HIPAA POLICIES AND PROCEDURES

|  |  |  |
| --- | --- | --- |
| **Policy Title:**  Security Management Root Process **ID: SecurityManagementRootProcess06302015**  **Revision: 0.82** | | **Approval Date:**  00/00/0000  **Effective Date:** 00/00/0000  **Revisited date:** 00/00/0000 |
| **Subject:** Risk analysis, management and compliance root policy | | |
| **Primary Responsible Departments and/or BAA:**  Security / Compliance | | **Review Frequency:** Anually  **Last Review:** 00/00/0000  **Next Review:** 00/00/0000 |
| **Secondary Responsible Departments and/or BAA:** IT / Administration / Workforce / BAAs | |

**Scope:**

All Workforce and Visitors; Google BAA and other BAA’s

**Purpose:**  
Create a standard policy framework for risk analysis and handling of personal health information (PHI) and electronic personal health information (EPHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Regulations and the 2010 HI-TECH expansion of the regulatory code as administered and guided by Human Health and Services(HHS); The Office of Civil Right(OCR); The National Institute of Standards and Technology(NIST); Google’s guidance on proper HIPAA implementation safeguards; and in accordance all other applicable laws and regulations; and our own policies.   
  
This root policy framework incorporates a Google Business Associate Agreement (BAA) and this covered entity (CE) such that information properly transacted within properly administered Google is handled and documented properly. PHI and EPHI outside the Google BAA or brought into the Google BAA via a creation process that extends beyond the Google BAA covered tools must be documented in full and incorporated into this policy framework to maintain compliance.

**Authoritative Reference:**

45 CFR §164.308(a)(1)(ii)(A)   
NIST Special Publication (SP) 800-30

**Policy Definitions:**

1. **Risk Analysis -** Risks are the sum of vulnerabilities and threats and should be prioritized and responded to by the Chief Compliance Agent in the order in which they present the greatest overall impact as determined by the Chief Compliance Agent and in accordance with these policies and in compliance with all applicable law and regulations.
   1. **Vulnerability** - Vulnerability is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.” Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.
   2. **Threat -** An adapted definition of threat, from NIST SP 800-30, is “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.” Threats may be grouped into general categories such as human and environmental. Examples of common threats in each of these general categories include: Natural threats such as floods, earthquakes, tornadoes, and landslides. Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
   3. **Risk**: An adapted definition of risk, from NIST SP 800-30, is: “The net mission impact considering:

(1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and

(2) the resulting impact if this should occur . . . .

[R]isks arise from legal liability or mission loss due to—

1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information

2. Unintentional errors and omissions

3. IT disruptions due to natural or man-made disasters

4. Failure to exercise due care and diligence in the implementation and operation of the IT system.” Risk can be understood as a function of

1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and

2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

**2. Risk Management** - As a covered entity under HIPAA and in accordance with these policies we must:

1. Maintain the integrity, confidentiality, and availability of all PHI and EPHI we create, receive, transmit or otherwise interact with (§164.306(a)(1)).
2. Protect against reasonably anticipated threats or risks to the security, integrity, and accessibility of the PHI/EPHI we interact with (§164.306(a)(2)).
3. Protect against reasonably anticipated unnecessary use or disclosure of PHI/EPHI(§164.306(a)(3)).
4. Ensure workforce compliance with this subpart (§164.306(a)(4) / 5(d)) and maintain and monitor compliance with these security regulations and policies such that we have all appropriate:
   1. **Administrative Safeguards**: Policies and procedures to manage the creation, development, implementation, maintenance, monitoring and training required for systems accessing, storing, transmitting or otherwise interacting with PHI and EPHI and limiting PHI to the minimum necessary to accomplish the intended purpose. This Includes the process for the formulation of new policies and procedures extending the scope of this framework.
   2. **Physical Safeguards**: Policies and procedures to control, secure and monitor electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion PHI and EPHI meets the integrity, confidentiality and accessibility standards of HIPAA and these policies.
   3. **Technical Safeguards**: Policies and procedures to ensure the accessing, storing, transmitting or otherwise interacting with PHI and EPHI meets the integrity, confidentiality and accessibility standards of HIPAA and these policies.

**3. Violations and Sanction Policy -** The sanction process shall meet the HIPAA regulatory standards and initial policy and procedures will rest with the chief security agent.Sanctions may include, but are not limited to:

a. Warnings (oral and written)

b. Suspension or limitation of access to information PHI and EPHI systems

c. (Re)Training and Development

d. Letter of warning

e. Suspension

f. Termination

**4. Information System Activity Review**  - The review process must meet the administratively feasible HIPAA standards. Control over the the policy, procedure and review process rests with the chief security agent responsible for policy compliance initially. All additional audited activity and review is incorporated and compliance detailed under the associated Google BAA.

**Related Policies and Procedures:**

**Administrative Safeguards**:

**Security Management Process** § **164.308(a)(1)**

**Assigned Security Responsibility** § **164.308(a)(2)**

**Workforce Security** § **164.308(a)(3)**

**Information Access Management** § **164.308(a)(4)**

**Security Awareness and Training** § **164.308(a)(5)**

**Security Incident Procedures** § **164.308(a)(6)**

**Contingency Plan** § **164.308(a)(7)**

**Evaluation** § **164.308(a)(8)**

**Business Associate Contracts and Other Arrangements** § 164.308(b)  
 **Google BAA**

**Physical Safeguards**:   
 **Facility Access Controls § 164.310(a)(1)**

**Device and Media Controls 164.310(d)(1)**

**Technical Safeguards**:

**Access Control Policy § 164.308(a)(4)**

Unique User Identification § 164.312(a)(1)

Passwords §164.312(a)(1) & (2)

Emergency Access Procedure §164.312(a)(2)(ii)

Automatic Logoff § 164.312(a)(2)(iii)

Encryption and Decryption - § 164.304 and § 164.312(a)(2)(iiii)   
**Workstation Use § 164.310(b)**

**Workstation Security § 164.310(c)**

**Audit Controls § 164.312(b)  
Information Integrity § 164.312(c)(1)**

**Authentication § 164.312(d)**

**Transmission Security § 164.312(e)(1)**

**Related Documents:**

**Administrative:**

HIPAA Security Management Root Process

HIPAA Assigned Security Responsibility  
HIPAA Workforce Security

HIPAA Information Access Management

HIPAA Security Awareness and Training

HIPAA Security Incident Procedures

HIPAA Contingency Plan

HIPAA Evaluation

**Physical:**

HIPAA Device and Media Control Policy

HIPAA Facility Access Control Policy

**Technical:**

HIPAA Access Control Policy

HIPAA Audit Policy

HIPAA Authentication Policy

HIPAA Workstation Use Policy

HIPAA Workstation Security Policy

HIPAA Information Integrity Policy

HIPAA Transmission Security Policy

**BAA’s and Other Agreements:**

HIPAA Business Associate and Other Agreement Policy  
Google BAA

**Templates:**

Policy Template

Procedure Template   
 Incident Template

**Additional Reference and Guidance Materials:**

[**HIPAA Administrative Simplification [45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013)]**](http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf)

[**Office of Civil Rights (OCR) Guidance - HIPAA Security SERIES**](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html) [**HIPAA Compliance & Data Protection with Google Apps Google Apps for Work HIPAA implementation guide**](https://www.google.com/work/apps/terms/2015/1/hipaa_implementation_guide.pdf)

[**OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule**](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf)