Workforce Member Sanctions Policies and Procedures

- §164.308(a)(1)(ii)(C)

164.308(a)(1)(ii)(C): Implementation Specification: Sanction Policy (Required). ***Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.***

[Company name] is to ensure that the subsequent Workforce Members Sanctions policies and procedures contained within the HIPAA Information Security Policies and Procedures Manual – and other supporting documentation – are in place and implemented to assist in implementing procedures to apply appropriate sanction against workforce members who fail to comply with the preceding and subsequent security policies contained within the HIPAA Information Security Policies and Procedures Manual. The confidentiality, integrity, availability (CIA) of PHI is highly dependent upon the use and application of well-documented information security and operational specific policies, procedures, and related processes.

Protected Health Information
Ensuring the safety and security of Protected Health Information (PHI) is one of the most critical components of compliance with the Health Insurance Portability and Accountability Act (HIPPA). With today's increasing reliance on information technology for all types of healthcare related procedures, PHI must be safeguarded at all times, both in electronic format and hard-copy, paper based documents. As for what constitutes PHI, it is consists of the following:

- Names.
- All geographical identifiers smaller than a state.
- Dates that directly relate to an individual (other than year).
- Phone Numbers.
- Fax Numbers.
- Email Addresses.
- Social Security Numbers.
- Medical Record Numbers.
- Health Insurance Beneficiary Numbers.
- Account Numbers.
- Certificate | License Numbers.
- VIN, serial numbers, license plate numbers.
- Device Identifiers and Serial Numbers.
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) addresses.
- Biometric Identifiers, such as finger, retinal and voice.
- Full Face Photograph Images
- Any other unique identifying number, character, code, etc.

Unacceptable Uses of PHI
As such, any misuse, abuse, and harmful activities that result in PHI being compromised will not be tolerated at any time by [company name], and will result in necessary sanctions being taken against such

individuals. More specifically, the unauthorized access, use, and/or disclosure of Protected Health Information (PHI) is a serious issue, one that will be aggressively enforced at all times by authorized personnel within [company name] consisting of reprimanding, suspending and/or terminating such individuals. Accessing PHI is a privilege, one granted to select users for performing his | her respective job functions, thus all necessary security safeguards are to be implemented at all times for protecting highly sensitive and confidential data.

Thus, any action resulting from the unauthorized access, use and disclosure of PHI that may potentially compromise the organization's network infrastructure, cause harm to other related systems, cause harm or pose a significant financial, operational, or business threat to the organization because of inappropriate and unacceptable access, use, and disclosure of PHI, will result in swift sanctions to be applied to such individuals.

The following Levels are to be assessed against employees regarding unauthorized access, use, and disclosure of PHI:

Level 1: Mistaken | Accidental Access, Use, and/or Disclosure of PHI

- **Level 1 Violation:** Any employee or other applicable user who mistakenly accesses, uses, and/or discloses PHI. This may range from accidentally accessing electronic and/or hard-copy PHI data, such as computer records, paper records, etc.
- **Level 1 Reprimand:** Written warning, along with undertaking HIPAA specific security awareness training procedures within fourteen (14) days of the reported violation. Please note that multiple instances of Level 1 violations will result in reprimanding, suspending and/or terminating such individuals.
- **Note:** Accident do happen, and [company name] is understanding of such issues, but also the need for ensuring all employees know what information they can and cannot access.

Level 2: Careless Access, Use, and/or Disclosure of PHI

- **Level 2 Violation:** Any employee or other applicable user who carelessly accesses, uses, and/or discloses PHI. This may range from leaving PHI unprotected in a public venue, not locking down your workstation, etc.
- **Level 2 Reprimand:** Written warning, along with undertaking HIPAA specific security awareness training procedures within seven (7) days of the reported violation. Please note that multiple instances of Level 2 violations will result in reprimanding, suspending and/or terminating such individuals.
- **Note:** Carelessness in the workplace, especially regarding the access, use, and/or disclosure of PHI, will not be tolerated at any time, thus the importance of ensuring the safety and security of PHI is critical at all times. Access to PHI is a privilege, one for which all employees must take seriously.

Level 3: Deliberate and Intentional Access, Use, and/or Disclosure of PHI

- **Level 3 Violation:** Any employee or other applicable user who deliberately and intentionally accesses, uses, and/or discloses PHI. This may range from knowingly accessing electronic and/or hard-copy PHI data, such as computer records, paper records, etc.

- **Level 3 Reprimand:** Immediate termination, with no exceptions, unless in the interest of national security.
- **Note:** Deliberate and intentional access, use, and/or disclosure of PHI, will not be tolerated at any time, ultimately resulting in the immediate termination of such individuals.

It's important that all employees and other workforce members are aware of the sanctions that can be imposed on them for unintentionally, carelessly, or deliberately accessing, using, and/or disclosing PHI. The safety and security of consumer information is of the utmost priority for the organization, thus [company name] will enforce such sanctions aggressively.

Note: The aforementioned policies and supporting procedures regarding an organization's "Workforce Members Sanctions" initiatives are a mandate for HIPAA compliance. Please modify the above language as necessary to reflect any specific changes you would like to make. The above information serves as best practices derived from years of regulatory compliance experience and first-hand knowledge. PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.

Information Security Cross-Reference Matrix

HIPAA Security Rule	Organizational Source Document(s) that Cover and/or Include Provisions for the stated HIPAA Security Rule
164.308(a)(1)(ii)(C): Implementation Specification: Sanction Policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	(1).
	(2).
	(3).

Note: In today's world of regulatory compliance, organizations often have numerous sets of various information security policies and procedures, and many of the mandates [for purposes of information security] often overlap one another. It's thus important to "cross-reference" the above listed HIPAA requirements with any additional documentation one may have as this helps provide clarity as to where the information is located, etc.

PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.

Information System Activity Review Policies and Procedures

- §164.308(a)(1)(ii)(D)

164.308(a)(1)(ii)(D): Implementation Specification: Information system activity review (Required). ***Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.***

[Company name] is to ensure that the subsequent Information System Activity Review policies and procedures contained within the HIPAA Information Security Policies and Procedures Manual – and other supporting documentation – are in place for implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports for information systems that store, process, and/or transmit Protected Health Information (PHI) – or any other related sensitive and confidential healthcare data. The confidentiality, integrity, availability (CIA) of PHI is highly dependent upon the use and application of well-documented information security and operational specific policies, procedures, and related processes.

Audit Logs and Access Reports
Effective protocols and supporting measures are to be implemented for ensuring all required events and their associated attributes for information systems (systems) that store, process, and/or transmit Protected Health Information (PHI) – or any other related sensitive and confidential healthcare data – are logged, recorded, and reviewed as necessary.

Additionally, all applicable elevated permissions (those for administrators) along with general access rights permissions (those for end-users) to such systems are to be reviewed on a [monthly/quarterly/bi-annual/annual] basis by an authority that is independent from all known users (i.e., end-users, administrator, etc.) and who also has the ability to understand, interpret, and ultimately identify any issues or concerns from the related output (i.e., log reports, and other supporting data). The specified authority reviewing the logs is to determine what constitutes any "issues or concerns", and to report them immediately to appropriate personnel.

Moreover, protocols such as syslog and other capturing and forwarding protocols and, or technology, such as specialized software applications, are to be used as necessary, along with employing security measures that protect the confidentiality, integrity, and availability (CIA) of the audit trails and their respective log reports (i.e., audit records) that are produced.

Additionally, all audit records are to be stored on an external log server (i.e., centralized syslog server or similar platform) that is physically separated from the original data source, along with employing effective backup and archival procedures for the log server itself. These measures allow [company name] to secure the audit records as required for various HIPAA specific legal and regulatory compliance mandates, along with conducting forensic investigative procedures if necessary.

Incident Tracking Reports
Data breaches, cyber security threats, and many other malicious exploits are growing more frequently and with greater severity in society, ultimately requiring comprehensive security measures for helping ensure the confidentiality, integrity, and availability (CIA) of [company name]'s information systems landscape.

Unfortunately, security breaches can happen - even with the best controls in place - thus the ability to respond swiftly and effectively, along with regularly reviewing records of incident tracking reports, helps in mitigating and properly planning for security issues.

Knowing what threats have occurred, how the exploits were undertaken, along with any other relevant information, is critical to ensuring the safety and security of [company name]'s information system landscape, specifically that of PHI.

Note: The aforementioned policies and supporting procedures regarding an organization's "Information Systems Activity Review" initiatives are a mandate for HIPAA compliance. Please modify the above language as necessary to reflect any specific changes you would like to make. The above information serves as best practices derived from years of regulatory compliance experience and first-hand knowledge. PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.

Information Security Cross-Reference Matrix

HIPAA Security Rule	Organizational Source Document(s) that Cover and/or Include Provisions for the stated HIPAA Security Rule
164.308(a)(1)(ii)(D): Implementation Specification: Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	(1).
	(2).
	(3).

Note: In today's world of regulatory compliance, organizations often have numerous sets of various information security policies and procedures, and many of the mandates [for purposes of information security] often overlap one another. It's thus important to "cross-reference" the above listed HIPAA requirements with any additional documentation one may have as this helps provide clarity as to where the information is located, etc.

PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.

Assigned Security Responsibility Policies and Procedures

- §164.308(a)(2)

164.308(a)(2): Standard: Assigned security responsibility. ***Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.***

In accordance with HIPAA, [company name] is to *identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate*. The following roles and responsibilities with [company name] are to be formalized and subsequently assigned to authorized personnel within [company name] regarding information systems (systems) that store, process, and/or transmit Protected Health Information (PHI) – or any other related sensitive and confidential healthcare data:

- **Chief Technology Officer (CTO) | Chief Information Officer (CIO):** Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The CTO | CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.

- **Director of Information Technology | Senior Information Security Officer**: Responsibilities include also providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations, along with researching and developing information security standards for the organization as a whole. This will require extensive identification of industry benchmarks, standards, and frameworks that can be effectively utilized by the organization for provisioning, hardening, securing, and locking-down critical system components. Subsequent to the researching of such standards, the senior security officer is to then oversee the establishment of a series of baseline configuration standards to include, but limited to, the following system components: network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms. Because baseline configuration can and will change, this authorized individual is to also update the applicable configurations, documenting all modifications and enhancements as required. Additional duties of the **Director of Information Technology | Senior Information Security Officer include the following:**

    - Responsible for all major facets of information technology throughout the organization, such as management, recommendations as necessary.
    - Providing leadership, direction and guidance for current and existing projects.
    - Overseeing the development of all applicable operational, business specific, and information security policies, procedures, forms, checklists, templates, provisioning and hardening documents and other necessary material.
    - Overseeing initiative for developing internal Requests for Proposals (RFPs), along with answering RFP's for services from the organization.

- Assistance in developing annual information technology budget.
- Displaying integrity, honesty, and independence at all times.
- Supporting the Director of Information Technology | Senior Information Security Officer and other members of senior management as necessary.

- **HIPAA Security Official:** Responsibilities include also providing overall direction, guidance, leadership and support for information systems (systems) that store, process, and/or transmit Protected Health Information (PHI) – or any other related sensitive and confidential healthcare data. Additionally, responsibilities include researching, authoring, refining, publishing, and maintaining all [company name] HIPAA specific information security policies, procedures, and other supporting documentation. Additionally, the HIPAA Security Official is to actively communicate with all other I.T. and operational personnel as necessary for ensuring the policies and stated procedures are implemented and adhered to.

- **Network Engineer | Systems Administrator:** Responsibilities include actually implementing the baseline configuration standards for all in-scope system components. This requires obtaining a current and accurate asset inventory of all such systems, assessing their initial posture with the stated baseline, and the undertaking the necessary configurations. Because of the complexities and depth often involved with such activities, numerous personnel designated as Network Engineers | System Administrators are often involved in such activities.

  Furthermore, these individuals are also responsible for monitoring compliance with the stated baseline configuration standards, reporting to senior management all instances of non-compliance and efforts undertaken to correct such issues. Additionally, due to the fact that these individuals are to undertake the majority of the operational and technical procedures for the organization, it is critical to highlight other relevant duties, such as the following:

  - Assessing and analyzing baseline configuration standards for ensuring they meet the intent and rigor for the overall safety and security (both logically and physically) of critical system components.
  - Ensuring the asset inventory for all in-scope system components is in fact kept current and accurate.
  - Ensuring that network topology documents are also kept current and accurate.
  - Facilitating requests for validation of baseline configurations for purposes of regulatory compliance assessments and audits – such as those for PCI compliance, SSAE 16 reporting, HIPAA, FISMA, GLBA, etc.
  - Continuous training and certification accreditation for purposes of maintaining an acceptable level of information security expertise necessary for configuration management.

  Additional duties of **Network Engineers | Systems Administrators include the following:**

  - Establishing networking environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards.

- Optimizing network performance by monitoring performance; troubleshooting network problems and outages; scheduling upgrades; collaborating with network architects on network optimization.
- Updating job knowledge by participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.
- Securing network system by establishing and enforcing policies; defining and monitoring access.
- Reporting network operational status by gathering, prioritizing information; managing projects.

- **Software Developers | Coders:** Responsibilities include actually developing secure systems by implementing the required baseline configuration standards into all systems and software development lifecycle activities. Coding for security, not functionality, is a core theme for which all software developers | coders are to adhere to. They are to also identify any other necessary baseline configuration standards when warranted. Ultimately, this requires removing, disabling, and not implementing insecure services, protocols, or ports that – while may be conducive for purposes of ease-of-use – ultimately compromise the applicable systems being developed.

  Additionally, these personnel are also responsible for following a structured project management framework, one that includes utilizing a documented SDLC process, complete with well-defined change management policies, processes, and procedures. Moreover, these personnel are to support and coordinate all required requests for validation of the baseline configurations within their systems being developed for purposes of regulatory compliance and/or internal audit assessments.

  Additional duties of **Software Developers | Coders include the following:**

  - Developing software solutions by studying information needs; conferring with users; studying systems flow, data usage, and work processes; investigating problem areas; following the software development lifecycle.
  - Determining operational feasibility by evaluating analysis, problem definition, requirements, solution development, and proposed solutions.
  - Effective documentation via flowcharts, layouts, diagrams, charts, code comments and clear code.
  - Preparing and installing solutions by effectively designing system specifications, standards, and programming.
  - Improving operations by conducting systems analysis; recommending changes in policies and procedures.
  - Obtaining and licensing software from vendors.

- **Change Management | Change Control Personnel:** Responsibilities include reviewing, approving, and/or denying all changes to critical system components and specifically for purposes of any changes to the various baseline configuration standards. While changes are often associated with user functionality, many times the issue of vulnerability, patch, and configuration management are brought to light with change requests. In such cases, authorized change management | change

control personnel are to extensively analyze and assess these issues for ensuring the safety and security of organizational-wide system components.

- **End Users:** Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such [company name] system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of [company name] system components, and are to also report such instance immediately to senior authorities.

- **Vendors, Contractors, Other Third-Party Entities:** Responsibilities for such individuals and organization are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

Note: The aforementioned policies and supporting procedures regarding an organization's "Assigned Security Responsibility" initiatives are a mandate for HIPAA compliance. Please modify the above language as necessary to reflect any specific changes you would like to make. The above information serves as best practices derived from years of regulatory compliance experience and first-hand knowledge. More specifically, the above listed titles and functions serves as an excellent example of the various roles and responsibilities that every organization should have in place regarding critical I.T. and compliance personnel, starting with a CTO | CIO, and all the way down to end-users. PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.

Information Security Cross-Reference Matrix

HIPAA Security Rule	Organizational Source Document(s) that Cover and/or Include Provisions for the stated HIPAA Security Rule
164.308(a)(2): Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	(1).
	(2).
	(3).

Note: In today's world of regulatory compliance, organizations often have numerous sets of various information security policies and procedures, and many of the mandates [for purposes of information security] often overlap one another. It's thus important to "cross-reference" the above listed HIPAA requirements with any additional documentation one may have as this helps provide clarity as to where the information is located, etc.

PLEASE DELETE THIS SECTION IN RED, AS THIS HAS BEEN PROVIDED AS REFERENCE MATERIAL ONLY.