this list is intended for guidance and information purposes only.

Guidelines & Tips

- Ensure your client's firewall is capable of VPN traffic and ensure they have enough VPN licenses
- Test your client's Unified Communication strategy and technology: VOIP phones, softphone technology that transfers to mobile phones from your client's office number and your client's use of internal chat technology like Teams and Slack and video conferencing
- Enable encryption on your client's local devices (laptops and PCs)
- Local devices (laptops and PCs) should not have admin privileges. If they do, ensure strong passwords are required
- Limit your client's external sharing through Cloud applications (OneDrive, etc.)
- Enable a Mobile Device Management software on all your client's devices
- Ensure that any Bring Your Own Device (BYOD) personal devices meet your client's policy standards and include proper security and remote wipe capabilities
- Review and enable your client's remote endpoint security tools to ensure that they can be centrally reviewed and monitored for your client's company and employee-owned devices
- Provide your client with the ability to securely exchange files and information externally and internally (i.e., office-365 encryption option enabled, on-premises solution, etc.)
- Limit the access to Sensitive Company Information, Personally Identifiable Information (PII), and electronic Protected Health Information (ePHI) when your client's employee is not using a secure workspace or device
- Enable Multifactor Authentication for remote connectivity
- Ensure your client's remote connectivity sessions are set to expire after 4-8 hours
- Review Incident Response procedures with all relevant parties
- Educate your clients and their employees on common social engineering and phishing scams, including new scams relating to current events

Bring Your Own Device Policy Introduction

(company name) is an organization under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, the organization is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. This policy reflects the organization's commitment to complying with such Regulations and their commitment to safeguarding ePHI.

Purpose of Policy

The purpose of the policy is to develop the appropriate policies and procedures to protect ePHI on employee personally owned devices. Proper security controls are essential to safeguard the sensitive information that may be on these devices. Documented instructions and requirements should be provided to all employees that may be accessing ePHI on their personally owned devices and acknowledgement of acceptance should be documented and retained.

Policy

(company name) should be aware that they are responsible for any breaches of ePHI that resulted from unsecured employee personally owned devices.

Employees must be aware that breaches or inappropriate use of their devices that may put ePHI at risk may negatively affect patients, the organization and the employee themselves. The organization has the right to revoke an employee's access to ePHI or levy sanctions laid forth in the organization's sanction policy.

The organization must be aware that encryption is the only safe harbor under the HIPAA Security Rule and the strongest protection against a data breach. The organization should attempt to encrypt devices that access ePHI.

Employees are not permitted to access ePHI, on personally owned devices, unless authorized and approved. Only approved devices that are properly configured will be given access to PHI.

The organization will limit who has access to ePHI on their personally owned devices. In accordance with the HIPAA Security Rule, the organization will provide employees with only the limited amount of access to patient information to perform their job function.

The organization and their Information Technology (IT) group/provider will work together to manage and enforce this Bring Your Own Device (BYOD) policy.

Procedure

(company name) will communicate this policy to their employees. Employees must request permission to use personally owned devices and fill in the registration form provided.

The organization and IT will periodically review and update this policy when new requirements are implemented or when security requirements change. Employees must be notified of any changes and a document of their acceptance/acknowledgment should be collected.

The organization and IT reserve the right to monitor and inspect devices registered in its BYOD program to ensure that ePHI is being properly protected.

Upon an employee's termination of employment, (company name) and IT will ensure that any devices the employee has with ePHI are returned to IT for a final analysis and removal of any ePHI or applications that access ePHI. This will be conducted as soon as possible to limit inappropriate access to ePHI.

Documentation, acknowledgement and registration forms will be retained for all employees and kept in their employee folder. Documentation must also be provided to employees initially and upon request.

Appendix A

Bring Your Own Device Policy

This document provides the guidelines for a Bring Your Own Device (BYOD) policy for (company name). It offers principles to help guide employees and staff and can be modified by the organization to better reflect their specific needs.

The organization's employees have the ability to bring and utilize various personal devices that may have the ability to access, store or transmit electronic Protected Health Information (ePHI). Devices include but are not limited to smartphones, tablets and laptops. Employees must be aware that when accessing ePHI on their personally owned devices they must protect that information. The ability for employees to utilize personally owned devices at the office should be treated as a privilege and (company name) reserves the rights to revoke this privilege if an employee does not abide by the policies laid forth.

Devices Permitted

Smartphones accepted (brand and model): _____

Tablets accepted (brand and model): _____

Laptops: personally owned laptops must be accepted and approved by (company name) management.

Additional Devices: other additional personal devices that may access or store patient information must be approved by (company name) management and IT.

Specifically excluded devices: _____

Security Specifications

Mobile Device Management service:

Encryption service:

Anti-Malware/Anti-Virus service:

Minimum Operating System required (laptop):

Minimum Operating System required (smartphones):

Minimum Operating System required (tablets):

Secure texting application required:

System Inactivity timeout setting (minutes):

HIPAA compliant email provider:

Security Requirements

- All devices must be password protected.
- Passwords must be complex; requiring a minimum of 6 characters, a combination of upper- and lower-case letters, numbers and symbols.

- Devices must lock after five incorrect password attempts.
- Devices must “time out” and require a password after a five minute period of inactivity.
- Text messages that may contain ePHI must be sent through the secure texting application provided.
- Emails that are sent through the device containing ePHI must be sent encrypted.

Restrictions and Limitations

- “Rooted” or “Jailbroken” devices are not permitted to access ePHI.
- Employees must notify management when selling, trading in, recycling or disposing of their personal devices.
- The employee’s device may have data remotely deleted / wiped if 1) the device is lost or stolen, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and/or technology infrastructure.
- Devices that are lost or stolen must be reported to management and/or IT as soon as possible but within 24 hours.
- Employees must inform management and IT if they plan to upgrade, recycle or dispose of their personally owned device.
- Employees who voluntarily resign from the organization must present their device(s) to management and IT within 48 hours to have all ePHI and/or access to ePHI deleted / removed from the device.
 - Employees who do not turn over their device(s) to management and IT within 48 hours after voluntary resignation are subject to a full remote wipe / deletion of all data including non ePHI on their device.
- The organization will prepare for scheduled terminations in advance and ensure that employees present their device(s) to management and IT the day of the scheduled termination to have all ePHI and/or access to ePHI deleted / removed from the device. Terminated employees that do not present their device(s) will be given an opportunity to bring in their device(s) to have all ePHI removed from the device(s). Terminated employees that fail to bring in their device(s), after given the opportunity, are subject to a full remote wipe / deletion of all data including non ePHI on their device.

Additional Information

The organization will provide any additional specifications, requirements or restrictions in this section.

Sanctions

Violations or abuse of this policy are subject to the repercussions laid out in the organization’s sanction policy.

Creation Date:

Effective Date:

Last Revision Date:

Bring Your Own Device – Device Registration form

Employee name: _____

Position/title: _____

Phone number: _____ Secondary Phone number: _____

Device and Description: _____

Serial Number: _____ MAC Address: _____

Access points; where will patient information be accessed (email, text messages, applications, web etc.):

Device Security Specifications (for IT and/or (company name) management to complete):

Security Specification	Implemented (yes or no)	Details or additional information
Operating system		
Encryption		
Anti-virus service		
Secure Texting Application		
Timeout/lock settings		
Password requirements		
Web browser		
Mobile wipe		
E-mail provider		

Additional information, specific device restrictions and requirements should be detailed below:

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of personally owned devices that may access, store or transmit ePHI. I am aware that violations of this guideline of appropriate use may subject me to retraction of this privilege or disciplinary action, including termination of employment. I further understand that inappropriate use of my device that may put ePHI at risk may negatively affect patients, (company name) and myself.

I am aware of the technical restrictions and requirements on my device that were provided in the device registration form. I will maintain and manage these security requirements on my device for as long as I continue to access, store or transmit ePHI. I understand that (company name) reserves the right to protect their patients' information that I may be accessing and therefore have the ability to remotely wipe / delete data from my device if the need arises.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

Signature	Date
Requestor's Immediate Supervisor Signature	Date
Information Technology Provider's Signature	Date

Artificial Intelligence (AI) Acceptable Use Policy

[Company Name]

1) Purpose

This policy establishes acceptable and responsible use of Artificial Intelligence (AI) at [Company Name] ("Company"). Its goals are to: (a) protect confidential and regulated data; (b) reduce legal, security, and ethical risks; and (c) enable safe, high-impact AI adoption aligned with our business strategy.

2) Scope

This policy applies to all employees, contractors, interns, and third parties who access Company systems or process Company data. It covers:

- General-purpose AI assistants (e.g., enterprise chatbots)
- AI features embedded in SaaS products (e.g., Copilot/Gemini features)
- Company-built AI applications and automations
- Company Approved AI Services

3) Key Terms

Artificial Intelligence (AI): Systems that perform tasks requiring human-like cognition (e.g., generating text, images, code; predictions; classification).

Approved AI Service (AAS): Vendor or internal AI system formally approved by the AI Review Board and listed in the Approved AI Registry.

Confidential Data: Any non-public information classified Confidential or Restricted (e.g., client data, Company IP, personnel and financial data).

PII / PHI: Personally Identifiable Information / Protected Health Information as defined by applicable law (HIPAA, state privacy laws, etc.).

Model Training: Use of customer content to improve vendor models. (AAS must be configured so that customer content is not used for model training.)

AI Review Board (AIRB): A small cross-functional group (AI Program Owner as chair, Security/IT, Legal/Privacy, and a rotating Business Owner; optional Data/Engineering and Compliance) that approves AI tools and use cases, sets guardrails, maintains the Approved AI Registry, and oversees exceptions and incidents.

4) Roles & Responsibilities

- **AI Program Owner (APO) or Other Defined Owner.** Owns this policy, AI roadmap, Approved AI Registry, and adoption KPIs.

- **AI Review Board (Security, Legal, Privacy, Compliance, IT, Product):** Reviews AI vendors/use cases; sets guardrails; approves exceptions.
- **Managers:** Ensure team compliance; facilitate training; maintain use-case backlog.
- **Employees/Contractors:** Use AAS responsibly; follow data handling rules; complete required training.

5) Approved AI Registry

The **AI Program Owner** maintains a living registry of AAS including ownership, data residency, retention, model-training settings, and allowed use cases.

Example (replace with your systems):

Service	URL	Owner	Data Residency	Model Training on Customer Data	Retention	Allowed Uses
ChatGPT Team/Enterprise	https://chat.openai.com	IT/Sec	[Region]	Disabled by default	[X days/configurable]	Ideation, drafting, code assistance, summarization of non-public content only when policy conditions met
Microsoft 365 Copilot	Microsoft 365	IT	Tenant-bound	Not used to train foundation models	M365 policies	Work content within M365 per user permissions
Google Gemini for Workspace	workspace.google.com	IT	Tenant-bound	Not used to train models for other customers	Admin-controlled	Work content within Workspace per user permissions

6) Data Handling & Allowed Use Matrix

AI usage is permitted only via AAS and in line with the matrix below:

Data Type	Examples	Consumer/Unapproved AI	Approved AI Service (AAS)
Public	Published marketing copy, public docs	Allowed	Allowed

Internal	Non-public process docs, drafts	Not allowed	Allowed with review & minimal-necessary disclosure
Confidential	Client records, contracts, financials, engineering IP	Prohibited	Conditionally allowed only when all safeguards in §7 are met
Regulated	PII, PHI, payment data, export-controlled	Prohibited	Conditionally allowed only if the AAS is approved for the regulation in question (e.g., HIPAA, PCI), and §7 safeguards are met

Principles: Minimum necessary; redact or tokenize sensitive fields; avoid free-text pastes of large datasets; prefer system-to-system integrations with logging.

7) Mandatory Safeguards (AAS Only)

Before entering **Confidential** or **Regulated** data into an AAS, **all** of the following must be true:

1. **No model training on our data** (vendor setting and contract).
2. **Data retention is limited/disabled** per Company policy; administrators can configure or request deletion.
3. **SSO/MFA & tenant isolation** are enforced; data remains in our tenant/trust boundary.
4. **Access control:** AAS only accesses content users already have permission to view.
5. **Logging & auditability:** Prompts and outputs are logged in accordance with our retention schedule.
6. **Redaction/minimization:** Sensitive fields are removed, masked, or narrowed to the minimum necessary.
7. **Review & human oversight:** Outputs used externally or for decisions undergo fact-checking/peer review.
8. **Third-party GPTs, extensions, and plugins** are **disabled by default**; allow only vetted ones.
9. **Vendor risk** (security, privacy, compliance) is reviewed; data processing agreements are in place.

8) Acceptable & Prohibited Uses

Acceptable (examples):

- Ideation/brainstorming; editing and tone adjustments

- Drafting internal/external communications with review
- Code assistance; test generation; documentation
- Summaries of documents the user is authorized to access
- Generating non-production datasets (synthetic) for testing

Prohibited (examples):

- Uploading **Confidential/Regulated** data to any **unapproved** tool
- Bypassing access controls; attempting to exfiltrate data
- Using AI to discriminate, harass, or create deceptive content
- Relying on AI output without appropriate human review for accuracy and bias
- Entering secrets/credentials, encryption keys, or unpublished vulnerabilities

9) Prompt Hygiene & Quality

- **C — Context:** Where and in what context will this content be used (e.g., social post, newsletter, report)? Do you need a list, a paragraph, or bullet points? The more context you provide, the better the output. Avoid unnecessary sensitive details; use redaction/placeholders when possible.
- **H — Hone:** Specify and define the boundaries of the output you want. Do you need a quick answer or an in-depth analysis? What should the AI know (domain/role), what to include/exclude, required length/format, and whether you want plain language or technical phrasing. Add constraints, examples, and success criteria.
- **A — Audience:** Who are you targeting? Stating the audience helps tailor the language, depth, and examples to the reader.
- **T — Tone:** Should the output be formal, casual, or something in between? Are you aiming to inform, persuade, or entertain? Provide brand/voice cues if relevant.

After you get a draft: Verify facts and sources (hallucination check), review for bias, and **label** AI assisted content where required by this policy.

10) Third-Party & Embedded AI in SaaS

- Treat AI features inside SaaS apps as separate processors; ensure the vendor has equal or stronger safeguards than this policy.
- Coordinate with IT/Security before enabling new AI features or connecting data connectors.

11) Incident Handling

Report suspected AI-related incidents (data leakage, insecure outputs, harmful content) to Security within **24 hours**. Security will investigate, notify stakeholders, and coordinate containment and remediation.

12) Training & Certification

- **Required:** AI Safety & Responsible Use training (hallucination awareness & output verification; handling sensitive information (PII/PHI) with minimum necessary/redaction; using only approved enterprise AI tools and plugins).
- **Ongoing learning:** Short, recurring training on secure and effective AI use (e.g., weekly tips and training courses on effective use of approved AI tools).

13) Exceptions

Exceptions require **AI Review Board** approval with documented compensating controls and end date.

14) Enforcement

Violations may result in disciplinary action up to termination, and legal action where applicable.

15) Review and Revisions

This policy is reviewed annually or upon significant changes to regulatory requirements or technology infrastructure. Updates are communicated to all users.

Approved By: _____

Creation Date:
Effective Date:
Last Revision Date:

Appendix A – Operational Guardrails

1. **Labeling:** Mark AI-assisted content in drafts; remove label after human review/approval.
2. **Use-Case Registry:** Track approved use cases, owners, risks, KPIs, and outcomes.
3. **Data Minimization Checklist:**
 - Do I need this field?
 - Can I use an identifier/token instead of raw data?
 - Can I summarize before sharing?
4. **Review Checklist (for external use):**
 - Fact-check sources
 - Bias/fairness assessment
 - Legal/regulatory review if required
5. **Model/Plugin Controls:** Third-party GPTs/plugins disabled by default; enable only after risk review.

Appendix B – AI Acceptable Use Employee Acknowledgement

I have read, understand, and agree to comply with the [Company Name] **Artificial Intelligence (AI) Acceptable Use Policy** ("Policy"), including requirements to use only **Approved AI Services**, handle data consistent with **Section 6 (Data Handling & Allowed Use Matrix)**, implement the **Section 7 (Mandatory Safeguards)** when applicable, and follow **Section 8 (Acceptable & Prohibited Uses)** and **Section 9 (Prompt Hygiene & Quality)**. I also agree to complete required and ongoing training under **Section 12 (Training & Certification)**. I understand that prompts and outputs created in the course of my work may be logged and retained as Company records. I am aware that violations of this Policy may subject me to disciplinary action up to and including termination and, where applicable, legal action. By signing this Acknowledgement, I agree to comply with the Policy. Failure to read the Policy is not an excuse for violating it.

Name: _____ **Title:** _____

Signature: _____ **Date:** _____

HIPAA Security Policy #12

Physical Safeguards
Workstation Security

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained, and that access is restricted to authorized workforce members.

Policy

12 Workstation Security

TYPE: Standard

REFERENCE: 45 CFR 164.310(c)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

1. The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access ePHI.
 - i. Workstations and laptops that are in common areas that store or access ePHI should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords or ePHI.
 - ii. Workstations and laptops that are in common areas that store or access ePHI should utilize privacy screens to prevent unauthorized access to ePHI.
 - iii. Workstations and laptops that are in common areas that store or access ePHI should be secured by restraints such as locking cables.
 - iv. Portable devices and media including laptops, smartphones, CD-ROMs, DVDs, USB Drives, data backup tapes, etc. that contains ePHI should utilize encryption to protect the ePHI.
 - v. Portable devices and media should be concealed when from view when offsite to prevent theft.

- vi. All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel. (See HIPAA Security Policy#10 – Facility Access Controls).
 - vii. All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Workforce members must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Workforce members must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.
 - viii. All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
2. The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.
- i. Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.
 - ii. All facilities that store systems that contain ePHI, should have appropriate smoke and/or fire detection devices, sprinklers or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.
 - iii. All servers that contain ePHI, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.
 - iv. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.
3. A user identification and password authentication mechanism shall be implemented to control user access to the system. (See HIPAA Security Policy #14 - Access Control).
4. Workforce members suspecting any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the HIPAA Security Officer.

Creation Date:
Effective Date:
Last Revision Date:

HIPAA Security Policy #13

Physical Safeguards Device and Media Controls

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the policy and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility; and the movement ePHI within the facility; and to implement methods to properly dispose of ePHI.

Policy

13 Device and Media Controls

TYPE: Standard

REFERENCE: 45 CFR 164.310(d)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."

1. The Company will develop policies and procedures that govern receipt, removal, movement and disposal of hardware and electronic media containing ePHI within the facility. The policies and procedures will address device and media controls relating to:
 - i. Disposal
 - ii. Media Re-use
 - iii. Accountability
 - iv. Data Backup and Storage

13.1 Disposal

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 64.310(d)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

1. The Company must take reasonable and appropriate steps to dispose of portable devices and media that contain ePHI. Removal steps must ensure that ePHI is properly copied off of the device and that destruction of ePHI prevents unauthorized access to the ePHI.

Procedure

1. Prior to destroying or disposing of any portable device or media, care must be taken to ensure that the device or media does not contain ePHI.
2. If the portable device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.
3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI.
3. HIPAA Security Officer or delegate will notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.
4. HIPAA Security Officer or delegate will determine data sensitivity of data to be disposed of. (See Data Classification Table below)
5. IT will assess the condition of the equipment, they will:
 - a. IT will track the disposal of the device (type of hardware, serial number, etc).
See Appendix A: Media Disposal Log
 - b. IT will run approved wiping software on all devices to make sure all patient information is removed from the device. This may include physical destruction (See Methods of Destruction below)
 - c. IT will verify the hardware's data has been removed
 - d. IT will dispose of the hardware
6. HIPAA Security Officer or delegate / IT will document the destruction of the asset and keep a record. See Appendix C: Media Disposal Log
7. If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained

Data Classification Table:

1. **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
 - Basic operating system, personal files,
2. **Medium (Sensitive)** - Erase the data using any means such as reformatting or degaussing.
 - Business related information that does not contain patient information (ePHI).
3. **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)
 - Media contains patient information (ePHI).

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- X-Rays / Ultrasound / Diagnostic Machines
- Any other hardware that contains ePHI

Methods of Destruction Table:

Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. A data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI. Overwriting cannot be used for media that are damaged or not rewriteable.)
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. - Disintegration, Pulverization, Melting, and Incineration. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. - Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm).

13.2 Media Re-use

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 64.310(d)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

1. The Company must take reasonable and appropriate steps to ensure that portable device and media do not contain ePHI prior to re-use the device or media. If the device or media does contain ePHI then steps must be taken to ensure that the ePHI is properly destroyed prior to re-use of the device or media.

Procedure

1. Prior to making a portable device or media available for reuse, care must be taken to ensure that the device or media does not contain ePHI.
2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.
3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI
4. The use of a data destruction tool before reuse is not required if the media is used for system or data backup, as long as the media is stored and transported in a secured environment.

13.3 Accountability

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 64.310(d)(2)(iii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

1. When using portable devices or media to transport ePHI, a procedure must be developed to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

Procedure

1. A log should be maintained of any hardware containing ePHI that has been received into or removed from The Company's facilities. The log should note the workforce member receiving or removing the equipment, the date of receipt or removal, the person approving the receipt or removal, and the date the hardware was returned. (See Appendix A Receipt of Hardware or Electronic Media Containing ePHI Log and Appendix B Removal of Hardware or Electronic Media Containing ePHI Log).

13.4 Data Backup and Storage

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 64.310(d)(2)(iv)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

1. Before moving any systems that contain ePHI, a procedure must be developed to ensure that the ePHI is properly backed up and secured prior to moving.

Procedure

1. If a system contains ePHI, all files containing ePHI must be backed up to a computer, tape, USB drive, CD-ROM, disk, or other storage media before equipment is moved within or outside of The Company facilities.
2. The backed-up data should be stored in a secure area until it is placed on different equipment or restored to the original equipment from which it was removed.

Creation Date:

Effective Date:

Last Revision Date:

Appendix A Receipt of Hardware or Electronic Media Containing ePHI Log

[illegible]

Appendix B Removal of Hardware or Electronic Media Containing ePHI Log

[illegible]

Appendix C: Media Disposal Log

The below data was disposed / destroyed as required in **HIPAA Security Policy #13 – Device and Media Control**.

Date of Destruction:

Authorized By: [Click here to enter text.](#)

Description of Information Disposed of or Destroyed (include Manufacturer/Model/Serial Number/etc):

[Click here to enter text.](#)

Backup of Protected Health Information (PHI)? Required if PHI is the only copy.

☐ Yes

☐ No

If Yes, List Backup Location: [Click here to enter text.](#)

Method of Destruction:

☐ **Clear** (One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)

☐ **Purge** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.)

☐ **Destroy** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.)

Destruction Method Used:

[Click here to enter text.](#)

Final Disposition of Media:

- ☐ Disposed
- ☐ Reused Internally
- ☐ Reused Externally (sold / donated / etc.)
- ☐ Returned to Manufacturer / Leasing Company / Vendor / etc.
- ☐ Other: [Click here to enter text.](#)

Save this log and retain indefinitely.

Media Disposal Log

The below data was disposed / destroyed as required in **HIPAA Security Policy #13 – Device and Media Control**.

Date of Destruction: 1/1/2014

Authorized By: [Click here to enter text.](#)

Description of Information Disposed of or Destroyed (include Manufacturer/Model/Serial Number/etc):

[Click here to enter text.](#)

Backup of Protected Health Information (PHI)? Required if PHI is the only copy.

☐ Yes

☐ No

If Yes, List Backup Location: [Click here to enter text.](#)

Method of Destruction:

☐ **Clear** (One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)

☐ **Purge** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.

☐ **Destroy** (Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack.

Disintegration, Incineration, Pulverization, and Melting. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed.

Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning

Destruction Method Used:

[Click here to enter text.](#)

Final Disposition of Media:

- ☐ Disposed
- ☐ Reused Internally
- ☐ Reused Externally (sold / donated / etc.)
- ☐ Returned to Manufacturer / Leasing Company / Vendor / etc.
- ☐ Other: [Click here to enter text.](#)

Save this log and retain indefinitely. Upload to the HIPAA Portal Compliance Portal.

HIPAA Security Policy #14

Technical Safeguards Access Control

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to assure that systems containing ePHI are accessed only by those persons or software programs that have been granted access rights under the HIPAA Security Policy #4 – Information Access Management.

Policy

14 Access Control

TYPE: Standard

REFERENCE: 45 CFR 164.312(a)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

1. The Company must develop procedures to ensure that access to ePHI is only permitted to authorized persons. The procedures should include the following:
 - i. All workforce members must be assigned a unique user identifier (i.e. userid) that allows for workforce member identification and tracking of access to ePHI.
 - ii. Emergency access procedures that enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency.
 - iii. Automatic Logoff procedures that protect ePHI from unauthorized access while workforce members are utilizing systems that access ePHI.
 - iv. The use of encryption where it is reasonable and appropriate to protect ePHI.
2. All networks that contain systems that access or store ePHI should be protected by a network firewall.

14.1 Unique User Identification

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.312(a)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Assign a unique name and/or number for identifying and tracking user identity."

1. All workforce members must comply with the measures outlined in this policy to uniquely identify and track each workforce member that access systems and applications that contain ePHI.
2. Any workforce member that requires access to any system, or application that access, transmits, receives, or stores ePHI, must be provided with a unique user identification string. (See HIPAA Security Policy #3 -- Workforce Security and HIPAA Security Policy #4 -- Information Access Management).
3. The Company will develop password policies that specify creating, modifying and protecting of passwords.

Procedure

1. Workforce members will be assigned an unique user identification (i.e. userid) in order to access any system or application that transmits, receives or stores ePHI.
2. Each workforce member must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.
3. If a workforce member believes their user identification has been comprised, they must report the security incident. (See HIPAA Security Policy #6-- Incident Response).
4. Workforce members should be aware of the following password procedures to create and use strong passwords to protect ePHI:
 - i. Should be a minimum of eight characters in length.
 - ii. Should incorporate both upper and lower case letters (e.g. a-z and A-Z)
 - iii. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # \$ % ^ & * () _ - + = { } [] : ; " ' | \ / ? < > , . ~ `)
 - i. Should not be words found in a Dictionary.
 - ii. Should not include easily guessed information such as personal information, names, pets, birth dates, etc.
5. Workforce members should be aware of the following procedures to protect passwords:
 - i. Passwords should not be written down
 - ii. Passwords should not be shared with other workforce members
 - iii. If a workforce member suspects that their passwords has been compromised they should report the incident immediately
6. Passwords should be changed at least every 90 days
7. After a number of failed password attempts, the workforce member's account should be disabled (e.g. 3 or 5 failed attempts)

14.2 Emergency Access Procedure

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.312(a)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish procedures for obtaining necessary electronic protected health information during an emergency."

1. The Company will take reasonable and appropriate steps to define procedures to enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency.

Procedure

1. The Company will ensure that the Disaster Recovery and Emergency Operations plans include steps to enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency. (See HIPAA Security Policy#7 – Contingency Planning)
2. The Company will train workforce members on the Disaster Recovery and Emergency Operations Plan (See HIPAA Security Policy#7 – Contingency Planning)

14.3 Automatic Logoff

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(a)(2)(iii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

1. When feasible, electronic sessions will be terminated and workforce members will be logged out of systems accessing or containing ePHI after a number of minutes (e.g., 5, 10 or 15 minutes), requiring the workforce member to be identified and authenticated again in order to regain access and continue the session.

Procedure

1. Systems that access or store ePHI should implement an automatic logoff after a determined period of inactivity. Workforce members would need to be identified and authenticated again to regain access and continue the session.
2. Workforce members should be trained that when leaving a server, workstation, or other computer system un-attended, they must lock or activate the system's automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.

14.4 Encryption and Decryption

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(a)(2)(iv)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement a mechanism to encrypt and decrypt electronic protected health information."

1. The Company should implement encryption mechanisms where it is reasonable and appropriate to protect and safeguard ePHI.
2. Encryption should be used on all portable devices and media to encrypt ensure ePHI is protected in the event the device or media is lost or stolen.

Procedure

1. Workforce members should be trained on the use of encryption to protect ePHI.
2. All portable devices and media that contain ePHI should be encrypted to protect ePHI in the event that they are lost or stolen.
3. All backup tapes and media that contain ePHI should utilize encryption to protect ePHI.
4. The Company should implement secure encrypted remote access procedures to protect systems that access or store ePHI
 - i. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing ePHI. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix client access.
5. The Company should implement secure encrypted wireless access procedures to protect systems that access or store ePHI.
 - i. All wireless access to The Company's networks should utilize encryption mechanisms.
 - ii. All encryption mechanisms implemented to comply with this policy should support a minimum of 128-bit encryption.

Creation Date:

Effective Date:

Last Revision Date:

HIPAA Security Policy #15

Technical Safeguards Audit Controls Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the hardware, software and/or procedural mechanisms that will be implemented by The Company to record and examine activity in information systems that contain or use ePHI.

Policy

15 Audit Controls

TYPE: Standard

REFERENCE: 45 CFR 164.312(b)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

1. The Company should implement, where reasonable and appropriate, audit mechanisms to track and audit access to systems that contain or use ePHI.
 - i. Each system(s) containing ePHI shall utilize a mechanism to log and store system activity.
 - ii. Each system's audit log shall include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
 - iii. System audit logs shall be reviewed on a regular basis. (See HIPAA Security Policy #1 – Security Management).
 - iv. Security incidents such as activity exceptions and unauthorized access attempts should be detected, logged and reported immediately to the appropriate systems management and the HIPAA Security Officer in accordance with the HIPAA Security Policy #6 - Security Incident Procedures.

Creation Date:

Effective Date:

Last Revision Date:

HIPAA Security Policy #16

Technical Safeguards Integrity Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the appropriate data authentication measures that The Company shall implement to ensure that ePHI is not improperly altered or destroyed.

Policy

16 Integrity

TYPE: Standard

REFERENCE: 45 CFR 164.312(c)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

1. The Company will implement procedures to ensure that ePHI is not improperly altered or destroyed.

Procedure

1. The Company will implement mechanisms to protect ePHI from alteration or destruction by Malicious Software such as a virus or malware. (See HIPAA Policy#12 – Workstation Security).
2. The Company will implement mechanisms to protect ePHI integrity during storage and use, including the use of data redundancy (i.e. Redundant Arrays of Inexpensive Disks [RAID] configurations) and error-correcting memory

16.1 Mechanism to Authenticate ePHI

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(c)(2)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

1. The Company must implement mechanisms to validate that ePHI has not been altered or destroyed in an unauthorized manner.

Procedure

1. The Company will take steps to ensure that, when reasonable and appropriate, electronic mechanisms are implemented to validate the integrity of ePHI by proving that it has not been improperly altered or destroyed. Examples of electronic mechanisms that are capable of detecting and reporting unauthorized alteration or destruction of EPHI include:
 - i. Checksum
 - ii. Hash values
 - iii. Digital signatures
 - iv. Encryption
 - v. Disk redundancy (such as Redundant Arrays of Inexpensive Disks or "RAID").
2. The use of electronic mechanisms to ensure that ePHI has not been altered or destroyed will be determined by the HIPAA Security Officer

Creation Date:

Effective Date:

Last Revision Date:

HIPAA Security Policy #17
Technical Safeguards
Person or Entity Authentication Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the procedures to be implemented by The Company to verify that a person or entity seeking access to ePHI is the person or entity claimed.

Policy

17 Person or Entity Authentication

TYPE: Standard

REFERENCE: 45 CFR 164.312(d)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

1. The Company will implement authentication mechanisms to ensure the authenticity of a person or entity prior to granting access to ePHI.

Procedure

1. All workforce members of The Company are provided a unique username and password for all systems containing ePHI. (See the HIPAA Security Policy #14 - Access Control Policy).
2. Workforce members will select a password in accordance to the HIPAA Security Policy #14 - Access Control Policy.
3. Workforce members of The Company must not use another person's account to access any system. If a workforce member requires access to a system, they must gain access using an account in their own name. If new or additional access to a system is required, the procedures outlined in HIPAA Security Policy #4 - Information Access Management must be followed.
4. If a workforce member becomes aware that someone has improperly obtained his or her username and password or has improperly accessed The Company's electronic system through the use of the username and password, the workforce member shall immediately report the incident (See HIPAA Security Policy#6 – Security Incident Procedures).

Creation Date:
Effective Date:
Last Revision Date:

HIPAA Security Policy #18

Technical Safeguards Transmission Security Policy

Statement of Policy

The Company is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect The Company's commitment to complying with such Regulations.

Purpose of Policy

The purpose of the policy is to define the technical security measures that The Company will implement to guard against unauthorized access to or modification of ePHI that is being transmitted over an electronic communications network or via any form of removable media.

Policy

18 Transmission Security Policy

TYPE: Standard

REFERENCE: 45 CFR 164.312(e)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

1. The Company will implement procedures to reasonable protect ePHI against unauthorized access while being transmitted over an electronic communications network. Measures to protect ePHI include:
 - i. Implementing Integrity Controls
 - ii. Data Encryption

18.1 Integrity Controls

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(e)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

1. The Company will implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Procedure

1. The use of Secure Sockets Layer (SSL) should be utilized when accessing or transmitting ePHI to or from any website.
2. Transmission of ePHI via other methods should use secure and encrypted mechanisms to safeguard and protect ePHI.

18.2 Encryption

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(e)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement a mechanism to encrypt protected health information whenever deemed appropriate."

1. The Company will implement and utilize data encryption where it is reasonable to protect and safeguard ePHI. Encryption should be utilized when:
 - i. Transmitting ePHI to outside entities
 - ii. Stored on Portable Devices and Media
 - iii. Sent via Email or messaging systems
 - iv. Sent over wireless networks

Procedure

1. The Company will utilize encryption to protect and safeguard ePHI when sending to entities that are outside of The Company's network. The file, document, or folder containing ePHI should be encrypted before transmission.
2. The Company should utilize encryption when transmitting ePHI on Portable Devices or Media. Portable Devices and Media include but are not limited to Laptops, Tablets, USB Drives, CD-ROMs, DVDs, Floppy Drives and (Backup) Tapes.
3. The Company will utilize encryption when send ePHI via email or messaging systems.
 - i. The Company should not send ePHI via email or messaging systems if encryption has not been implemented.
4. The Company will utilize secure encrypted wireless networks to transmit ePHI.
 - i. The Company's workforce members should not access ePHI when using public non-encrypted wireless networks.

Creation Date:

Effective Date:

Last Revision Date:

(company name) HIPAA Privacy Manual

Table of Contents

Section 1 – Introduction	3
Section 2 – Definitions.....	4
Section 3 – Administration / Workforce Policies and Procedures.....	6
A. HIPAA Privacy Officer	6
B. Training of Workforce Members.....	7
C. Workforce Sanctions	8
D. Patient Complaints	9
E. Privacy Violations	9
F. Suspected Privacy Breach Reporting.....	10
G. Privacy Breach Determination	10
Section 4 – Disclosure of PHI without a Patient’s Authorization.....	11
A. Use and Disclosures to the individual	11
B. Use and Disclosures to Parents and Other Authorized Representatives.....	11
C. Use and Disclosures for Treatment, Payment and Health Care Operations.....	11
D. Use and Disclosure to Business Associates	12
E. Public Health Activities.....	12
F. Victims of Abuse, Neglect or Domestic Violence	13
G. Health Oversight Activities.....	14
H. Judicial and Administrative Proceedings.....	14
I. Law Enforcement	14
J. Decedents.....	16
K. Organ, Eye or Tissue Donation	16
L. To Avert a Serious Threat to Health or Safety.....	16
M. Specialized Government Functions.....	17
N. Workers Compensation.....	17
O. De-Identified Information	18
P. Limited Data Set	18
Section 5 – Special Circumstances	20
A. Marketing	20
B. Fundraising	20
C. Research	21

Section 6 – Disclosure of PHI Requiring an Opportunity to Agree or Object	22
A. Family Members and Close Friends	22
B. Disaster Relief Purposes.....	22
Section 7 – Use and Disclosures Requiring Authorization	23
A. General Rule	23
B. Psychotherapy Notes	23
C. Patient Authorizations	24
Section 8 – Minimize Use and Disclosure of PHI	26
A. Minimum Necessary Standard	26
B. Incidental Use and Disclosures.....	27
C. Verification	27
Section 9 – Patient Rights.....	30
A. Right to Notice.....	30
B. Right to Request Restrictions	31
C. Right to Confidential Communications	32
D. Right to Access PHI	33
E. Right to Amend PHI.....	37
F. Right to an Accounting of Disclosures of PHI.....	39
Appendix A: Acknowledgement of Receipt of Notice of Privacy Practices	43
Appendix B: Request for Amendment of Addition to Protected Health Information	45
Appendix C: Patient Authorization to Release Health Information	47
Appendix D: Patient Complaint Form	50
Appendix E: Request for Accounting of Disclosures Form	53
Appendix F: Accounting of Disclosures Log	55
Appendix G: Restriction of Protected Health Information Request Form.....	57
Appendix H: Request for Confidential Communications	59

Section 1 – Introduction

Statement of Policy

(company name) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Regulations. As such, (company name) is required to safeguard protected health information (PHI) in accordance with the HIPAA Privacy Rule Regulations. These policies and associated procedures reflect (company name)'s commitment to complying with such Regulations.

In instances where state law and federal law differ in governing the privacy of individually identifiable health information, the law that provides the greater privacy for the individual shall be followed.

Section 2 – Definitions

Authorization - an individual allows for the use and disclosure of Protected Health Information (PHI) for purposes other than treatment, payment, health care operations or uses and disclosures permitted or required by the HIPAA Privacy Rule.

Business Associate - a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to a Covered Entity.

- A Business Associate is not a member of a Covered Entity's workforce
- Business Associate functions include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
- Business Associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.
- Examples of Business Associates includes lawyers, auditors, consultants, contractors, clearinghouses, third-party administrators, and life insurance issuers.
- Subcontractors of Business Associates are considered Business Associates

Covered Entity – include:

- A health plan (includes insurance companies (such as Aetna, Blue Cross Blue Shield), Medicare, Medicaid
- A health care clearinghouse
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA

Designated Record Set - A group of records maintained by or for a covered entity that includes:

- Medical or billing records about individuals maintained by or for covered health care providers;
- Enrollment, payment, claims adjudication and case or medical management records systems maintained by or for a health plan; or
- Use by or for a Covered Entity to make decisions about individuals

Disclosure - means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Health Care Operations - includes, medical staff, risk or quality improvement management, or members of the quality improvement team who assess the care and outcomes of individual cases

Health Care Provider - a provider of health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

HIPAA - the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations found in 45 CFR Parts 160, 162 and 164.

HIPAA Omnibus Rule - a set of final regulations, published January 25, 2013, modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement various provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

HITECH - the Health Information Technology for Economic and Clinical Act of 2009 and its implementing regulations, found in 45 CFR Parts 160, 162 and 164.

Individually Identifiable Health Information - health information collected from an individual that is created or received by a health care provider, a health plan, a health care clearing house or an employer and that does all of the following:

- Involves the past, present, or future physical or mental health, or condition of an individual; the providing of health care to an individual; or the past, present or future payment for the providing of health care to an individual; and
- Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Minimum Necessary Standard - reasonable efforts are made to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Payment - includes activities undertaken by a Covered Entity to obtain or provide reimbursement for the provision of health care.

Privacy officer - the individual designated by an organization to develop and implement privacy policies and procedures for the organization.

Protected Health Information (PHI) - individually identifiable health information maintained or transmitted by a Covered Entity in any form or medium, including information transmitted orally, or in written or electronic form.

Treatment - includes the use and disclosure of PHI to provide, coordinate, or manage health care and related services of a patient. This also may include the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use - the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.

Workforce – employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Section 3 – Administration / Workforce Policies and Procedures

- A. HIPAA Privacy Officer – (company name)** will designate an individual to be responsible for HIPAA privacy compliance. This individual will be the HIPAA Privacy Officer and will be responsible for:

I. Privacy Policies and Procedures

The HIPAA Privacy Officer is responsible for developing and implementing written policies and procedures consistent with and meeting the requirements of The HIPAA Privacy Rule, and updating and revising as necessary.

II. Workforce Member Training

The HIPAA Privacy Officer is responsible for ensuring workforce members receive initial and on-going HIPAA privacy training;

III. Data Safeguards

The HIPAA Privacy Officer is responsible for maintaining appropriate physical and administrative safeguards to protect patient information in any format from misuse, whether accidental or intentional. Examples of such practices are providing areas for secure/private conversations, shredding of documents, proper filing and maintenance of records and limiting access to PHI procedures.

IV. Monitoring

The HIPAA Privacy Officer is responsible for monitoring use and disclosures of PHI and assisting workforce members with determining appropriate use and disclosures of PHI.

V. Investigating Privacy Concerns

The HIPAA Privacy Officer is responsible for investigating HIPAA privacy concerns and complaints. The HIPAA Privacy Officer is responsible for implementing clear processes for handling complaints, both from patients and workforce members, concerning privacy policy and practices.

VI. Breach Assessment and Notification

The HIPAA Privacy Officer is responsible for developing and implanting policies and procedures for potential and actual violations of PHI by workforce members or business associates constituting a breach as defined by law.

VII. Mitigation of Harmful Effects

The HIPAA Privacy Officer shall be responsible for mitigation of any harmful effects that may occur in regards to the use and disclosure for PHI, when a violation of the (company name)'s policies or the Privacy Rule has been detected. (company name) must have and apply sanctions for workforce members who fail to comply with (company Name)'s privacy policies and procedures.

VIII. Documentation and Record Retention

The HIPAA Privacy Officer shall be responsible for the accurate maintenance of all documents related to privacy policies and procedures, revisions, workforce training, complains, breaches, risk assessments, sanctions, etc. in accordance with the law. All documentation will be kept for a minimum of six (6) years.

(company name)'s HIPAA Privacy Officer is: _____

B. Training of Workforce Members

(company name) will ensure that all workforce members receive HIPAA privacy training on how to use, disclose and protect PHI. Workforce members should be trained on (company name)'s policies and procedures and receive appropriate training for workforce members to carry out their respective job duties. All workforce members must be aware of the proper methods necessary for handling PHI. Workforce members must also be trained on proper procedures concerning any problems or breaches should they arise. Training must be ongoing and include changes in policy as they occur.

I. Standardization of Training

The HIPAA Privacy Officer and the HIPAA Security Officer are responsible for developing or approving appropriate training materials. All workforce members must receive initial HIPAA privacy and security training.

II. Timing of Training

Workforce members must receive on-going HIPAA privacy and security, at least annually. New workforce members must receive HIPAA privacy and security training within thirty (30) days of hiring. Annual training must be completed within thirty (30) days of notification from HIPAA Privacy or Security Officer.

III. Level of Training

The training may be customized according to the type of work required by the individual, and the level of access they require to fulfill their duties.

IV. Methods of Training

Methods of delivering HIPAA Privacy or Security training may include: live presentations, videos, seminars, web-based training, emails, memorandums, newsletters or any other method that has been approved.

V. Documentation

Written documents of all HIPAA Privacy and Security training requirements and assessments shall be maintained for proof of compliance. All documentation will be kept for a minimum of six (6) years.

C. Workforce Sanctions

I. Enforcement

All workforce members are expected to adhere to (company name)'s HIPAA Privacy and Security policies and procedures. Workforce members that violate the policies and procedures may receive sanctions that include but are not limited to:

1. Verbal counselling;
2. Written warning that is placed in a workforce member's personnel file;
3. Placement on probation;
4. Retraining on HIPAA Privacy and/or Security policies and procedures;
5. Suspension;
6. Demotion or reassignment of duties;
7. Transfer or;
8. Termination of employment;
9. In addition to the above sanctions, workforce members may receive penalties for the misuse of PHI that could include criminal penalties as defined by HIPAA regulations. Civil damages may also be pursued; and
10. Sanctions should be applied consistently and equally. Sanctions should not be based on the individual or position of a workforce member.

II. Documentation

All sanctions and/or disciplinary actions against workforce members will be documented and retained for at least six (6) years. Documentation will include:

1. Workforce member's name and contact information;
2. A description of the violation that occurred;
3. The date of the violation; and
4. A description of the sanction against the workforce member

D. Patient Complaints

(company name) is committed to protecting the privacy of its patients. All patient privacy complaints will be taken seriously and investigated. The following procedure will be used to allow for reporting, investigation and response to all patient privacy complaints.

I. Reporting of Patient Complaints

1. All patients will be informed, through the Notice of Privacy Practices, of their right to make complaints regarding the privacy of their information.
2. All patient complaints must be submitted in writing to the HIPAA Privacy Officer or designate. The form, or similar form, in **Appendix D – Patient Compliant Form** will be used to document all patient complaints.
3. All patient complaints will be reviewed by the HIPAA Privacy Officer. The HIPAA Privacy Officer will investigate the complaint and utilize the **HIPAA Breach Determination procedure found in HIPAA Security Policy #6 – Incident Response**.
4. The HIPAA Privacy Officer will inform the patient, in writing, within 15 days of the outcome of the investigation. If the investigation results in a determination that the patient's privacy was breached the patient will be informed of measures that were taken to address or resolve the breach. All documentation of the patient complaint, investigation and determination and response will be kept for six (6) years.
5. If the patient wishes to file a complaint with the Office of Civil Rights (OCR), the patient will be directed to the OCR website which details the process for filing complaints. The OCR website is:
<http://www.hhs.gov/ocr/privacy/hipaa/complaints/>

II. Non-Retaliation Policy

All patients who file complaints will be treated fairly and without bias. Workforce members will not retaliate against any patient that files a privacy complaint.

E. Privacy Violations

All suspected patient privacy violations that are either reported by patients, workforce members or any other method will be taken seriously and investigated. All suspected patient privacy violations will utilize the HIPAA Breach Determination procedure found in **HIPAA Security Policy #6 – Incident Response**.

F. Suspected Privacy Breach Reporting

(company name) is committed to protecting patient privacy. Workforce members have a responsibility to promptly report any actions that are suspected to be a breach of a patient's privacy or are suspected to violate (company name)'s HIPAA Privacy and Security policies and procedures.

I. Reporting

Workforce members are required to report any suspected privacy breaches to either their direct superior or to the HIPAA Privacy Officer. If reported to a workforce member's superior, the superior will document the information and report it to the HIPAA Privacy Officer.

II. Non-Retaliation Policy

(company name) will not retaliate against any workforce member who, in good faith, reports a privacy violation or who assists in an authorized investigation of alleged privacy violations. Self-reported violations may still be subject to sanctions as documented in **Section 3 –C Workforce Sanctions**.

G. Privacy Breach Determination

The HIPAA Privacy Officer will investigate all reported privacy breaches. All suspected breaches of a patient's privacy and/or of (company name)'s policies and procedures should be taken seriously. Procedures documented in the **HIPAA Breach Determination procedure found in HIPAA Security Policy #6 – Incident Response** will be used to determine all suspected HIPAA privacy and security breaches.

Section 4 – Disclosure of PHI without a Patient’s Authorization

The purpose of this policy to provide clear guidelines for disclosure and use of protected health information (PHI) for medical evaluation, treatment and health services as well as related business services associated with this care. This is to include all workforce members involved in patient care or contracted by **(company name)** to provide services related to that care. These guidelines are put in place to ensure that the patient's information is kept private and in compliance with the minimum necessary standard.

(company name) workforce members may use and disclosure PHI without a patient’s authorization as follows:

A. Use and Disclosures to the individual

(company name) may use and disclose PHI to the patient requesting care and treatment.

B. Use and Disclosures to Parents and Other Authorized Representatives

I. Legally Authorized Representatives

There may be instances when a patient is legally or otherwise incapable of exercising their own rights or choses to designate another to act on their behalf. (company name) may disclose PHI to a Legally Authorized Representative and will treat the Legally Authorized Representative the same as the patient with respect to these policies and procedures.

II. Minor

If under state or federal law, a parent, guardian or other person acting in loco parentis (temporary custodian, foster parent, etc.) of an unemancipated minor who has authority to act on behalf of the minor in decisions regarding health care, (company name) will treat that person the same as the patient with respect to these policies and procedures.

III. State Law

If State law allows an unemancipated minor to consent to obtain health care without parental consent, (company name) will not treat the parent, guardian or other person acting in loco parentis the same as the patient with respect to these policies and procedures.

C. Use and Disclosures for Treatment, Payment and Health Care Operations

(company name) may use and disclose PHI without a patient’s authorization as follows:

I. Disclose to workforce

(company name) is permitted to use and disclose PHI to workforce members for purpose of treatment, payment and operations

II. Disclose to other providers

(company name) has permission to gather and use PHI in order to provide medical services requested from the patient. This permission includes but is not limited to coordination and management of care and the ability to share this information with other covered entities and providers involved with providing care to the patient.

III. Disclose for payment

(company name) is permitted to use or disclose PHI to process and obtain payment for services received and/or predetermination of prior approval of treatment recommendations. This includes such entities as other covered entities, insurance companies and their business associates and their subcontractors, and/or any third party payer for the services provided to the patient. This also includes collection processes, utilization review, and certain specific disclosures to consumer reporting agencies.

IV. Disclose for operations

(company name) is permitted to use or disclose PHI for health care operations, to another covered entity if the entity either has or had a relationship with the individual who is the subject of the information. Health care operations include but are not limited to the following: risk assessments, quality assurance and improvement activities, customer service, training and credentialing, accreditation, medical review and audits functions, legal services, and business planning, development and administration. PHI may be disclosed for administrative functions such as patient appointment reminders, office sign in sheets and calling patient names upon arrival.

D. Use and Disclosure to Business Associates

(company name) is permitted to disclose PHI to Business Associates (BA) subject to a signed Business Associate Agreement (BAA). See **HIPAA Security Policy #9 Administrative Safeguards Business Associate Contracts**.

E. Public Health Activities

(company name) may disclose PHI for the purpose of public health reporting:

- I. To a public health authority authorized by law to receive reports for the purpose of controlling or preventing disease, injury or disability (e.g., reporting of communicable diseases, births, deaths, etc.);
- II. A public health authority or other appropriate government authority authorized to receive reports regarding suspected child abuse or neglect;
- III. To the Food and Drug Administration (FDA) or persons subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

1. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
 2. To track FDA related products;
 3. To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or
 4. To conduct post marketing surveillance;
- IV.** A person who may have been exposed to a communicable disease or who may be at risk of contracting a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

F. Victims of Abuse, Neglect or Domestic Violence

(company name) will disclose PHI to a law enforcement official about a patient who is believed to be the victim abuse or neglect. Decisions to report are based on the professional judgment of (company name) workforce members after treating or seeing where;

- I.** The disclosure is required by federal or state law;
- II.** The patient agrees to the disclosure;
- III.** The disclosure is allowed by state or federal law and:
 1. (company name) workforce members believe the disclosure is necessary to prevent serious harm to the patient or other potential victims or;
 2. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- IV.** The minimum amount of PHI shall be released to support the allegation of abuse or neglect.

(company name) must promptly inform the patient that a report has been or will be made unless in the professional judgment it is believed:

- I.** Informing the patient would place the patient at risk of serious harm; or
- II.** The person being informed would be a personal representative who is responsible for the abuse, neglect or other injury and informing that person would not be in the best interest of the patient.

G. Health Oversight Activities

(company name) may disclose PHI as required to health oversight agencies (such as to the U.S. Department of Health and Human Services or as otherwise required by local, state or federal laws or regulations) for the audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions.

H. Judicial and Administrative Proceedings

(company name) may disclose PHI in relation to a judicial or administrative proceeding when:

- I. Ordered to do so by a court of law; or
- II. Upon receipt of a subpoena, discovery request, judicial order, warrant, summons, grand jury subpoena, or such other document requesting or ordering the disclosure of PHI for use in a judicial or administrative proceeding and/or law enforcement purposes.

(company name) should seek legal advice on how to respond to these orders and/or requests for PHI in accordance with applicable law and to ensure that satisfactory assurance are received as required by the HIPAA Privacy Rule 45 CFR Part 164.512(e).

I. Law Enforcement

(company name) may disclose PHI for the purpose of law enforcement to a law enforcement official in the following situations:

- I. When required by law including:
 1. Federal or state law requiring the reporting of certain types of wounds or injuries (e.g. gunshot wounds)
 2. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
 3. A grand jury subpoena; or
 4. Upon receipt of an administrative subpoena, summons or investigative demand.
- II. For identification of suspects, fugitives or witnesses

Other than the disclosures above, (company name) may disclose only the following limited patient health information to law enforcement officials in response to their request made for purposes of identifying or locating a suspect, fugitive, material witness or missing person:

- 1) Name and address

- 2) Date and place of birth
- 3) Social Security number
- 4) ABO blood type and rh factor
- 5) Type of injury
- 6) Date and time of treatment
- 7) Date and time of death, if applicable
- 8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

III. Patients who are crime victims

(company name) may disclose PHI to a law enforcement official about a patient who is the victim of a crime if:

1. The patient agrees to the disclosure; or
2. (company name) is unable to obtain the patient's agreement due to his/her incapacity and:
 - i. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
 - ii. That immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - iii. The disclosure is in the patient's best interest as determined by (company name)'s professional judgment.

IV. Decedents

(company name) may disclose PHI about a patient who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

V. Crime on premises

(company name) may disclose PHI to a law enforcement official that (company name) believes in good faith constitutes evidence of criminal conduct that occurred on the premises of (company name).

(company name) should seek legal advice on how to respond to law enforcement requests for PHI in accordance with applicable law and to ensure compliance with HIPAA Privacy Rule 45 CFR Part 164.512(f).

J. Decedents

I. Coroners and medical examiners.

(company name) may use or disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

II. Funeral directors.

(company Name) may use or disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.

III. (company name) may use and disclose PHI as per this policy for a period of 50 years. After 50 years, PHI is no longer protected under HIPAA regulations.

K. Organ, Eye or Tissue Donation

I. (company name) may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

L. To Avert a Serious Threat to Health or Safety

(company name) may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if (company name), in good faith, believes the use or disclosure:

- I. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or**
- II. Is necessary for law enforcement authorities to identify or apprehend an individual:**
 - 1. Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or**

2. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.
3. (company name) may disclose only the following limited patient health information to law enforcement officials in response to their request made for purposes of identifying or locating a suspect, fugitive, material witness or missing person:
 - i. Name and address
 - ii. Date and place of birth
 - iii. Social Security number
 - iv. ABO blood type and rh factor
 - v. Type of injury
 - vi. Date and time of treatment
 - vii. Date and time of death, if applicable
 - viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

M. Specialized Government Functions

(company name) may use and disclose PHI of individuals who are Armed Forces including Military (domestic and foreign), veteran, national security, intelligence and protective service activities (for President or other authorized federal officials personnel) for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission:

(company name) may use and disclose PHI to correctional institutions and other law enforcement custodial situations

N. Workers Compensation

(company name) may disclose PHI to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

O. De-Identified Information

(company name) may use or disclose PHI that has been properly de-identified. De-identified PHI is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

OCR has provided guidance regarding methods and use of de-identified PHI at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>

P. Limited Data Set

(company name) may use or disclose a limited data set if (company name) enters into a data use agreement with the recipient of the limited data set and if the purpose of the use or disclosure is for research, public health, or health care operations. (company name) may use or disclose a limited data set only if the data use agreement demonstrates satisfactory assurance, as per the HIPAA Privacy Rule § 164.514 (e), that the limited data set recipient will only use or disclose the PHI for limited purposes.

A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- I.** Names
- II.** Postal address information, other than town or city, State, and zip code;
- III.** Telephone numbers;
- IV.** Fax numbers;
- V.** Electronic mail addresses;
- VI.** Social security numbers;
- VII.** Medical record numbers;
- VIII.** Health plan beneficiary numbers;
- IX.** Account numbers;
- X.** Certificate/license numbers;
- XI.** Vehicle identifiers and serial numbers, including license plate numbers;
- XII.** Device identifiers and serial numbers;

- XIII.** Web Universal Resource Locators (URLs);
- XIV.** Internet Protocol (IP) address numbers;
- XV.** Biometric identifiers, including finger and voice prints; and
- XVI.** Full face photographic images and any comparable images.

Section 5 – Special Circumstances

The purpose of this policy to provide clear guidelines for disclosure and use of protected health information (PHI) when used for marketing, fundraising and research.

(company name)'s workforce members **may not** use and disclosure PHI without a patient's valid authorization. A valid authorization is required for the following:

A. Marketing

(company name) may not use or disclose PHI for marketing purposes without written authorization from a patient. Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. If the marketing involves direct or indirect financial payment to (company name) from a third party, the authorization must state that such payment is involved. The following exceptions apply:

- I. Marketing discussions are face to face with the patient
- II. The product or service to be marketed of nominal value (examples include: brochure, business card, pen, etc.)
- III. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, as long as any remuneration is reasonably related to the cost of making the communications. Accordingly, a drug manufacturer may subsidize the cost for sending out refill reminders.

B. Fundraising

(company name) may not use or disclose PHI for fundraising purposes unless a statement is included in (company name)'s Notice of Privacy Practices. Fundraising communications must have a clear and conspicuous opportunity to elect not to receive any further fundraising communications. If a patient opts out of fundraising communications, no further fundraising communications shall be made to the patient.

(company name) may only use the following PHI for fundraising purposes:

- I. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth
- II. Date health care services were provided
- III. Department of service information
- IV. Treating physician(s)
- V. Outcome Information

VI. Health insurance status

C. Research

(company name) may not use or disclose PHI for research purposes without written authorization from a patient unless:

- I. PHI will be used for research purposes and (company name) obtains documentation that a Waiver of Authorization has been approved by an Institutional Review Board (IRB) as defined in the HIPAA Privacy Rule 45 CFR 164.512 (i)
- II. (company name) obtains from the researcher a signed agreement that the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research, the PHI is necessary for research purposes and that no PHI is to be removed from (company name) by the researcher in the course of the review.

Section 6 – Disclosure of PHI Requiring an Opportunity to Agree or Object

The purpose of this policy is to provide clear guidelines for disclosure and use of protected health information (PHI) provided that the patient is informed in advance of the use or disclosure and has the opportunity to agree to or object or restrict the use or disclosure. (company name) is permitted to orally inform the individual of and obtain the individual's agreement or objection to a use or disclosure

A. Family Members and Close Friends

(company name) may disclose to a family member, other relative or close friend or any other person the patient identifies, PHI directly relevant to such person's involvement with the patient's care or payment related to the patient's care provided:

- I. The patient's agreement is obtained orally;
- II. The patient is allowed to object to the disclosure and does not express any objection; or
- III. A (company name)'s workforce member reasonably infers from the circumstances, based on professional judgment that the patient does not object to the disclosure;
- IV. The patient is not physically present or the patient is incapacitated (sedated, unconscious, etc.) or in the case of an emergency, (company name)'s workforce members may determine, using professional judgment, that disclosure of a limited amount of PHI would be in the patient's best interest. Examples include picking up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

(company name) may use or disclose PHI to locate or assist in the notification of a family member or another person responsible for the care of the patient. The information that is to be used or disclosed may include the patient's location, general condition, or death, if the above criteria are met.

B. Disaster Relief Purposes

(company name) may use or disclose PHI, if required by law, to a public or private entity to assist in disaster relief efforts. The use or disclosure of PHI should follow the above requirements to have the patient present (I – III) or not present (IV) and provide agreement or objection. In the case the patient objects, the use of professional judgment should be made to determine if the objection will interfere with the ability to respond to emergency circumstances.

Section 7 – Use and Disclosures Requiring Authorization

A. General Rule

(company name) will not use or disclose PHI except where allowed by the HIPAA Privacy Rule and/or (company name)'s Privacy Policies.

B. Psychotherapy Notes

If applicable to (company name), the following policies and procedures will apply to the use or disclosure of psychotherapy notes:

Psychotherapy notes shall be maintained separately from other portions of the patient's medical record and shall only be used or disclosed as allowed by law and this policy.

I. Authorization required

Except as otherwise allowed by law and this policy, a separate Authorization specifically limited to use or disclosure of psychotherapy notes must be obtained from the patient or his/her legal representative before psychotherapy notes can be used or disclosed.

II. Authorization NOT required

An Authorization is not required to carry out the following treatment, payment or health care operations:

1. Use by the originator of the psychotherapy notes for treatment;
2. Use or disclosure by (company name) for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
3. Use or disclosure by (company name) to defend itself in a legal action or other proceeding brought by the individual;
4. Use or disclosure to the Department of Health and Human Services to determine compliance with the privacy rule; and
5. Use or disclosure required or allowed by law. See Section 4 – Disclosure of PHI without a Patient's Authorization

C. Patient Authorizations

Except for situations defined in **Section 4 – Disclosure of PHI without a Patient’s Authorization**, PHI may not be used or disclosed unless a written authorization has been signed by the patient.

I. Valid Authorizations

A valid authorization must:

1. Be in writing and written in plain language;
2. Must be signed and dated by the patient or personal representative;
3. Must not be expired or revoked;
4. Must be filled out completely;
5. Must have required language stated in HIPAA regulations;
6. Cannot be combined with other documents

II. Authorization Form

(company name) will use the form in **Appendix C – Patient Authorization to Release Health Information** or will use a similar form that has the same or similar content.

III. Prohibition on Condition of Authorizations

(company name) may not condition the provision of treatment to any patient on the receipt of a valid HIPAA Authorization, except as allows below:

1. Condition research related treatment on the receipt of a valid authorization for such research;
2. Condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party. Examples may include pre-employment physical that require an authorization to release information to the prospective employer.

IV. Revocation of Authorization

A patient may revoke their authorization at any time by providing a written and signed revocation.

V. Documentation

(company name) must keep all authorizations or six (6) years from the date of signature or the date when it was last in effect, whichever is later.

Section 8 – Minimize Use and Disclosure of PHI

A. Minimum Necessary Standard

(company name) will make reasonable efforts to minimize the use or disclosure of PHI or request the minimal amount of PHI from another covered entity or business associate necessary to accomplish the intended purpose.

I. Workforce members

(company name) will disclose PHI to workforce members but the disclosure will be limited based on the workforce member's need to use or access PHI to perform their job function. Workforce members that do not have a legitimate need to access PHI will be restricted from having such access.

II. Requests received for disclosure of PHI

1. Whenever possible (company name) will provide a Limited Data Set (see Section 4 – Disclosure of PHI without a Patient's Authorization) to satisfy requests received for disclosure of PHI.
2. For any type of disclosure that it receives on a routine and recurring basis, (company name) must implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.
3. For non-routine and recurring requests for disclosure, (company name) will develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and will review each request on an individual basis against the criteria.

III. Requests for PHI by (company name)

1. For any type of disclosure that it makes on a routine and recurring basis, (company name) must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to achieve the purpose of the request.
2. For non-routine and recurring requests for disclosure it makes, (company name) will develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and will review each request on an individual basis against the criteria.

IV. Exceptions

The Minimum Necessary Standard does not apply to the following exceptions:

1. Disclosures to or requests by a health care provider for treatment;
2. Disclosures made to the patient;
3. Disclosures made pursuant to a patient's written authorization;
4. Disclosures made to the Secretary of Health and Human Services (HHS);
5. Disclosures required by law; and
6. Disclosures required by HIPAA Privacy or Security Rules

B. Incidental Use and Disclosures

(company name) may incidentally disclose PHI as long as the Minimum Necessary Standard is applied and reasonable safeguards are in place. Examples include patient sign-in sheets or calling out patient names in a waiting room. Note: sign-in sheets should have no medical information such as what medical problem for which the patient is seeing the physician.

C. Verification

Prior to disclosing PHI, (company name) workforce members should request verification of identity and the authority of any such person to have access to PHI. No verification is necessary if the person requesting PHI is the patient or the identity and authority of the person is known.

I. Verification Procedures

1. Patient requesting PHI:
 - i. If the patient appears in person and is known, no verification is necessary;
 - ii. If the patient appears in person and is NOT known, verification should be obtained by requesting photo identification (i.e. driver's license); or
 - iii. If the person claiming to be the patient calls via telephone and requests PHI, verification should be obtained. Verification may include date of birth, last 4 digits of social security number, mother's maiden name, etc.
2. Person other than patient requesting PHI:
 - i. If the person and the authority of the person to request PHI is known, no verification is necessary; or

- ii. If the person and the authority to request PHI is not known, obtain any documentation/statement, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of disclosure.
3. Public official or law enforcement representative requesting PHI:
 - i. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
 - ii. If the request is in writing, the request is on the appropriate government letterhead; or
 - iii. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
 - iv. Authority of public officials should be obtained which includes:
 - A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
 - If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
4. Health care providers or insurance companies requesting PHI:
 - i. If the health care provider or insurance company is known, no further verification is required
 - ii. If the health care provider or insurance company is not known, a written request on company letterhead should be requested for verification.
5. Exercise of professional judgment:

(company name) workforce members should use professional judgment when making use or disclosures of PHI.

 - i. Detailed PHI should not be left on answering machines.
 - ii. Verify phone number and identity prior to faxing PHI. Caution should be used when faxing PHI to avoid sending to an incorrect fax number. Fax cover sheets should be used explaining that the information contained in the fax is confidential and should be destroyed if the fax is received by someone other than the intended recipient.
 - iii. Care should be used when sending PHI via mail. Sealed envelopes should be used and verification that the correct address of the intended recipient is correct.

- iv. Minimum Necessary Standard should be used when disclosing PHI to known or unknown individuals.

Section 9 – Patient Rights

Patients have rights established by the HIPAA Privacy Rule. All patient rights should be recognized and enforced.

A. Right to Notice

A Notice of Privacy Practices (NPP), the same or similar to a ***copy found as a separate document to this Privacy Manual***, will be given to all patients for their inspection. This notice will provide patients with valuable information concerning the use and disclosure of their PHI and how (company name) uses and safeguards their PHI. The NPP will contain all the elements required by the HIPAA Privacy and Omnibus Rules.

I. Providing the NPP to Patients

(company name) will provide a copy of the NPP to all new patients on their first visit or in an emergency treatment situations, as soon as reasonably practicable after the emergency treatment situation.

II. Patient acknowledgement

(company name) will make a good faith effort to obtain a written acknowledgment of receipt of the NPP. If the acknowledgement is not obtained, document the good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained. Patients will be asked to sign the acknowledgment using the form in ***Appendix A – Acknowledgement of Receipt of Notice of Privacy Practices*** or a similar form that has the same or similar content;

III. Placement and delivery of the NPP

The NPP should be posted in the lobby or reception area or in a location that is accessible to all patients. The NPP should be posted on (company name)'s website if applicable.

The NPP may be emailed to a patient if the patient agrees to electronic notice and such agreement has not been withdrawn.

IV. Document retention

All NPP acknowledgements and/or documentation of good faith efforts to obtain acknowledgment will be kept for a minimum of six (6) years from the date they are signed or documented.

B. Right to Request Restrictions

A patient has the right to request restrictions regarding the use and disclosure of their PHI for treatment, payment and health care operations. Patients have the right to request restrictions on disclosures made to family members, relatives and close friends.

I. Written requests

All patient requests for restrictions of PHI should be written and submitted using the form in **Appendix G – Restriction of Protected Health Information Request Form** or will use a similar form that has the same or similar content.

II. Honor or rejection of requested restrictions

(company name) does not have to agree to or honor a patient's requested restriction of PHI. If (company name) agrees to a restriction then PHI may not be used or disclosed in violation of the agreed upon restriction except;

1. If the patient who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, then the use or disclosure of restricted PHI may be used to provide such emergency treatment; and
2. If restricted PHI is disclosed to a health care provider for emergency treatment, then (company name) must request that the health care provider not further use or disclose the information.

(company name) will notify patients in writing if the requested restriction has been approved or rejected. If a restriction is approved then a notation should be made in the patient's chart identifying that use and disclosure of PHI is restricted.

III. Disclosures required by law

Restrictions of PHI requested by a patient and agreed upon by (company name) will not be honored if the use or disclosure of PHI is required by law or required under HIPAA regulations.

IV. Mandatory restrictions

(company name) must honor a request for restriction of PHI if the disclosure is for the purposes of carrying out payment or health care operations and not otherwise required by law; and the PHI pertains solely to a health care item or service for which the patient has paid for services in full out of pocket.

V. Termination of restrictions

(company name) may terminate its agreement to a restriction if;

1. The patient agrees to or requests the termination in writing;

2. The patient orally agrees to the termination and the oral agreement is documented; or
3. (company name) informs the patient that it is terminating its agreement to a restriction. The termination is only effective to PHI created or received after the patient has been notified.

VI. Documentation

All patient requests and responses for restrictions to PHI will be documented and kept for a minimum of six (6) years from the date of the documents.

C. Right to Confidential Communications

A patient has the right to reasonably request to receive communications by an alternative means or at alternative locations, if the patient clearly states that the disclosure of all or part of that information could endanger the patient.

I. Conditions on providing confidential communications

(company name) may condition requests for confidential communications on the following:

1. Written request

A patient should request confidential communications via writing using the form in **Appendix H – Request for Confidential Communications** or will use a similar form that has the same or similar content. The patient should provide an alternative address or other method of contact requested. Approved requests for confidential communications will be noted in a patient's chart noting the alternative address and/or the alternative communication method.

2. Payment information

(company name) will require assurances of how payment for services will be handled.

II. No demand for explanations

(company name) will not require an explanation from the patient as to the basis for the request as a condition of providing communications on a confidential basis.

III. Documentation

All patient requests and responses for confidential communications will be documented and kept for a minimum of six (6) years from the date of the documents.

D. Right to Access PHI

A patient has the right to request access to inspect and to request a copy of PHI in a designated records set with exceptions that are defined in this section.

I. Designated Record Set

A Designated Record Set for PHI, either in paper or electronic form, will include the following types of information:

1. Patient's medical records;
2. Patient's billing, financial and collection information;
3. PHI created or maintained by Business Associates; and
4. Any information used to make decisions about a patient

Items excluded from a Designated Record Set include:

1. Psychotherapy notes;
2. PHI exempt under the Clinical Laboratory Improvements Act (CLIA);
3. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or
4. Other information that is exempt from disclosure under state or federal law

II. Procedure for requesting access to PHI

1. Request and timing

(company name) may require that a patient request in writing to have access to their PHI. If the request for access is approved then the patient will be given a copy of their PHI either in paper or electronic format. The following timeframes will apply:

- i. If the PHI is maintained onsite, access and copies of the PHI will be given to the patient within 30 days after the receipt of the request.
- ii. If the PHI is not maintained onsite, access and copies of the PHI will be given to the patient within 60 days after the receipt of the request.
- iii. If (company name) is not able to provide access to PHI, despite best attempts, that is either maintained onsite or not maintained onsite within the above timeframes, a **one-time** extension of 30 days will be allowed.

The patient must be notified in writing of the reasons for the delay and the date by which the request will be completed.

2. Form of access

- i. (company name) will provide the patient with access to PHI in the form or format requested by the patient if it is readily producible. If the form or format is not readily producible, PHI will be provided in a hard copy form or other format (i.e. Word, Excel, PDF, etc.) that is mutually agreeable.
- ii. (company name) may provide the patient with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI, if the patient agrees in advance to the summary or explanation and if the patient agrees in advance to any fees imposed for the summary or explanation.

3. Manner of access

(company name) will provide the patient with a convenient time and place to inspect or obtain a copy of the protected health information.

4. Fees

(company name) may charge a reasonable, cost-based fee to provide a copy or summary of PHI. The fee must only include the cost of copying, postage or labor for preparing the information.

5. Denial of access

If (company name) denies a patient access to PHI the following must be done:

- i. The denial must be in written format to the patient and be written in plain language. The written denial must include:
 - Basis for the denial;
 - If applicable, statement of the patient's right to have the denial reviewed and the procedure for the review; and
 - A description of how the patient may complain to either (company name) or to the Secretary of Health and Human Services (HHS). The description must include the name or title and the telephone number of the (company name) designated contact person.
- ii. (company name) must, to the extent possible, give the patient access to any other PHI after excluding the PHI to which (company name) has denied access.

- iii. If (company name) does not maintain the requested PHI but knows where the PHI is maintained, then the patient must be informed of where they should direct a request for access.

6. Denial of access with review

(company name) may deny a patient access to PHI and provide the patient with the ability to review the decision with a licensed health care professional that did not participate in the original decision to deny access. Denial of access to PHI may be determined in the following circumstances:

- i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
- ii. The PHI makes reference to another person (that is not a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person; or
- iii. The request for access is made by the patient's personal representative and a licensed health care professional has determined, that access to the personal representative is reasonably likely to cause substantial harm to the patient or another person.

7. Review of a denial of access

If a patient requests a review of a denial of access the following will occur:

- i. The patient will request in writing that they request a review of the denial.
- ii. The request will be given to the HIPAA Privacy Officer.
- iii. The review will be performed by a licensed health care professional that is chosen by (company name) that did not participate in the original decision to deny access.
- iv. The review will occur in a reasonable period of time.
- v. The outcome of the review must be communicated to the patient in written format promptly after the decision has been made.
- vi. (company name) will provide or deny access to the request PHI in accordance with the review decision.

8. Denial without review

(company name) may deny a patient access to PHI without providing an opportunity to review the decision in the following circumstances:

- i. The PHI requested contains psychotherapy notes;
- ii. PHI exempt under the Clinical Laboratory Improvements Act (CLIA);
- iii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or
- iv. Other information that is exempt from disclosure under state or federal law;
- v. (company name) is acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
- vi. The patient, when consenting to participate in research that includes treatment, agrees to temporary denial of access to PHI created or obtained by a health care provider in the course of research, and the research is not yet complete.
- vii. PHI requested are subject to the Privacy Act and the denial of access meets the requirement of that law.
- viii. The PHI requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

9. Documentation

All documentation regarding patient requests for access and any denial or any other documentation will be kept for a minimum of six (6) years from the date of the documents.

E. Right to Amend PHI

Patients have the right to request an amendment or correction to PHI if they feel the information is incomplete or inaccurate.

I. Procedure for requesting amendment to PHI

The following procedure will be followed for a request to amend PHI:

1. Written request

All requests to amend or correct PHI must be in written. Patients will use the form in **Appendix B – Request for Amendment of Addition to Protected Health Information** or will use a similar form that has the same or similar content. Requests will be forwarded and reviewed by the HIPAA Privacy Officer

2. Timing

(company name) will act on the patient's request for an amendment no later than 60 days after receipt of such a request.

If (company name) is not able to act on the request within 60 days, a **one-time** extension of 30 days will be allowed. The patient must be notified in writing of the reasons for the delay and the date by which the request will be completed.

3. Accepting the amendment

If (company name) accepts the requested amendment the following steps must be performed.

- i. Make the amendment to the patient's record or provide a link or reference to the location of the amendment;
- ii. Inform the patient that the amendment is accepted;
- iii. (company name) will obtain from patient agreement and identification of person(s) that the amendment needs to be shared with;
- iv. (company name) must make reasonable efforts, within a reasonable timeframe to provide the amendment to persons, including business associates that (company name) knows have the PHI that is the subject of the amendment and that may have relied, or could likely rely on the information to the detriment of the patient.

4. Denying the amendment

If the request for amendment is denied, (company name) will provide the patient, in a reasonable timeframe, a written explanation, in plain language, of why the request was denied. The written explanation will contain the following:

- i. The reason for the denial. Reasons for denial may include:
 - The PHI was not created by (company name) unless the originator of the PHI is no longer available to act on the requested amendment;
 - The PHI is not part of the patient's health record;
 - The PHI is not accessible to the patient because federal or state laws do not permit access to the PHI; or
 - The PHI is accurate and complete
- ii. The patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;
- iii. A statement that if the patient does not submit a statement of disagreement, the patient may request that (company name) include the patient's request for amendment and the denial along with any future disclosures of PHI that is subject of the requested amendment.
- iv. A description of how the patient may complain to either (company name) or to the Secretary of Health and Human Services (HHS). The description must include the name or title and the telephone number of the (company name) designated contact person.

5. Statement of disagreement

A patient will be permitted to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of the disagreement. The disagreement will be limited to one (1) hand written or typed piece of letter sized paper.

6. Rebuttal statement

(company name) may prepare a written rebuttal to the patient's statement of disagreement. The patient must be given a copy of the rebuttal statement.

7. Recordkeeping

(company name) will identify the PHI that is subject to the disputed amendment and append or link to the patient's request for amendment, the denial of amendment and any statement of disagreement and/or rebuttal statements.

8. Future disclosures

- i. If a statement of disagreement has been submitted by the patient, the statement will be included or an accurate summary will be included with any subsequent disclosures of PHI to which the disagreement relates to.
- ii. If the patient has not submitted a written statement of disagreement, the individual's request for amendment and its denial, or an accurate summary of the information, will be included with any subsequent disclosure of PHI only if the patient has requested such action.
- iii. When a subsequent disclosure made using a standard transaction that does not permit the additional material to be included with the disclosure, (company name) will transmit the required material separately.

9. Amendment by other covered entities

If another covered entity notifies (company name) that an amendment of PHI has been made to a patient's record, (company name) will:

- i. Make the amendment to the patient's record or provide a link or reference to the location of the amendment;
- ii. (company name) must make reasonable efforts, within a reasonable timeframe to provide the amendment to persons, including business associates that (company name) knows have the PHI that is the subject of the amendment and that may have relied, or could likely rely on the information to the detriment of the patient.

10. Documentation

All documentation regarding patient requests for amendment and any denial or any other documentation will be kept for a minimum of six (6) years from the date of the documents.

F. Right to an Accounting of Disclosures of PHI

A patient has the right to receive an accounting of disclosures of their PHI made by (company name) and/or its business associates. The accounting of disclosures of PHI will include all disclosures in the six (6) years prior to the date of the request. A patient has the right to request accounting of disclosures for a period less than six (6) years.

I. Disclosures excluded

Excluded disclosures that do not have to be reported to a patient include:

- 1. To carry out treatment, payment and health care operations;
- 2. To the patient;

3. Incident to a use or disclosure otherwise permitted by the HIPAA Privacy Manual or the HIPAA Privacy Rules;
4. Pursuant to an authorization signed by the patient;
5. To people involved in the patient's care;
6. For national security or intelligence purposes;
7. To correctional institutions or law enforcement officials;
8. Limited Data Sets;
9. Disclosures that occurred prior to April 14, 2003

II. Suspension of the right to accounting of disclosures

(company name) must temporarily suspend a patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by that agency or official if giving the accounting would impede the agency's activities.

III. Content of the accounting

Information to be included in the accounting of disclosures:

1. Date of disclosure;
2. Name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed; and
4. Brief statement of the purpose of the disclosure or a copy of the written request for disclosure.
5. Multiple disclosures to the same person or entity for a single purpose will have a summary entry. A summary entry includes all information for the first disclosure (date of first disclosure, who it was disclosed to, description, etc.), the frequency with which disclosures were made, and the date of the last disclosure during the accounting period.
6. Accounting for disclosure for the purpose of research will follow requirements defined in the HIPAA Privacy Rule 45 CFR Part 164.528(b)(4)(i).

IV. Procedure for accounting of disclosures

1. Request accounting of disclosures

All requests for accounting of disclosures will be made in writing and will be forwarded to the HIPAA Privacy Officer. Patients will use the form in **Appendix**

E – Request for Accounting of Disclosures Form or will use a similar form that has the same or similar content. A sample log is included in ***Appendix F - Accounting of Disclosures Log*** that can be used to document and provide an accounting of disclosures.

2. Timing

The patient will be provided with an accounting of disclosures within 60 days from the receipt of the request. If (company name) is not able to act on the request within 60 days, a one-time extension of 30 days will be allowed. The patient must be notified in writing of the reasons for the delay and the date by which the request will be completed.

3. Fees

Accounting of disclosures will be provided to the patient free of charge for a request made once in a 12 month period. A reasonable, cost-based fee can be charged for each subsequent request for an accounting within the 12 month period, provided the patient is informed in advance of the fee and provides the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

4. Documentation

All documentation regarding patient requests for accounting and any other documentation will be kept for a minimum of six (6) years from the date of the documents.

HIPAA Privacy Manual
Appendix of Forms

Appendix A: Acknowledgement of Receipt of Notice of Privacy Practices

Acknowledgement of Receipt of Notice of Privacy Practices

Practice Name: _____ Contact Person: _____

Contact Phone, Email and Fax: _____

Notice to Patient:

We are required to provide you with a copy of our Notice of Privacy Practices, which states how we may use and/or disclose your health information.

Our Office Policies contains important information regarding payment, insurance, collections, cancellations, returns, refunds and other important information.

By signing this form, I acknowledge that I have received a copy of this office's Notice of Privacy Practices, and Office Policies. You may refuse to sign this acknowledgment, if you wish.

Patient Name / Relationship: _____

Print your Name: _____

Signature: _____

Date: _____

For Office Use Only

We have made every effort to obtain written acknowledgment of receipt of our Notice of Privacy Policies from this patient but it could not be obtained because:

☐ The Patient refused to sign ☐ We were not able to communicate with the Patient

☐ Due to an emergency situation it was not possible to obtain a signature

Other (please provide details): _____

Employee Signature: _____ Date: _____

Appendix B: Request for Amendment of Addition to Protected Health Information

Request for Amendment of or Addition to Protected Health Information

Practice Name: _____ Contact Person: _____

Contact Phone, Email and Fax: _____

As required by the Health Information Portability and Accountability Act of 1996 you have a right to request that health information that pertains to you be amended if you believe that it is incorrect or incomplete. We will review your request and either grant your request or explain the reason why it will not be granted. In the event that your request is not granted, you have the right to submit a statement of disagreement that will accompany the information in question for all future disclosures.

Patient Name / Relationship: _____

Date of Birth: _____

Patient Address: _____

Patient Phone Number: _____

Items to be amended

Date of entry to be amended: _____ Type of entry to be amended: _____

Please explain how the entry is incorrect or incomplete. What revisions would you like to be made to the entry? (Please use additional paper if necessary):

Would you like us to notify anyone else regarding the amendment? Please provide the name and address:

Name: _____ Address: _____

Name: _____ Address: _____

Signature of Patient or
Legal Representative: _____ Date: _____

If we agree to change your information, we will communicate the changed information to persons or entities that you have designated above. We will also communicate the changed information to any other persons or entities that we know have received the information before it was amended. If we are not able to act on this request in 60 days, we will notify of the reasons for the delay.

Appendix C: Patient Authorization to Release Health Information

Authorization for Release of Health Information

Practice Name: _____

I understand and agree that:

- This authorization is voluntary;
- My health information may contain information created by other persons or entities including health care providers and may contain medical, pharmacy, dental, vision, mental health, substance abuse, HIV/AIDS, psychotherapy, reproductive, communicable disease and health care program information;
- I may not be denied treatment, payment for health care services, or enrollment or eligibility for health care benefits if I do not sign this form except (1) if my treatment is related to research, or (2) health care services are provided to me solely for the purpose of creating protected health information for disclosure to a third party ;
- My health information may be subject to re-disclosure by the recipient, and if the recipient is not a health plan or health care provider, the information may no longer be protected by the federal privacy regulations;
- This authorization will expire one year from the date I sign the authorization. I may revoke this authorization at any time by notifying in writing; however, the revocation will not have an effect on any actions taken prior to the date my revocation is received and processed.

Who May Receive and Disclose my Information:

I authorize the disclosure of my individually identifiable health information to the following person(s) or organization(s):

Full Name of Person(s) or Organization(s)

Full Address of Person(s) or Organization(s)

Type of Information to be Disclosed:

☐ I authorize disclosure of all my health information, including information relating to medical, pharmacy, dental, vision, mental health, substance abuse, HIV/AIDS, psychotherapy, reproductive, communicable disease and health care program information; or

☐ I authorize only the disclosure of the following information:

Type of Information

Purpose of Disclosure:

- ☐ My health information is being disclosed at my request or at the request of my personal representative; or
- ☐ My health information is being disclosed for the following purpose:

Explain Purpose (No purpose need be stated if the request is made by the patient and the patient does not wish to state the purpose.)

Signature of Patient or Patient's Representative

Date

Printed Name of Patient's Representative (if applicable)

Relationship to Patient (if applicable)

**** YOU ARE ENTITLED TO A COPY OF THIS DOCUMENT ****

Appendix D: Patient Complaint Form

HIPAA Privacy Related Compliant Form

Practice Name: _____

Patient Name: _____

Name of person submitting this complaint (if other than patient):

Relationship to Patient: _____

Telephone #: _____ Email: _____

Address: _____

Information regarding your complaint

Date(s) Action Occurred: _____

Describe situation and effect on privacy (attach separate sheet, if needed):

Practice personnel involved in this matter: _____

Describe how you feel your complaint could be resolved:

Signature of Patient or Patient's Representative

Date

Individuals who request an outside agency to review their complaint may contact:

US Department of Health and Human Services

Office for Civil Rights

233 N. Michigan Ave. Suite 240

Chicago, Illinois 60601

Voice phone: (800)368-1019 or TDD: (800) 537-7697

FAX: (312) 886-1807

OCRComplaint@hhs.gov <http://www.hhs.gov/ocr/privacy/hipaa/complaints/>

For Office Use Only

Date Received: _____ Received By _____

Report Received (attach): _____ In Person _____ Email _____ Mail _____

Summary of investigation:

Follow-up action taken

Appendix E: Request for Accounting of Disclosures Form

REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

Practice Name: _____ Contact Person: _____

Contact Phone, Email and Fax: _____

Patient Name: _____ Date of Birth: _____

Name of person submitting this complaint (if other than patient):

Relationship to Patient: _____

Telephone #: _____ Email: _____

Address: _____

Please list the dates for which you are requesting an accounting (may not be more than six years prior to the date of your request):

From ____/____/____ To ____/____/____

If you wish to limit the accounting to those disclosures made to a specific person or entity, please identify that person or entity here. If this section is left blank, an accounting of *all* disclosures made during the time period listed above (except those for which we not required to account for) will be provided:

Signature: _____ Date: _____

Appendix F: Accounting of Disclosures Log

Accounting of Disclosure of Protected Health Information Log

Date	Name of Individual	Name of Party to Whom Information Was Disclosed	Summary of Disclosed Information	Purpose or Basis

Appendix G: Restriction of Protected Health Information Request Form

Restriction of Protected Health Information Request Form

Practice Name: _____ Contact Person: _____

Contact Phone, Email and Fax: _____

You have the right to request that we restrict how protected health information about you is used or disclosed for treatment, payment, or healthcare operations. ***We are not required to agree to this restriction, but if we do, we are bound by our agreement. Any restriction we accept will not apply when the restricted information is needed to provide you with emergency treatment. We further have the right to terminate any agreed upon restriction by informing you of the termination in writing. Any such termination will only apply to information created or received after we have informed you of the termination.***

Please complete this form to request a restriction and we will notify you of our ability to comply with your request by returning a copy of this form to you, no later than 30 days from its receipt. You also have the right to request us to terminate a restriction to the extent that such termination applies to information created or received after the date of termination.

Requested Restrictions (please provide specific details and dates):

Print Patient Name: _____

**Signature of Patient or
Authorized Representative:** _____

Date: _____

Relationship to Patient: _____

For Practice Use Only:

Practice: ☐ Accepts ☐ Denies

Privacy Officer Signature: _____

Date: _____

Note: The Practice must honor requests for restrictions of health information by the patient if (1) the disclosure will be to an insurance company for purposes of payment or health care operations, and (2) the patient has paid for the service out of pocket in full.

Appendix H: Request for Confidential Communications

Request for Confidential Communications

Practice Name: _____ Contact Person: _____

Contact Phone, Email and Fax: _____

Patients have the right to request that we communicate their protected health information by an alternative means or to an alternative location ("confidential communication"). All requests for confidential communication must be in writing and include the information documented on this form. We will review each request but reserve the right to refuse the request as established by federal law.

Patient Name: _____ Date of Birth: _____

Telephone #: _____ Email: _____

Address: _____

*****Select the confidential communication means being requested: *****

☐ Alternate address:

Address: _____

If the address provided above is not your home address or is not a street address, please provide us with a street address for purposes of ensuring payment:

Payment Address: _____

☐ Alternate phone number:

Telephone #: _____

☐ Other:

Please provide the requested communication and what should be communicated: _____

Signature: _____ Date: _____

HIPAA Privacy Rule
Receipt of Notice of Privacy Practices
Written Acknowledgement Form

Acknowledgement of receipt of Information Practices Notice (§164.520(a))

I, _____, (patient's name) understand that as part of my healthcare, this facility originates and maintains health records describing my health history, symptoms, examination and test results, diagnosis, treatment and any plans for future care or treatment. I acknowledge that I have been provided with and understand that this facility's Notice of Privacy Practices provides a complete description of the uses and disclosures of my health information. I understand that:

- I have the right to review this facility's Notice of Privacy Practices prior to signing this acknowledgement
- This facility reserves the right to change their Notice of Privacy Practices and prior to implementation of this will mail a copy of any revised notice to the address I've provided if requested.

Signature of Individual or Legal Representative Witness _____

Printed Name of Individual or Legal Representative _____

Date: _____

FOR OFFICE USE ONLY

We attempted to obtain written acknowledgement of receipt of our Notice of Privacy Practices, but it could not be obtained because:

- ☐ Individual refused to sign
- ☐ Communication barrier prohibited obtaining the acknowledgement
- ☐ An emergency situation prevented us from obtaining acknowledgement
- ☐ Others (please specify)

PDF instructions

Each fillable field includes instructions for what information to add. The instructions are also listed here.

The field on page 7 of the Booklet Notice and page 4 of the Full Page and Layered Notices is for special notes to add *if* they apply to your entity. If notes are not needed, the field can be left blank. However you must click inside the field and add a word space to delete the instructions so they will not print.

If fields are not highlighted when you open the PDF, click on "Highlight Fields" in the upper right corner.

Booklet Notice for Health Care Providers

Page 1 • Instruction A: Insert the covered entity's name

Page 7 • Instruction B: Insert any special notes that apply to your entity's practices such as "we do not create or manage a hospital directory" or "we do not create or maintain psychotherapy notes at this practice."

Instruction C: The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.

Instruction D: If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.

Page 8 • Instruction E: If your entity is part of an OHCA (organized health care arrangement) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment, and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."

Instruction F: Insert the covered entity's name, address, web site and privacy official's (or other privacy contact) email address and phone number.

Instruction G: Insert Effective Date of Notice here.

Full Page and Layered Notices for Health Care Providers

Page 1 • Instruction A: Insert the covered entity's name

Instruction B: Insert the covered entity's address, website and privacy official's phone and email address and other contact information

Page 4 • Instruction C: Insert any special notes that apply to your entity's practices such as "we do not create or manage a hospital directory" or "we do not create or maintain psychotherapy notes at this practice."

Instruction D: The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.

Instruction E: If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.

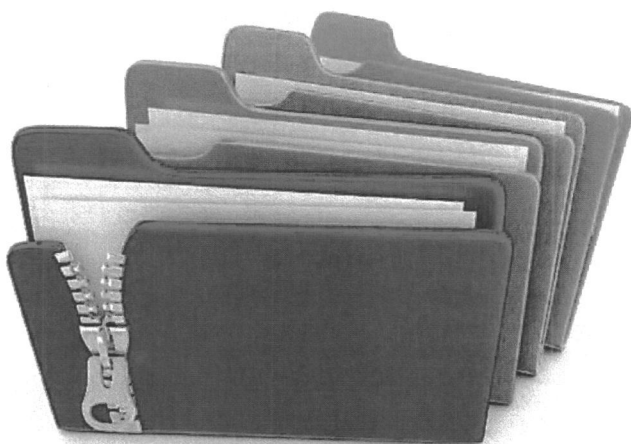
Page 5 • Instruction F: Insert Effective Date of Notice here.

Instruction G: If your entity is part of an OHCA (organized health care arrangement) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment, and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."

Instruction H: Insert name or title of the privacy official (or other privacy contact) and his/her email address and phone number.

Instruction A: Insert the covered entity's name

Instruction B: Insert the covered entity's address, web site and privacy official's phone, email address, and other contact information.



Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.
Please review it carefully.

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

continued on next page

Your Rights *continued*

Ask us to limit what we use or share

- You can ask us **not** to use or share certain health information for treatment, payment, or our operations.
 - We are not required to agree to your request, and we may say “no” if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer.
 - We will say “yes” unless a law requires us to share that information.

Get a list of those with whom we’ve shared information

- You can ask for a list (accounting) of the times we’ve shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We’ll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice

- You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated

- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory
- Contact you for fundraising efforts

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases we *never* share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:

- We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures

How do we typically use or share your health information? We typically use or share your health information in the following ways.

Treat you

- We can use your health information and share it with other professionals who are treating you.

Example: A doctor treating you for an injury asks another doctor about your overall health condition.

Run our organization

- We can use and share your health information to run our practice, improve your care, and contact you when necessary.

Example: We use health information about you to manage your treatment and services.

Bill for your services

- We can use and share your health information to bill and get payment from health plans or other entities.

Example: We give information about you to your health insurance plan so it will pay for your services.

continued on next page

How else can we use or share your health information? We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues	• We can share health information about you for certain situations such as: • Preventing disease • Helping with product recalls • Reporting adverse reactions to medications • Reporting suspected abuse, neglect, or domestic violence • Preventing or reducing a serious threat to anyone's health or safety
Do research	• We can use or share your information for health research.
Comply with the law	• We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.
Respond to organ and tissue donation requests	• We can share health information about you with organ procurement organizations.
Work with a medical examiner or funeral director	• We can share health information with a coroner, medical examiner, or funeral director when an individual dies.
Address workers' compensation, law enforcement, and other government requests	• We can use or share health information about you: • For workers' compensation claims • For law enforcement purposes or with a law enforcement official • With health oversight agencies for activities authorized by law • For special government functions such as military, national security, and presidential protective services
Respond to lawsuits and legal actions	• We can share health information about you in response to a court or administrative order, or in response to a subpoena.
Substance Abuse Disorders" (for federally assisted programs that provide substance use diagnosis, treatment, or <u>referral for treatment</u>)	• Patients can allow a single consent for redisclosures for treatment, payment, and healthcare operations (TPO), but the purpose for these must be noted. • Separate consents must be issued for the following: redisclosure for law enforcement investigations, legal proceedings/prosecutions, and counseling notes. • The Amended HIPAA Privacy Rule (finalized 2/8/2024) simplified the consent process by allowing a single consent for future healthcare operations (TPO) uses, until the patient revokes consent in writing. • Now, upon a breach of Substance Use Disorder (SUD) records, patients must be notified.

continued on next page

Reproductive rights

- We can share health information involving reproductive health when
 - If we need to defend ourselves in an investigation or proceeding regarding professional misconduct or negligence involved in providing reproductive healthcare.
 - If we need to defend any person in any criminal, civil, or administrative proceeding when liability could be imposed on said person for providing reproductive healthcare.
 - When PHI is used to conduct audits by an Inspector General.
 - We can NOT share your health information when
 - If PHI is to be used to conduct criminal, civil, or administrative liability for seeking, obtaining, providing, or facilitating reproductive health care, when said health care is lawful under the circumstances in which it was provided.
 - If the PHI is to identify any person for the purpose of conducting such investigation or imposing liability.
 - An attestation will be required when a request for PHI is potentially related to reproductive health care. This applies to requests for health oversight activities, judicial and administrative proceedings, law enforcement purposes, and disclosures to coroners and medical examiners.
-

Instruction C: Insert any special notes that apply to your entity's practices such as "we do not create or manage a hospital directory" or "we do not create or maintain psychotherapy notes at this practice."

Instruction D: The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.

Instruction E: If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.

To leave this section blank, add a word space to delete the instructions.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of This Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Instruction F: Insert Effective Date of Notice here.

This Notice of Privacy Practices applies to the following organizations.

Instruction G: If your entity is part of an OHCA (organized health care arrangement) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment, and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."

Instruction H: Insert name or title of the privacy official (or other privacy contact) and his/her email address and phone number.

SAMPLE CONDENSED NOTOCE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used or disclosed, as well as how you can access this information. **Please review it carefully.**

Your Rights

- The ability to obtain a copy of your medical records (within 30 calendar days with all required documentation provided).
- To request your medical records be amended. Any denials will be sent in writing within 60 days.
- Request confidential communications (i.e. which phone number & reasonable options).
- Ask for limitations in what we share for treatment, payment, or our operations.
- Obtain a list of those with whom we have shared your information.
- To obtain a copy of this privacy notice.
- Choose someone to act on your behalf.
- File a complaint if you feel these rights have been violated.

Your Choices (with certain information)

- Whether certain people involved in your care can have information shared to them.
- Sharing information in a disaster relief situation, include it in a hospital directory, and/or contact you for fundraising efforts (we may contact you, but you can tell us not to contact you again)
- We will NEVER share without your permission: for marketing, sale of your information, and most sharing of psychotherapy notes.

Our Uses and Disclosures

- Your health information will be used to treat you, coordinate your care, run and improve our practice/care, and bill for services.
- Public Health and Safety situations regarding preventing disease, product recalls, adverse reactions to medications, preventing serious threats to health or safety, and reported suspected abuse/neglect/domestic violence.
- For research purposes.
- To comply with state or federal laws or to respond to subpoenas or court/administrative orders.
- Responding to organ donor and tissue donation requests.
- Sharing information with coroners, medical examiners, and funeral directors.
- Reproductive Health related records can be disclosed when needing to protect our organization or any person in providing reproductive care. We can NOT disclose your information for any type of civil, criminal, administrative investigations when said healthcare was obtained under lawful circumstances.
- Substance Abuse Disorder (SUD) patients can opt to use a single consent for redisclosures for treatment, payment, and healthcare operations (TPO), but the purpose for disclosures must be noted with their consent.
 - Separate consents must be issued for the following: redisclosure for law enforcement investigations, legal proceedings/prosecutions, and counseling notes.
- The Amended HIPAA Privacy Rule (finalized 2/8/2024) simplified the consent process by allowing a single consent for future healthcare operations (TPO) uses, until the patient revokes consent in writing.
- Now, upon a breach of Substance Use Disorder (SUD) records, patients must be notified.

Our Responsibilities

- We are required to maintain the privacy and security of your Protected Health Information.
- To follow the duties/privacy practices in this notice & provide you a copy of it.
- We will not disclose information mentioned here unless permission is given, and that permission can be revoked.
- Any future changes to this notice will available upon request.

Model Attestation Regarding a Requested Use or Disclosure of Protected Health
Information Potentially Related to Reproductive Health Care

Entire form is required to be completed for attestation to be valid.

Name of person(s), or the specific identification of the class of person(s), to receive the requested PHI.

Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure.

Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting.

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

- ☐ The purpose of the use or disclosure of protected health information is **not** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.
- ☐ The purpose of the use or disclosure of protected health information is to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was **not lawful** under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person

Signature of Requestor

Date

If you have signed as a representative of the person requesting PHI, provide a description of your authority to act for that person.

Telehealth Policy

Statement of Policy

[Company Name] is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, [Company Name] is required to safeguard Electronic Protected Health Information (ePHI) in accordance with the HIPAA Security Rule Regulations. These policies reflect the organization's commitment to comply with such Regulations and their commitment to safeguarding PHI/ePHI.

Purpose of Policy

The purpose of the Telehealth Policy is to ensure that all employees of [Company Name] are adhering to the standards of the HIPAA Security and Privacy regulations.

Definition

The Department of Health and Human Services defines telehealth as "the use of electronic information and telecommunications technologies to support and promote long distance clinical health care, patient and professional health-related education, and public health/health administration." The technology involved with telehealth would be video conferencing, the internet, landline, and wireless communications.

Procedure

1. Information exchange - encryption must be used when sending any correspondence that includes Protected Health Information (PHI/ePHI). Safeguarded methods, like requesting encryption, must also be requested from parties sending any correspondence containing PHI/ePHI to [Company Name] or any of its employees.
2. Telehealth meetings – private settings will be used for both parties when meeting in a telehealth setting. Both parties should be in a location where they cannot be seen or heard by an outside party. If this is not possible for the patient/client, "reasonable precautions" must be taken. Reasonable precautions include, but are not limited to, lowered voices, use of earphones, and the patient /client physically distancing from outside parties. If using video conferencing, it should be a non-public facing method of video communication.
 - a. Verification of identity – any individual not known to a covered entity, must have their identity verified either orally or in writing.
 - b. Non-public facing communications – platforms that typically utilize end-to-end encryption and support individual user accounts/logins/passcodes (e.g. Zoom, Skype, FaceTime).
 - i. Best practice is the use of a service provider that adheres to HIPAA guidelines, has increased capability to protect PHI, and provides a Business Associate Agreement (BAA).

- ii. Unacceptable methods of telehealth communications would be public-facing communications (some examples being TikTok, Facebook Live, Twitch) and would be considered a breach.
- 3. In addition, all HIPAA Security and Privacy regulations should be abided by while practicing any form of telehealth service.

Creation Date: 04/17/2023

Effective Date: 04/17/2023

Last Revision Date:

Telehealth FAQs

What is telehealth?

- The Department of Health and Human Services defines telehealth as “the use of electronic information and telecommunications technologies to support and promote long distance clinical health care, patient and professional health-related education, and public health/health administration.” The technology involved with telehealth would be video conferencing, the internet, landline, and wireless communications.

Do I have to verify the identity of new clients?

- Yes, the Office of Civil Rights released HHS guidance on 6/13/2022, which noted that if a client is not known to the provider, all covered entities must verify the identity of the individual orally or in writing.

How do I get paperwork to my telehealth client?

- Make sure you are sending documents to and from clients using encryption. In all areas, it is best to use whatever encryption and privacy options that are available to you.

Are there recommendations for where services should take place?

- Practitioners should continue to use private settings, like an office. If using a home office, make sure nobody can intentionally/unintentionally see PHI or a client. Private settings should be used **FOR ALL PARTIES**. If not possible, “reasonable precautions” must be taken (i.e., lowered voices, earphones, and the patient/client moving away from other people).

Do I need a specific video service to provide telehealth services?

- HIPAA states “non-public facing” remote communications must be used. Some examples would include Zoom, Microsoft Teams, Apple FaceTime, Facebook Messenger video chat. These are acceptable because these platforms support accounts for individual users, and the accounts, passwords, and logins offer a degree of control over who can access them. Public-facing products (i.e., TikTok, Facebook Live, or chat rooms). While it may be obvious to not use these for one-on-one services, a practitioner also should make sure not to use them for presentations because all viewers would be able to access some level of information about other patients. Best practice: use a video service that adheres to HIPAA Security rules. These providers have increased capability to protect your PHI, and typically provide a BAA.

Are there any non-privacy related limitations to using telehealth?

- Medicare has regulations about billing and telehealth. Information specifically about telehealth and Medicare is available at <https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet>

and <https://edit.cms.gov/files/document/medicare-telehealth-frequently-asked-questions-faqs-31720.pdf> - PDF.

What is the Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency?

- The Department of Health and Human Services (HHS) will be exercising discretion in how it applies Privacy, Breach, and Security Notification Rules under HIPAA. The HHS Office of Civil Rights (OCR) won't be imposing penalties for the noncompliance of HIPAA rules against covered providers in connection with good faith provision of telehealth during the COVID-19 public health emergency. It is important to remember that this does not apply to areas outside of telehealth during the emergency.

What is not covered by the Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency?

- A covered provider's bad faith in providing telehealth. Some examples are using public-facing remote communications products (TikTok, live streaming, etc.), using data/PHI for marketing, selling data, ethical violations or state licensing law violations that result in disciplinary action, and any criminal act or fraudulent activity.

What services can be provided via telehealth during the public health emergency?

- Providers will use their professional judgement to determine what telehealth services are appropriate during our current health emergency. The HHS specifies "diagnosis or treatment of COVID-19 related conditions, such as taking a patient's temperature or other vitals remotely, and diagnosis or treatment of non-COVID-19 related conditions, such as review of physical therapy practices, mental health counseling, or adjustment of prescriptions, among many others."