|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***HIPAA Integrity*®**  **&**  ***CFR***  **Codes for Security Rule Safeguards** | **Administrative**  **Safeguard Standards** | **Administrative Safeguard Implementation Specifications** | ***HIPAA Integrity*®**  **Forms (F) for Administrative Safeguards** | ***HIPAA Integrity*®**  **Administrative Safeguard Policies and Procedures in Word Format** | **Pages** |
|  | Table of Contents |  |  |  | 1-2 |
|  |  |  |  |  |  |
| ***Security Rule (SR)***  ***Administrative Safeguards (AS)***  SR AS 0  45 CFR 164.308(a) | Introduction to Administrative Safeguard Standards |  |  |  |  |
| SR AS 1.0  45 CFR 164.308(a)(1)(i) | Security Management Process |  |  |  |  |
| SR AS 1.1  45 CFR 164.308(a)(1)(ii)(A) |  | Risk Analysis (R) | *HIPAA Integrity*  Risk Analysis  Template  (Form separate from SR, AS.1.1) | Risk Analysis (R) | 8-9 |
| SR AS 1.2  45 CFR 164.308(a)(1)(ii)(B) |  | Risk Management (R) | 1.2.F: Risk Analysis Report Log | Risk Management (R) | 10 |
| SR AS 1.3  45 CFR 164.308(a)(1)(ii)(C) |  | Sanction Policy (R) | 1.3.F: Workforce Member Sanctions Policy Acknowledgement | Sanction Policy (R) | 11 |
| SR AS 1.4  45 CFR 164.308(a)(1)(ii)(D) |  | Information System Activity Review (R) |  | Information System Activity Review (R) | 12 |
| SR AS 2.0  45 CFR 164.308(a)(2) | Assigned Security Responsibility |  | 2.0.F: Security Safeguard Complaint Log | Assigned Security Responsibility | 13 |
| SR AS 3.0  45 CFR 164.308(a)(3)(i) | Workforce Security |  |  |  |  |
| SR AS 3.1  45 CFR 164.308(a)(3)(ii)(A) |  | Authorization and/or Supervision (A) | 3.1.F1: Workforce Member Authorization Acknowledgement;  3.1.F2: Stationary Hardware Assignment and Encryption Log | Authorization and/or Supervision (A) | 14 |
| SR AS 3.2  45 CFR 164.308(a)(3)(ii)(B) |  | Workforce Clearance Procedure (A) | 3.2.F: Workforce Member Background Check Log | Workforce Clearance Procedure (A) | 15 |
| SR AS 3.3  45 CFR 164.308(a)(3)(ii)(C) |  | Termination Procedures (A) | 3.3.F1: Workforce Member Exit Checklist;  3.3.F2: Workforce Member Exit Interview Acknowledgement | Termination Procedures (A) | 16 |
| SR AS 4.0  45 CFR 164.308(a)(4)(i) | Information Access Management |  |  |  |  |
| SR AS 4.1  45 CFR 164.308(a)(4)(ii)(A) |  | Isolating Health Care Clearinghouse Functions (R) |  | Isolating Health Care Clearinghouse Functions (R) | 17 |
| SR AS 4.2  45 CFR 164.308(a)(4)(ii)(B) |  | Access Authorization (A) |  | Access Authorization (A) | 18 |
| SR AS 4.3  45 CFR 164.308(a)(4)(ii)(C) |  | Access Establishment and Modification (A) | 4.3.F1: Workforce Member Right of Access Authorization Modification Acknowledgement;  4.3.F2: Workforce Member Right of Access Authorization Modification Log | Access Establishment and Modification (A) | 19 |
| SR AS 5.0  45 CFR 164.308(a)(5)(i) | Security Awareness and Training |  | 5.0.F: Security Safeguard Training for Workforce Members Log |  |  |
| SR AS 5.1  45 CFR 164.308(a)(5)(2)(A) |  | Security Reminders (A) |  | Security Reminders (A) | 20 |
| SR AS 5.2  45 CFR 164.308(a)(5)(2)(B) |  | Protection from Malicious Software (A) |  | Protection from Malicious Software (A) | 21 |
| SR AS 5.3  45 CFR 164.308(a)(5)(2)(C) |  | Log-in Monitoring (A) |  | Log-in Monitoring (A) | 22 |
| SR AS 5.4  45 CFR 164.308(a)(5)(2)(D) |  | Password Management (A) |  | Password Management (A) | 23 |
| SR AS 6.0  45 CFR 164.308(a)(6)(i) | Security Incident Procedures |  |  |  |  |
| SR AS 6.1  45 CFR 164.308(a)(6)(ii) |  | Response and Reporting (R) | 6.1.F: Security Incident Report Log | Response and Reporting (R) | 24 |
| SR AS 7.0  45 CFR 164.308(a)(7)(i) | Contingency Plan |  |  |  |  |
| SR AS 7.1  45 CFR 164.308(a)(7)(ii)(A) |  | Data Backup Plan (R) |  | Data Backup Plan (R) | 25 |
| SR AS 7.2  45 CFR 164.308(a)(7)(ii)(B) |  | Disaster Recovery Plan (R) |  | Disaster Recovery Plan (R) | 26 |
| SR AS 7.3  45 CFR 164.308(a)(7)(ii)(C) |  | Emergency Mode Operation Plan (R) |  | Emergency Mode Operation Plan (R) | 27 |
| SR AS 7.4  45 CFR 164.308(a)(7)(ii)(D) |  | Testing and Revision Procedures (A) |  | Testing and Revision Procedures (A) | 28 |
| SR AS 7.5  45 CFR 164.308(a)(7)(ii)(E) |  | Applications and Data Criticality Analysis (A) |  | Applications and Data Criticality Analysis (A) | 29 |
| SR AS 8.0  45 CFR 164.308(a)( | Evaluation |  |  | Evaluation | 30 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***HIPAA Integrity*®**  **&**  ***CFR***  **Codes**  **for**  **Security Rule Safeguards** | **Business Associate Contracts and Other Arrangements Standard** | **Business Associate Contracts and Other Arrangements Implementation Specification** | ***HIPAA Integrity*®**  **Form (F) for Business Associate Contracts and Other Arrangements** | **Business Associate Contracts and Other Arrangements Policies and Procedures in Word Format** | **Pages** |
|  | Table of Contents |  |  |  | 3 |
|  |  |  |  |  |  |
| ***Security Rule (SR)***  ***Business Associate (BA)***  SR BA 0  45 CFR 164.308(b)(1) & (2) | Introduction to & Requirements for Business Associate Contractors and Subcontractors |  |  |  |  |
| SR BA 1.0  45 CFR 164.308(b)(3) |  | Written Contract or Other Arrangement | 1.0.F: Business Associate Agreement Status Tracking Log | Written Contract or Other Arrangement | 31 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***HIPAA Integrity*®**  **&**  ***CFR***  **Codes for**  **Security Rule Safeguards** | **Physical**  **Safeguard Standards** | **Physical**  **Safeguard Implementation Specifications** | ***HIPAA Integrity*®**  **Forms (F) for Physical**  **Safeguards** | ***HIPAA Integrity*®**  **Physical Safeguard**  **Policies and Procedures in Word Format** | **Pages** |
|  | Table of Contents |  |  |  | 4-5 |
|  |  |  |  |  |  |
| ***Security Rule (SR)***  ***Physical Safeguards (PS)***  SR PS 0  45 CFR 164.310 | Introduction to Physical  Safeguard Standards |  |  |  |  |
| SR PS 1.0  45 CFR 164.310(a)(1) | Facility Access Controls |  |  |  |  |
| SR PS 1.1  45 CFR 164.310(a)(2)(i) |  | Contingency Operations (A) |  | Contingency Operations (A) | 32 |
| SR PS 1.2  45 CFR 164.310(a)(2)(ii) |  | Facility Security Plan (A) |  | Facility Security Plan (A) | 33 |
| SR PS 1.3  45 CFR 164.310(a)(2)(iii) |  | Access Control and Validation Procedures (A) |  | Access Control and Validation Procedures (A) | 34 |
| SR PS 1.4  45 CFR 164.310(a)(2)(iv) |  | Maintenance Records (A) | 1.4.F: Maintenance Record Log | Maintenance Records (A) | 35 |
| SR PS 2.0  45 CFR 164.310(b) | Workstation Use |  |  | Workstation Use | 36 |
| SR PS 3.0  45 CFR 164.310(c) | Workstation Security |  |  | Workstation Security | 37 |
| SR PS 4.0  45 CFR 164.310(d)(1) | Device and Media Controls |  |  |  |  |
| SR PS 4.1  45 CFR 164.310(d)(2)(i) |  | Disposal (R) | 4.1.F: Log for Disposal of Hard Copy and Electronic Media Containing Protected Health Information | Disposal (R) | 38 |
| SR PS 4.2  45 CFR 164.310(d)(2)(ii) |  | Media Re-use (R) | 4.2.F: Log for Removal of Protected Health Information on Electronic Media Before Re-use | Media Re-use (R) | 39 |
| SR PS 4.3  45 CFR 164.310(d)(2)(iii) |  | Accountability (A) | 4.3.F1: Log of Movements of Stationary Information Systems and Electronic Media  4.3.F2: Log of Use of Portable Electronic Media Outside of the Facility—Assignment and Encryption | Accountability (A) | 40 |
| SR PS 4.4  45 CFR 164.310(d)(2)(iv) |  | Data Backup and Storage (A) |  | Data Backup and Storage (A) | 41 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***HIPAA Integrity*®**  **&**  ***CFR***  **Codes for**  **Security Rule Safeguards** | **Technical**  **Safeguard Standards** | **Technical**  **Safeguard Implementation Specifications** | ***HIPAA Integrity*®**  **Forms (F) for Technical**  **Safeguards** | ***HIPAA Integrity*® Technical Safeguard**  **Policies and Procedures in Word Format** | **Pages** |
|  | Table of Contents |  |  |  | 6 |
|  |  |  |  |  |  |
| ***Security Rule (SR)***  ***Technical***  ***Safeguards (TS)***  SR TS 0  45 CFR 164.312 | Introduction |  |  |  |  |
| SR TS 1.0  45 CFR 164.312 | Access Control |  |  |  |  |
| SR TS 1.1  45 CFR 164.312 |  | Unique User Identification (R) |  | Unique User Identification (R) | 42 |
| SR TS 1.2  45 CFR 164.312 |  | Emergency Access Procedure (R) | 1.2.F: Emergency Access Log | Emergency Access Procedure (R) | 43 |
| SR TS 1.3  45 CFR 164.312 |  | Automatic Log-off (A) |  | Automatic Log-off (A) | 44 |
| SR TS 1.4  45 CFR 164.312 |  | Encryption and Decryption (*Data at Rest*) (A) | 1.4.F: *Data at Rest* Encryption Log | Encryption and Decryption (*Data at Rest*) (A) | 45 |
| SR TS 2.0  45 CFR 164.312 | Audit Controls |  |  | Audit Controls | 46 |
| SR TS 3.0  45 CFR 164.312 | Integrity |  |  |  |  |
| SR TS 3.1  45 CFR 164.312 |  | Mechanism to Authenticate Electronic Protected Health Information (A) |  | Mechanism to Authenticate Electronic Protected Health Information (A) | 47 |
| SR TS 4.0  45 CFR 164.312 | Person or Entity Authentication |  |  | Person or Entity Authentication | 48 |
| SR TS 5.0  45 CFR 164.312 | Transmission Security |  |  |  |  |
| SR TS 5.1  45 CFR 164.312 |  | Integrity Controls (A) |  | Integrity Controls (A) | 49 |
| SR TS 5.2  45 CFR 164.312 |  | Encryption (*Data in Motion*) (A) | 5.2.F: *Data in Motion* Encryption Log | Encryption (*Data in Motion*) (A) | 50 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***HIPAA Integrity*®**  **&**  ***CFR***  **Codes for**  **Security Rule Safeguards** | **Compliance Protocol**  **Standards** | **Compliance Protocol**  **Implementation Specifications** | **Compliance Protocol**  **Exhibits** | ***HIPAA Integrity*®**  **Compliance Protocol**  **Policies and Procedures in Word Format** | Pages |
|  | Table of Contents |  |  |  | 7 |
|  |  |  |  |  |  |
| ***Security Rule (SR)***  ***Compliance Protocols (CP)***  SR CP 0  45 CFR 164.316 | Introduction |  |  |  |  |
| SR CP 1.0  45 CFR 164.316(a) | Policies and Procedures |  |  | Policies and Procedures | 51 |
| SR CP 2.0  45 CFR 64.316(b)(1) | Documentation |  |  |  |  |
| SR CP 2.1  45 CFR 164.316(b)(2)(i) |  | Time Limit (R) |  | Time Limit (R) | 52 |
| SR CP 2.2  45 CFR 164.316(b)(2)(ii) |  | Availability (R) |  | Availability (R) | 53 |
| SR CP 2.3  45 CFR 164.316(b)(2)(iii) |  | Updates (R) |  | Updates (R) | 54 |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 1.1** | **45 CFR 164.308(a)(1)(ii)(A)** |
| **Key Activity**  Administrative Safeguards  **Security Management Process: Risk Analysis** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has conducted a *Risk Analysis* to assess potential risks and vulnerabilities to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information (ePHI), and has established policies and procedures based on findings from the risk analysis to safeguard the confidentiality, integrity, and availability of our organization’s ePHI. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with our organization’s *Risk Analysis* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process. For purposes of this implementation specification, we use the following definitions, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  Our workforce members are required to be trained on and comply with *Risk Analysis* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a *Risk Analysis* program for assessing, and mitigating through policies and procedures, potential risks and vulnerabilities to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI. Our risk analysis is based on nine National Institute of Standards and Technology (NIST) protocols that are the foundation for the *HIPAA Safeguard Risk Analysis Template* that is an exhibit to SR, AS.1.1. These protocols, which are included in NIST Special Publications (SP) 800-66 Revision 1 and 800-30 Revision 1 (see References), are:   1. Define the scope of the risk analysis of your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI. 2. Identify and compile relevant information pertaining to your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI. 3. Identify relevant threats to your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI.   A *threat* is “the potential for a person or thing to exercise (accidently trigger or intentionally exploit) a specific vulnerability.” [NIST SP 800-30 Revision 1]   1. Identify potential vulnerabilities in or related to your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI.   A *vulnerability* is “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidently triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.” [NIST SP 800-30 Revision 1]   1. Assess your organization’s current administrative, physical, and technical safeguards (security controls) in place to protect your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI. 2. Determine the likelihood and impact of any identified threat exercising a vulnerability that would affect your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI. 3. For each such potential occurrence, determine level(s) of risk to your organization’s electronic networks, systems, and applications, and stationary, portable, and mobile devices and media that contain ePHI. 4. Identify and recommend administrative, physical, and technical safeguards, as applicable, to mitigate such risk(s). [These safeguards are designated herein as: SR, AS. (Administrative); SR, PS. (Physical); and SR, TS. (Technical). 5. Document your organization’s risk analysis findings.   Our organization is aware of the importance of the risk analysis as the foundation of establishing administrative, physical, and technical policies and procedures to protect our organization’s ePHI, and of the need to periodically review and update the risk analysis in the event of regulatory or operational changes or a security incident or breach involving ePHI. Our Security Official is responsible for managing the *Risk Analysis* implementation specification (see SR, AS.2.0, *Assigned Security Responsibility* standard). | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 1.2** | **45 CFR 164.308(a)(1)(ii)(B)** |
| **Key Activity**  Administrative Safeguards  **Security Management Process: Risk Management** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has conducted a *Risk Analysis* to assess potential risks and vulnerabilities to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI, and, based on findings from its *Risk Analysis*, has established policies and procedures and implemented reasonable and appropriate *Risk Management* security measures to mitigate risks and vulnerabilities in compliance with the Security Rule *General Requirements* (45 CFR 164.306(a)):   * Ensure confidentiality, integrity, and availability of all electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits. * Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. * Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule. * Ensure compliance with the HIPAA Security Rule by the workforce.   Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with our organization’s *Risk Management* policies, procedures, and security measures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting *Risk Management* policies and procedures, implementing reasonable and appropriate security measures, and evaluating their effectiveness as part of our ongoing risk analysis process. For purposes of this implementation specification, we use the following definitions, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a *Risk Management* program for mitigating through policies and procedures, and reasonable and appropriate security controls, potential risks and vulnerabilities to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI, based on outcomes of our organization’s *Risk Analysis* (see SR, AS.1.1). Our Security Official is responsible for the *Risk Management* implementation specification (see SR, AS.2.0, *Assigned Security Responsibility* standard).  Our Security Official shall take into consideration the following *Flexibility of Approach* factors (45 CFR 164.306(b)) in selecting reasonable and appropriate security measures for mitigating risks and threats to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI:   * Size, complexity, and capabilities of our organization. * Technical infrastructure, hardware, and software security capabilities. * Cost of security measures. * Probability and criticality of potential risks to our organization’s ePHI.   Our Security Official is responsible for managing our organization’s security measures and related policies and procedures in conformance with findings from our *Risk Analysis* (see SR, AS.1.1), so that our organization operates at acceptable levels of risk.  Our organization is aware of the importance of *Risk Analysis* as the foundation for establishing administrative, physical, and technical safeguard policies and procedures to protect our organization’s ePHI, and, as part of our organization’s *Risk Management* program, of the need to periodically review and update the *Risk Analysis* process in the event of regulatory or operational changes or a security incident or breach involving ePHI. Our Security Official is responsible for documenting our risk analysis process, using the *Risk Analysis Report Log*, which is the Exhibit (SR, AS.1.2.F) after the list of References to SR, AS.1.2. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 1.3** | **45 CFR 164.308(a)(1)(ii)(C)** |
| **Key Activity**  Administrative Safeguards  **Security Management Process: Sanction Policy** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop, implement, and enforce a *sanction policy* for workforce members who do not comply with the security policies and procedures designed to safeguard confidentiality, integrity, and availability of ePHI contained in its electronic networks, systems, applications, devices, and media. Sanctions will be developed from findings from our organization’s risk analysis and will be based on our organization’s estimate of harm resulting from a security violation, incident, or breach. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on our organization’s *Sanction Policy* and consequences for noncompliance with our organization’s security policies and procedures. Our Security Official is responsible for documenting *Sanction Policy* procedures and for evaluating their effectiveness as part of our ongoing risk analysis process. For purposes of this implementation specification, we use the following definitions, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a *Sanction Policy* that is an outcome of findings from its risk analysis, with provisions of the *Sanction Policy* related to our organization’s determination of harm from a particular violation, incident, or breach. For determination of appropriate sanctions, our Security Official shall consult the American Health Information Management Association (AHIMA) document: “Sanction Guidelines for Privacy and Security Violations (2013 Update),” which is available online at: <http://library.ahima.org/PB/SanctionGuidelines#.V2LNKFc3e5A>. Our Security Official is responsible for communicating the *Sanction Policy* and enforcement procedures periodically to workforce members and designated representatives of business associates to serve as a reminder to comply with security policies and procedures and to deter noncompliant behavior. Our Security Official shall scale penalties to likely harm from a discovered security violation, incident, or breach. For example, publicly posting a password on a workstation or desktop might receive a warning and a reminder of the password safeguard for a first violation, while that persistent behavior could require harsher punishment, such as further training for a second violation, suspension for a third violation, and termination of employment for a fourth violation (see the five step sanction set at PR, AR.5.1). Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with our organization’s safeguardpolicies and procedures and subject to sanctions for noncompliance, and for acknowledging their understanding our organization’s *Sanctions Policy* by signing the *Workforce Member Sanctions Policy Acknowledgement*, which is an Exhibit (SR, AS.1.3.F)after the list of References to SR, AS.1.3. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 1.4** | **45 CFR 164.308(a)(1)(ii)(D)** |
| **Key Activity**  Administrative Safeguards  **Security Management Process: Information System Activity Review** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop, implement, and regularly review audit logs, access reports, and security incident tracking reports pertaining to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information (ePHI). Our Security Official is responsible for implementing regular review procedures for audit logs (see SR, TS.2.0), access reports (see SR, AS.5.3), and security incident tracking reports (SR, AS.6.0) to safeguard confidentiality, integrity, and availability of ePHI contained in its electronic networks, systems, applications, devices, and media. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on our organization’s *Information System Activity Review* procedures, frequency of review, and consequences for noncompliance with our organization’s security policies and procedures. Our Security Official is responsible for documenting *Information System Activity Review* procedures and for evaluating their effectiveness as part of our ongoing risk analysis process. For purposes of this implementation specification, we use the following definitions, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Information System Activity Review* proceduresthat are based on findings from its risk analysis. Our Security Official will work with our IT system vendors to implement in our electronic networks, systems, applications, devices, and media that contain ePHI functionality creating audit logs, access reports, and security incident tracking reports.  *Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.  45 CFR 164.304  Our Security Official is responsible for implementing weekly review of logs and reports, with greater frequency of review if circumstances warrant. Our Security Official shall determine if any suspect activities with or unauthorized access to ePHI has occurred, respond immediately to discovered vulnerabilities, implement improved safeguards, and take disciplinary action as called for under our organization’s *Sanction Policy* (see SR, AS.1.3). Our Security Official shall maintain a *dated review log* of our organization’s audit logs, access reports, and security incident tracking reports, and the review log, audit logs, access reports, and security incident tracking reports shall be maintained according to the HIPAA Security Rule *Documentation Standard* (SR, CP.2.0). Our Security Official is responsible for communicating our *Information System Activity Review* process periodically to workforce members and designated representatives of business associates to serve as a reminder to comply with security policies and procedures and to deter noncompliant behavior. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 2.0** | **45 CFR 164.308(a)(2)** |
| **Key Activity**  Administrative Safeguards  **Assigned Security Responsibility** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has identified and assigned its Security Official who is responsible and accountable for development and implementation of policies and procedures for *administrative*, *physical*, and *technical* standards and implementation specifications for safeguarding our electronic protected health information (ePHI) and electronic networks, systems, applications, devices, and media containing such information. Our organization has specified the Security Official’s duties and responsibilities in a job description. Our organization has informed all workforce members and representatives of business associates of the name and responsibilities of the Security Official so that they know to whom to report a security incident, defined at 45 CFR 164.304 as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” Our Security Official is responsible for conducting, and periodically reviewing and updating as necessary, a *Risk Analysis* to assess potential risks and vulnerabilities to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI, and, based on findings from its *Risk Analysis*, establishing or modifying policies and procedures and implementing reasonable and appropriate security measures to mitigate risks and vulnerabilities in compliance with Security Rule *General Requirements* at 45 CFR 164.306(a):   * Ensure *confidentiality, integrity, and availability* of all electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits. * Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. * Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule. * Ensure workforce member compliance with the HIPAA Security Rule.   **Sample Procedures**: <Name of Covered Entity or Business Associate> has identified and assigned its Security Official who is responsible and accountable for development, implementation, and management of *administrative*, *physical*, and *technical* standards and implementation specifications for safeguarding our electronic protected health information (ePHI) and electronic networks, systems, applications, devices, and media containing such information. Our organization has specified the Security Official’s duties and responsibilities in a job description based on the American Health Information Management Association (AHIMA) document: *Healthcare Information Security Officer: Sample Job Description*, which is available online at: <http://bok.ahima.org/doc?oid=58684#.V2RHmVc3e5A>.  Our organization has informed all workforce members and representatives of business associates of the name and responsibilities of the Security Official so that they know to whom to report a security incident, defined at 45 CFR 164.304 as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” Our Security Official is responsible for managing our organization’s security measures and related policies and procedures in conformance with findings from our *Risk Analysis* (see SR, AS.1.1), so that our organization operates at acceptable levels of risk. Our Security Official shall take into consideration the four factors at 45 CFR 164.306(b)(2)(i)-(iv) in selecting reasonable and appropriate security measures for mitigating risks and threats to our organization’s electronic networks, systems, applications, devices, and media that contain ePHI:   * Size, complexity, and capabilities of our organization. * Technical infrastructure, hardware, and software security capabilities. * Cost of security measures. * Probability and criticality of potential risks to our organization’s ePHI.   Our Security Official is responsible for documenting each HIPAA Security Rule complaint in the *Security Safeguard Complaint Log*, which is an Exhibit (SR, AS.2.0.F) after the list of References to SR, AS.2.0. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 3.1** | **45 CFR 164.308(a)(3)(ii)(A)** |
| **Key Activity**  Administrative Safeguards  **Workforce Security: Authorization and/or Supervision** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement procedures for authorizing and supervising workforce members who work with electronic protected health information or in locations where it can be accessed. Our organization’s policy is to authorize workforce members with a defined business need to have access to our electronic networks, systems, applications, devices, and media that contain electronic protected health information, and to prevent those without a defined business need to access or be exposed to such information. Our organization’s objective with respect to workforce authorization and supervision is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information. Our organization’s Security Official is responsible for ensuring that authorization and supervision procedures are in force and their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our organization’s workforce members and any other designated user, such as representatives of business associates, are responsible for complying with *Authorization and/or Supervision* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented procedures for authorizing and supervising workforce members who work with electronic protected health information or in locations where it can be accessed. Our Security Official is responsible for authorizing workforce members with a defined business need to have access to our electronic networks, systems, applications, devices, and media that contain electronic protected health information, and to prevent those without a defined business need to access or be exposed to such information. Our Security Official is responsible for ensuring that, based on business need, there are defined roles and responsibilities for all job functions; there is an appropriate level of security oversight, training, and access for each role; and that each workforce member’s role, job functions, and appropriate access granted (authorization) is specified in a written job description. The Security Official is responsible for ensuring that each workforce member or candidate is qualified to fulfill an assigned role and perform the specified job functions. The Security Official is responsible for ensuring that our organization’s chain of command and lines of authority are effective in providing appropriate security oversight and mitigating threats and vulnerabilities to the confidentiality, integrity, and availability of our organizations electronic protected health information, and that effectiveness is evaluated as part of our risk analysis process. Our organization’s workforce members and any other designated user, such as representatives of business associates, are responsible for complying with *Authorization and/or Supervision* policies and procedures and subject to sanctions for noncompliance, and for acknowledging their understanding and accountability for authorization by signing the *Workforce Member Authorization Acknowledgement*, which is Exhibit 1 (SR, AS.3.1.F.1) after the list of References to SR, AS.3.1. The Security Official is responsible for assigning hardware and providing encryption of *data at rest* and encryption of *data in motion* (if applicable), using Exhibit 2 (SR, AS.3.1.F.2.) herein.  **Note**. Exhibit 2 (SR, AS.3.1.F.2.) is relevant to physical and technical safeguard standards, as noted in the Exhibit. This Exhibit is resident here because assignment of hardware is closely related to authorization to access electronic protected health information on that hardware. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 3.2** | **45 CFR 164.308(a)(3)(ii)(B)** |
| **Key Activity**  Administrative Safeguards  **Workforce Security: Workforce Clearance Procedures** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement *Workforce Clearance* procedures for granting, changing, or terminating access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information by workforce members or candidates. Our organization’s policy is to authorize workforce members with a defined business need to have access to our electronic networks, systems, applications, devices, and media that contain electronic protected health information, and to prevent those without a defined business need to access or be exposed to such information. Accordingly, and as appropriate for the role and job functions of a position with a defined business need in our organization, we shall conduct an educational, employment, financial, and criminal background and references check of each workforce member candidate for whom our organization considers giving access to our electronic protected health information. Our organization’s objective with respect to appropriate clearance is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information. Our organization’s Security Official is responsible for ensuring that background checks are conducted, as appropriate for the workforce member position, and that their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Workforce Clearance* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Workforce Clearance* procedures for granting, changing, or terminating access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information by workforce members or candidates. Our Security Official is responsible for authorizing workforce members with a defined business need to have access to our electronic networks, systems, applications, devices, and media that contain electronic protected health information, and to prevent those without a defined business need to access or be exposed to such information. Accordingly, and as appropriate for the role and job functions of a position with a defined business need in our organization, our Security Official shall be responsible for ensuring that our organization conducts an educational, employment, financial, and criminal background and references check of each workforce member candidate for whom our organization considers giving access to our electronic protected health information. The Security Official is responsible for documenting these workforce clearance procedures, using the *Workforce Member Background Check Log*, which is an Exhibit (SR, AS.3.2.F) after the list of References to SR, AS.3.2. Based on the background and references check, our Security Official is responsible for ensuring that each workforce member or candidate is qualified to fulfill an assigned role and perform the specified job functions. The Security Official is responsible for ensuring that our organization’s workforce clearance procedures are effective in providing an appropriate grant of access to our electronic protected health information and mitigating threats and vulnerabilities to the confidentiality, integrity, and availability of our organizations electronic protected health information, and that their effectiveness is evaluated as part of our risk analysis process. Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Workforce Clearance* policies and procedures and are subject to sanctions for noncompliance. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 3.3** | **45 CFR 164.308(a)(3)(ii)(C)** |
| **Key Activity**  Administrative Safeguards  **Workforce Security: Termination Procedures** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement *Termination Procedures* for workforce members that voluntarily terminate employment from or involuntarily are terminated by our organization. Our organization will develop and implement a checklist for an exit interview for all terminations. Prior to that interview, all direct or remote authorized access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information, email, and voice mail must be terminated, passwords invalidated, and all such devices and media, along with any data or other organization proprietary information (e.g., employee handbook, policy and procedure documentation) returned to the Security Official or his designee. In addition, our organization requires at the exit interview return of all identification badges, keys, other access cards, credit card(s), as well as any organization telecommunication devices. At the exit interview, the terminated individual shall be handed a checklist and information document, with space to tick off that all devices, information, information has been returned to the care of the organization; to be informed in writing that any access authorizations are denied; to be informed of federal penalties for unauthorized access to electronic protected health information; and by signature to acknowledge his or her understanding of the content of the document and receipt of a copy of the document, just signed. Our organization’s objective with respect to appropriate termination is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information, and return of organization property to its care. Our organization’s Security Official is responsible for ensuring that termination policy is enforced and procedures are conducted, acknowledged, and documented, and that their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our organization’s workforce members and any other designated user, such as representatives of business associates, are responsible for complying with *Termination* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Termination Procedures* for workforce members that voluntarily terminate employment from or involuntarily are terminated by our organization. Our Security Official is responsible for implementing a checklist for an exit interview for all terminations. Prior to that interview, the Security Official is responsible for ensuring that all direct or remote authorized access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information, email, and voice mail must be terminated, passwords invalidated, and that all such devices and media, along with any data or other organization proprietary information (e.g., employee handbook, policy and procedure documentation) in the possession of the terminated individual are returned to the Security Official or his designee. In addition, our Security Official is responsible for ensuring that at the exit interview the terminated party returns all forms of organization identification, keys, access cards, credit card(s), as well as any organization telecommunication devices. The Security Official is required to attend the exit interview, if practicable, where the terminated individual shall be handed a checklist and information document, with space for the terminated individual to tick off that all required devices and information has been returned to the care of the organization; to be informed in writing that any access authorizations are denied; to be informed of federal penalties for unauthorized access to our organization’s electronic protected health information, and referral of the breach to appropriate authorities if done so; and by signature to acknowledge his or her understanding of the content of the document and receipt of a copy. For these procedures, the Security Official, or his designee, is responsible for documenting the termination process, using the *Workforce Member Exit Checklist* as Exhibit 1 (SR, AS.3.3.F.1) and the *Workforce Member Exit Interview Acknowledgement* as Exhibit 2 (SR, AS.3.3.F.2) that are after the list of References to SR, AS.3.3. The Security Official is responsible for ensuring that our organization’s termination procedures are effective in preventing unauthorized access to our electronic protected health information and mitigating threats and vulnerabilities to the confidentiality, integrity, and availability of our organizations electronic protected health information, and that their effectiveness is evaluated as part of our risk analysis process. Our organization’s workforce members and any other designated user, such as representatives of business associates, are responsible for complying with *Termination* policies and procedures and are subject to sanctions for noncompliance. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 4.1** | **45 CFR 164.308(a)(4)(ii)(A)** |
| **Key Activity**  Administrative Safeguards  **Information Access Management: Isolating Health Care Clearinghouse Functions** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has a health care clearinghouse that is part of its organization. Our policy is to separate health care clearinghouse functions to prevent unauthorized access to locations within the organization that house electronic networks, systems, applications, devices, media, transactions, and processes that contain electronic protected health information. Our policy is to require the health care clearinghouse to fully implement all Security Rule administrative, physical, and technical safeguard standards, implementation specifications, and requirements to safeguard the electronic protected health information that it creates, receives, maintains, and transmits. Our policy is to inform all organization workforce members that a segment of the organization constitutes a health care clearinghouse and that unauthorized access to its facility or facilities, or networks, systems, applications, devices, or media that contain electronic protected health information shall result in organization sanctions, including suspension or dismissal from employment. Our organization’s health care clearinghouse Security Official shall serve as liaison to the organization for informing all organization workforce members about the requirements to safeguard electronic protected health information and sanctions for unauthorized access to the health care clearinghouse.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Isolating Health Care Clearinghouse Functions* procedures for its healthcare clearinghouse. Our organization has designated the Security Official of the our health care clearinghouse as liaison to the organization for purposes of informing all organization employees of the Security Rule standards, implementations, and requirements under which it operates and the necessity to prevent unauthorized access to its facility or facilities, or networks, systems, applications, devices, or media that contain electronic protected health information in order to safeguard the *confidentiality, integrity, or availability* of and mitigate potential threats and vulnerabilities to that information. The Security Official shall outline the organization sanction policy for unauthorized access, including suspension or dismissal from employment, and inform organization workforce members that health care clearinghouse workforce members are under a HIPAA-mandated sanction policy as well. The Security Official is responsible for training the heath care clearinghouse workforce members on safeguarding electronic protected health information from disclosure to the larger organization. The Security Official shall review the effectiveness of unauthorized access and disclosure policies and procedures periodically as they apply to the role of the health care clearinghouse as part of the larger organization. All workforce members are required to comply with the *Isolating Health Care Clearinghouse Functions* implementation specification and are subject to sanctions for noncompliance. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 4.2** | **45 CFR 164.308(a)(4)(ii)(B)** |
| **Key Activity**  Administrative Safeguards  **Information Access Management: Access Authorization** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement procedures for granting access for its workforce members to our electronic protected health information in our electronic networks, systems, applications, devices, and media and in locations where such information can be accessed. Our organization’s policy is to authorize access to workforce members with a defined business need, and to prevent those without a defined business need to access or be exposed to such information. Our organization’s objective with respect to granting access is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information. Our organization’s Security Official is responsible for ensuring that access authorization procedures are in force and their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Access Authorization* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented procedures for granting access for its workforce members to our electronic protected health information in our electronic networks, systems, applications, devices, and media and in locations where such information can be accessed. Our organization’s Security Official is responsible, in conjunction with our organization’s key information technology workforce members and hardware and software vendors, as appropriate, for designing access authorization procedures; ensuring that, based on business need, there are defined roles and responsibilities for all job functions; there is an appropriate level of security oversight, training, and access granted for each role; and that each workforce member’s role, job functions, and appropriate access granted (authorization) is specified in a written job description. Our Security Official is responsible for ensuring that access is granted and explained to workforce members with a defined business need to access our electronic protected health information for the efficient conduct of our business, and prevent and explain to those workforce members without a business need to have access to that information. Our organization’s objective with respect to granting access is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information. Our organization’s Security Official is responsible for ensuring that access authorization procedures are in force and their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our Security Official is responsible for ensuring that all workforce members receive training on the access authorization process and that the subject is included as part of the *security reminders* program (see SR, AS.5.1). Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Access Authorization* policies and procedures and subject to sanctions for noncompliance, and for acknowledging their understanding and accountability for access authorization by signing the *Workforce Member Authorization Acknowledgement* form that is an Exhibit appearing after the list of SR, AS.3.1 References. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 4.3** | **45 CFR 164.308(a)(4)(ii)(C)** |
| **Key Activity**  Administrative Safeguards  **Information Access Management: Access Establishment and Modification** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement policies and procedures that, based on our access authorization policies and procedures, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process. Our organization’s policy is to authorize access to workforce members with a defined business need, and to prevent those without a defined business need to access or be exposed to such information. Accordingly, our policy is to modify access authorization to a workstation, transaction, program, or process when role and job functions change. Our organization’s objective with respect to granting access is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information. Our organization’s Security Official is responsible for ensuring that modification of user’s rights to access are enforced through chain of command and lines of authority that are documented in job descriptions. Our organization will make sure modification of access authorization procedures are in force and that the effectiveness of the procedures is evaluated as part of the organization’s ongoing risk analysis process. Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Access Establishment and Modification* policies and procedures and subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Access Establishment and Modification* procedures for granting appropriate rights of access for its workforce members to our workstations, transactions, programs, and processes. Our organization’s Security Official is responsible for ensuring that workforce members in the chain of command have lines of authority for reviewing and modifying a user’s right of access when the user’s role or job functions change. The Security Official is responsible for establishing a modification policy and related procedures to follow for any change in a user’s right of access, including providing written documentation for the modification (see Exhibit 1 (SR, AS.4.3F1) after the list of References to SR, AS.4.3) and noting such modification in an access authorization modification log maintained by the Security Official (see Exhibit 2 (SR, AS.4.3F2) to SR, AS.4.3). The Security Official is responsible for ensuring that any and all access authorizations pertain only to the *minimum necessary* electronic protected health information needed for job performance, with exceptions presented in the Note below. Our Security Official is responsible for ensuring that access is granted and explained to workforce members with a defined business need to access our electronic protected health information for the efficient conduct of our business, and prevent and explain to those workforce members without a business need to have access to that information. Our organization’s objective with respect to granting access is mitigating threats and vulnerabilities to *confidentiality, integrity, or availability* of our electronic protected health information irrespective of where it is accessed (e.g., workstation, transaction, program, or process). Our organization’s Security Official is responsible for ensuring that access authorization modification procedures are in force and their effectiveness is evaluated as part of the organization’s ongoing risk analysis process. Our Security Official is responsible for ensuring that all workforce members receive training on the access authorization modification process and that the subject is included as part of the *security reminders* program (see SR, AS.5.1). Our organization’s workforce members and any other designated users, such as representatives of business associates, are responsible for complying with *Access Establishment and Modification* policies and procedures and subject to sanctions for noncompliance, and for acknowledging their understanding and accountability for access authorization by signing the *Workforce Member Authorization Acknowledgement* form that is the Exhibit (SR, AS.3.1F) after the list of References to SR, AS.3.1.  **Note**. The term *minimum necessary* in the procedures text above pertains to 45 CFR 164.502(b): *Uses and Disclosures of Protected Health Information: Standard: Minimum Necessary.*  (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. (see ***HIPAA Integrity*®** PR, UDA.2.1.1**)**  (2) *Minimum necessary does not apply.* This requirement does not apply to: (i) Disclosures to or requests by a health care provider for treatment; (ii) Uses or disclosures made to the individual, as *permitted* under paragraph (a)(1)(i) or as *required* by paragraph (a)(2)(i) of this section; (iii) Uses or disclosures made pursuant to an authorization that is *required* by 45 CFR 164.508; (iv) Disclosures made to the Secretary [of HHS] in accordance with *Compliance and Investigations* [subpart C of General Administrative Requirements, 45 CFR 160]; (v) Uses or disclosures that are *required* by law described by 45 CFR 164.512(a); and (vi) Uses or disclosures that are *required* for compliance with applicable requirements of *Administrative Data Standards and Related Requirements* of HHS. (see ***HIPAA Integrity*®** PR, UDA.2.1.2**)** | | |
| ***HIPAA Integrity*®** | **SR, AS 5.1** | **45 CFR 164.308(a)(5)(ii)(A)** |
| **Key Activity**  Administrative Safeguards  **Security Awareness and Training: Security Reminders** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement a plan for distributing security reminders to all workforce members on a periodic basis. The security reminders will focus on mitigating potential threats and vulnerabilities that are identified in our organization’s risk analysis, and shall be focused on the following definitions, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  Our organization’s Security Official is responsible for documenting *Security Reminders* procedures and ensuring their currency, evaluating their effectiveness as part of our ongoing risk analysis process, and ensuring their distribution to each workforce member and representatives of our organization’s business associates. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on our organization’s *Security Reminders* policy and procedures and to comply with them.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a monthly *Security Reminders­* distribution program that covers all workforce members (including management) and representatives of our organization’s business associates. Our organization’s security reminders are outcomes of our risk analysis and focus on safeguarding our organization’s electronic protected health information (ePHI), and focus on key attributes of the Security Rule: *confidentiality*, *integrity*, and *availability* of ePHI. Our organization uses distribution methods, including, but not limited to, posts in work areas, entries in employee handbooks, booklets on policies and procedures for business associates and contractors, email blasts to workforce members and representatives of business associates, and discussions at meetings of workforce members where at least one security reminder issue is formally identified in the meeting agenda. Our Security Official is responsible for communicating the *Security Reminders* policy to workforce members and designated representatives of business associates, and emphasizing that such reminders are designed to encourage compliance with safeguards and to deter noncompliant behavior. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 5.2** | **45 CFR 164.308(a)(5)(ii)(B)** |
| **Key Activity**  Administrative Safeguards  **Security Awareness and Training: Protection from Malicious Software** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement procedures for guarding against, detecting, and reporting malicious software as part of its security awareness program. These procedures will focus on mitigating potential threats and vulnerabilities to electronic protected health information (ePHI) that are identified in our organization’s risk analysis, and shall be focused on reinforcing the following definitions related to ePHI, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  Malicious software, also known as *malware*, is “a program that is inserted into a host, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim” (see NIST, SP-800-83 Revision 1 in References).  Our organization’s Security Official is responsible for working with our electronic networks, systems, applications, device, and media vendors to identify commercially available virus detection and firewall software programs for guarding against, detecting, and auditing malicious software attempts on all of our organization’s electronic networks, systems, applications, device, and media that contain ePHI. Our workforce members and any other designated users, such as representatives of business associates, are required to install approved virus detection and firewall software programs on our organization’s electronic networks, systems, applications, devices, and media, and are subject to our organization’s sanction policy for failure to comply.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented procedures for guarding against, detecting, and reporting malicious software as part of its security awareness program. These procedures are designed to mitigate threats and vulnerabilities to our organization’s electronic networks, systems, applications, device, and media that contain ePHI. Our organization’s Security Official is responsible for implementing these procedures, working in concert with our electronic networks, systems, applications, devices, and media vendors., and communicating to and training workforce members and designated representatives of business associates on *Protection from Malicious Software* policies and procedures. Our workforce members and any other designated users, such as representatives of business associates, are required to install approved virus detection and firewall software programs on our organization’s electronic networks, systems, applications, devices, and media, and are subject to our organization’s sanction policy for failure to comply. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 5.3** | **45 CFR 164.308(a)(5)(ii)(C)** |
| **Key Activity**  Administrative Safeguards  **Security Awareness and Training: Log-in Monitoring** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will implement *log-in monitoring* procedures for ensuring that only authorized users have access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information and that attempts at unauthorized access are detected. These procedures will focus on mitigating potential threats and vulnerabilities to electronic protected health information (ePHI) that are identified in our organization’s risk analysis, and shall be focused on reinforcing the following definitions related to ePHI, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  Our organization’s Security Official is responsible for working with our electronic networks, systems, applications, device, and media vendors to identify commercially available log-in monitoring and reporting software programs for ensuring authorized access and deterring unauthorized access attempts. Our workforce members and any other designated users, such as representatives of business associates, are required to be authorized for log-in access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information and are subject to our organization’s sanction policy or termination of the business associate agreement, respectively, for failure to comply.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *log-in monitoring* procedures for ensuring that only authorized users have access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information and that attempts at unauthorized access are detected. Our Security Official is responsible for ensuring that an operating system *log-in monitoring* capability or commercially viable *log-in monitoring* software program is always activated for tracking authorized log-ins and unauthorized log-in attempts. Our Security Official is responsible for examining log-in reports and investigating immediately any sequence of <e.g., three (3)> sequential unauthorized log-in attempts to ensure that our organization’s electronic protected health information has not been compromised. Our Security Official is responsible for maintaining *log-in monitoring* reports according to the Security Rule *Documentation* Standard (SR, CP.2.0). Our Security Official is responsible for periodically informing all workforce members and any other designated users, such as representatives of business associates, of our organization’s *log-in monitoring* policy and reporting procedures as a *security reminder*. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 5.4** | **45 CFR 164.308(a)(5)(ii)(D)** |
| **Key Activity**  Administrative Safeguards  **Security Awareness and Training: Password Management** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will implement *password management* procedures for creating, changing, and safeguarding passwords for ensuring that only authorized users have access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information and that attempts at unauthorized access are deterred. These procedures will focus on mitigating potential threats and vulnerabilities to electronic protected health information (ePHI) that are identified in our organization’s risk analysis, and shall be focused on reinforcing the following definitions related to ePHI, from 45 CFR 164.304:  *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.  *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.  *Availability* means the property that data or information is accessible and usable upon demand by an authorized person.  Our organization’s Security Official is responsible for working with our information technology (IT) administrator and vendors of electronic networks, systems, applications, devices, and media to establish procedures so that all workforce members (including management) and any other designated users, such as representatives of business associates, employ *strong* passwords, change them periodically, and protect against disclosure. Such passwords must have at least three characters drawn from the following four character groups: lowercase letters, uppercase letters, digits, and symbols. Our workforce members and any other designated users, such as representatives of business associates, are required to comply with these procedures and are subject to our organization’s sanction policy or termination of the business associate agreement, respectively, for failure to comply.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *password management* procedures for ensuring that only authorized users have access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information and that attempts at unauthorized access are deterred. Our Security Official is responsible for ensuring that a *strong* password selection procedure is in place, and that workforce members and any other designated users, such as representatives of business associates, that are authorized access to our organization’s electronic networks, systems, applications, devices, and media that contain electronic protected health information are required to change their passwords periodically based on threat exposures (e.g., every <30, 60, or 90> days, with timing based on findings from our organization’s risk analysis). Such passwords must have at least three characters drawn from the following four character groups: lowercase letters, uppercase letters, digits, and symbols. Our Security Official also is responsible for training workforce members and any other designated users, such as representatives of business associates, on the importance of safeguarding against password disclosure, such as posting a password on a workstation, hiding it under a desk pad, or *sharing* it with other workforce members. Our Security Official is responsible for periodically informing all workforce members and any other designated users, such as representatives of business associates, of our organization’s *password management* policy and procedures as a *security reminder*.  **Note**. The one exception for password *sharing* relates to the Administrative Safeguard Standard: *Contingency Plan*. The Security Official should safeguard a sealed envelope of passwords of key workforce members who would be responsible for disaster recovery, along with an emergency password for invoking the emergency mode operations plan (see SR, AS.7.3). | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 6.1** | **45 CFR 164.308(a)(6)(ii)** |
| **Key Activity**  Administrative Safeguards  **Security Incident Procedures: Response and Reporting** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will develop and implement security incident *Response and Reporting* procedures for identifying, responding to, mitigating, documenting, and reporting on security incidents. Our organization has designed a reporting mechanism for workforce members and business associates to report immediately to our Security Official a suspected or known security incident, namely, whenever this is a breakdown in administrative, physical, and technical safeguards for protecting electronic networks, systems, applications, devices, and media that contain electronic protected health information that actually or potentially compromises the *confidentiality, integrity, or availability* of the electronic protected health information that our organization creates, receives, maintains, or transmits. The Security Official shall investigate the security incident and initiate our organization’s response team and authorize reasonable and appropriate resources to mitigate any harms resulting from the incident and restore confidentiality, integrity, and availability, as applicable, of our organization’s electronic protected health information. The Security Official shall document each security incident, response, and outcome, and provide such documentation as input in the risk analysis process to strengthen our organization’s administrative, physical, and technical safeguards in order to minimize the likelihood of such security incidents in the future. The Security Official also shall report on each security incident according to the response and notification requirements of the Breach Notification Rule (see ***HIPAA Integrity*®** BN, N series of policies and procedures). Our workforce members are required to comply with our organization’s security incident *Response and Reporting* policies and procedures, and are subject to our organization’s sanction policy for failure to comply. Business associate representatives in our facility or facilities are required to report a known or suspected security incident to our Security Official as soon as discovered. A business associate that discovers a security incident pertaining to our organization’s electronic protected health information in its care is responsible for reporting the incident to our Security Official under requirements of the Breach Notification Rule (45 CFR 164.410, at BN, N.4.1) and Security Rule (45 CFR 164.314(a)(2)(i)(C) at SR, BAA.1.0).  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented security incident *Response and Reporting* procedures for identifying, responding to, mitigating, documenting, and reporting on security incidents. Our organization’s Security Official is responsible for training our workforce members and designated users, such as representatives of business associates, on our organization’s security incident policies and procedures, and on reporting a known or suspected security incident to our Security Official. The trigger for a report of a security incident is whenever there is a discovery of a breakdown in administrative, physical, and technical safeguards for protecting electronic networks, systems, applications, devices, and media that contain electronic protected health information that actually or potentially compromises the *confidentiality, integrity, or availability* of the electronic protected health information that our organization creates, receives, maintains, or transmits. The Security Official shall create a *security incident checklist* for investigating any reported security incident, using the checklist guidance provided in NIST SP 800-61 Revision 2 (see *Incident Handling Checklist* on p. 42) in References. The Security Official shall maintain a log of all security incidents in the *Security Incident Report Log* that is an Exhibit (SR, AS.6.1F) after the list of References to SR, AS.6.1. Based on findings of the investigation, the Security Official shall initiate our organization’s response team and authorize reasonable and appropriate resources to mitigate any harms resulting from the incident and to restore confidentiality, integrity, and availability, as applicable, to our organization’s electronic protected health information. The Security Official shall document each security incident, response (actions taken), and outcome, and provide such documentation as input in the risk analysis process to strengthen our organization’s administrative, physical, and technical safeguards in order to minimize the likelihood of such security incidents in the future. The Security Official shall issue a *security reminder* (see SR, AS.5.1) about each incident to all workforce members (including management) and business associates that identifies the security safeguard breakdown and how to avoid a future occurrence. The Security Official also shall report on each security incident according to the requirements of the Breach Notification Rule (see BN, N series of policies and procedures). Our workforce members are required to comply with our organization’s security incident *Response and Reporting* policies and procedures, and are subject to our organization’s sanction policy for failure to comply. Business associate representatives in our facility or facilities are required to report a known or suspected security incident to our Security Official. A business associate that discovers a security incident pertaining to our organization’s electronic protected health information in its care is responsible for reporting the incident to our Security Official under requirements of the Breach Notification Rule (45 CFR 164.410 at BN, N.4.1) and Security Rule (45 CFR 164.314(a)(2)(i)(C) at SR, BAA.1.0). | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 7.1** | **45 CFR 164.308(a)(7)(ii)(A)** |
| **Key Activity**  Administrative Safeguards  **Contingency Plan: Data Backup Plan** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will implement *Data Backup Plan* procedures to create and maintain up-to-date, retrievable exact copies of our organization’s electronic protected health information, and periodically perform integrity checks to verify that backed-up copies of that information are exact. Our organization’s workforce members are responsible for complying with the *Data Backup Plan* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Data Backup Plan* procedures to create and maintain up-to-date, retrievable exact copies of our organization’s electronic protected health information at a secure off-site location. Our Security Official, using NIST SP 800-34 Revision 1 for guidance (see References), and in consultation with our organization’s vendors of electronic networks, systems, applications, devices, media, and telecommunications, is responsible for ensuring that “exact backup” systems are in place to maintain the integrity of our organization’s electronic protected health information. Our Security Official also is responsible to ensure that our business associates that create, receive, maintain, or transmit electronic protected health information on our behalf also have “exact backup” systems in place that maintain the integrity and the retrievability of that information. Our Security Official is responsible for ensuring on a daily basis, which may be delegated to a key workforce member of our information technology (IT) department, that backups in accordance with this implementation specification are performed, and that exact copies of our organization’s backed-up electronic protected health information are maintained in a database archive on a daily, weekly, monthly, and quarterly replaceable basis. Our Security Official is responsible for ensuring on a daily basis, which may be delegated to a key workforce member of our information technology (IT) department, that backups are tested for integrity to ensure that the process of backup is producing exact copies. If delegated, the IT Department is responsible for providing a written status report to the Security Official on a frequency to be determined by a finding from our organization’s risk analysis. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 7.2** | **45 CFR 164.308(a)(7)(ii)(B)** |
| **Key Activity**  Administrative Safeguards  **Contingency Plan: Disaster Recovery Plan** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will implement *Disaster Recovery Plan* procedures to restore any loss of data with retrievable exact copies of our organization’s backed up electronic protected health information. Our organization will periodically perform integrity checks to verify that backed-up copies of our electronic protected health information are exact. Our organization’s workforce members are responsible for complying with the *Data Backup Plan* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has established *Disaster Recovery Plan* procedures, which will be implemented to restore any loss of electronic protected health information with an exact copy of backed up electronic protected health information. Our Security Official, using NIST SP 800-34 Revision 1 for guidance (see References), and in consultation with our organization’s vendors of electronic networks, systems, applications, devices, media, and telecommunications, is responsible for ensuring that backup systems for restoring an exact copy of our electronic protected health information are in place should such operational information be lost. Our Security Official also is responsible to ensure that our business associates that create, receive, maintain, or transmit electronic protected health information on our behalf also have backup systems in place that maintain the integrity and the retrievability of that information, for restoration should that information be lost. Our Security Official is responsible for ensuring on a periodic basis, which may be delegated to a key workforce member of our information technology (IT) department, that tests of backed-up electronic protected health information are performed according to the disaster recovery plan. Our Security Official is responsible for ensuring on a daily basis, which may be delegated to a key workforce member of our IT department, that backups are tested for integrity on a periodic basis to ensure that the process of backup is producing exact copies. If delegated, the IT Department is responsible for providing a written status report to the Security Official on a frequency to be determined by a finding from our organization’s risk analysis. The Security Official is responsible for evaluating the effectiveness of the procedures for the *Disaster Recovery Plan* and reporting findings during the organization’s risk analysis process.  **Note**. The Security Official should determine from vendors during the consultation process if any software in our organization’s electronic installations accommodates exact copy backup. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 7.3** | **45 CFR 164.308(a)(7)(ii)(C)** |
| **Key Activity**  Administrative Safeguards  **Contingency Plan: Emergency Mode Operation Plan** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will design and implement as necessary an *Emergency Mode Operation Plan* in order to continue critical business processes for safeguarding electronic protected health information while operating in an emergency mode. The *Emergency Mode Operation Plan* shall be a consideration in our risk analysis as our organization considers scenarios that could result in operating in an emergency capacity, ranging from loss of electricity to a natural disaster (e.g., fire, tornado, or hurricane) that could require our organization establishing operations in a different facility or locale. Our policy is to involve all workforce members in the design of the *Emergency Operation Mode Plan* based on their workflows pertaining to business processes involving our electronic networks, systems, applications, devices, and media that contain electronic protected health information. Our organization will establish an Emergency Mode Operation Team, describe functions, and make personnel assignments to carry on the business in emergency mode should circumstances warrant, and test Team response to simulated emergency conditions at least once annually. Based on results from such tests, our organization will evaluate the *Emergency Mode Operation Plan* for effectiveness and make adjustments to it as necessary as part of our risk analysis review process. Our organization’s workforce members are responsible for complying with the *Emergency Mode Operation Plan* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has established an *Emergency Mode Operation Plan* and relatedprocedures, which will be implemented to restore any loss of operational capacity so that our organization can safeguard its electronic protected health information, if necessary with an exact copy of backed up electronic protected health information. Our Security Official, in consultation with our organization’s vendors of electronic networks, systems, applications, devices, media, and telecommunications, is responsible for designing an *Emergency Mode Operation Plan* that examines a range of contingencies, from loss of electricity to a natural disaster destroying or impairing our physical and technical infrastructure, thereby requiring establishment of an emergency facility to continue operation of critical business processes (workflows) for ensuring that our electronic protected health information or an exact backed-up copy is protected. Our Security Official shall identify those critical business processes and determine options for their continuation under different contingencies. Our Security Official shall, as part of the *Emergency Mode Operation Plan*, involve all workforce members in the design of the plan, select key workforce members for implementing and operating according to the *Emergency Mode Operation Plan*, and ensure that there are guidelines for triggering the plan, should the need arise. Our Security Official also is responsible to ensure that our business associates that create, receive, maintain, or transmit electronic protected health information on our behalf, as well as customers and other key individuals and entities, are informed that our organization is operating under the *Emergency Mode Operation Plan*, and that they will be informed of further developments and actions taken to return to normal operations. The Security Official is responsible for evaluating the effectiveness of the *Emergency Mode Operation Plan*, relatedprocedures, tests, and findings from actual invocation of the plan, and for reporting findings during the organization’s risk analysis review process. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 7.4** | **45 CFR 164.308(a)(7)(ii)(D)** |
| **Key Activity**  Administrative Safeguards  **Contingency Plan: Testing and Revision Procedures** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will design and implement *Testing and Revision Procedures* for determining the effectiveness of its contingency plans, including its *Data Backup*, *Disaster Recovery*, and *Emergency Mode Operation* plans. Our organization shall test its data backup plan to ensure that it can regularly create and maintain retrievable exact copies of its electronic protected health information. Our organization shall test its disaster recovery plan to ensure that it can restore any loss of electronic protected health information so that confidentiality, integrity, and availability of that information are not impaired. Our organization shall test its emergency mode operation plan to ensure that the organization can continue its critical business processes for safeguarding our electronic protected health information should we have to operate in an emergency mode. During each of these tests, our organization will document actions, responses, response times, procedural weaknesses, successes, and failures, and those documented results, along with an evaluation of the effectiveness of the plans, will be used in the risk analysis review process for consideration of revising the data backup, disaster recovery, and emergency mode operation plan to increase the likelihood of successful plan implementation and effectiveness. Our organization’s workforce members are responsible for complying with the *Testing and Revision Procedures* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented *Testing and Revision Procedures* to make sure that our organization’s contingency plans—data backup, disaster recovery, and emergency mode operation—are effective. Our organization’s Security Official shall be responsible for testing our data backup plan to ensure that it can regularly create and maintain retrievable exact copies of our electronic protected health information. Our organization’s Security Official shall be responsible for testing our disaster recovery plan to ensure that it can restore any loss of electronic protected health information so that confidentiality, integrity, and availability of that information are not impaired. Our organization’s Security Official shall be responsible for testing our emergency mode operation plan to ensure that the organization can continue its critical business processes for safeguarding our electronic protected health information should we have to operate in an emergency mode. During each of these tests, our organization’s Security Official shall document actions, responses, response times, procedural weaknesses, successes, and failures, and present those documented results, along with an evaluation of the effectiveness of the plans, during the risk analysis review process for consideration of revising the data backup, disaster recovery, and emergency mode operation procedures to increase the likelihood of successful plan implementation and effectiveness. Our Security Official is responsible for overseeing the test designs, may draw on our organization’s workforce members, business associates, and other resources to assist in that regard, and for implementing the tests. Our Security Official is authorized to schedule tests, and may delegate any test functions to key workforce members, but remains responsible for ensuring that all reports are documented and retained according to the Security Rule *Documentation* standard (SR, CP.2.0). | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 7.5** | **45 CFR 164.308(a)(7)(ii)(E)** |
| **Key Activity**  Administrative Safeguards  **Contingency Plan: Applications and Data Criticality Analysis** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will design and implement an ongoing *Applications and Data Criticality Analysis* for sustaining its business operation in normal operating circumstances and should the need arise to recover from a contingency by designing appropriate and effective *Data Backup, Disaster Recovery*, and *Emergency Mode Operation Plan­­­­s*. Our organization has determined that the three required *Contingency Plan* standard implementation specifications—*Data Backup*, *Disaster Recovery*, and *Emergency Mode Operation* plans—are critical applications in our business operation in the event of an emergency or other contingency. Our organization has determined that its proprietary operational, financial, and human resource information and electronic protected health information are critical data. Our organization shall use the risk analysis review process and findings from it to ensure that our policies and procedures focus on mitigating risks to our critical business processes, programs, and applications, to our contingency plans, and to our critical proprietary and electronic protected health information. Our organization’s workforce members are responsible for complying with the *Applications and Data Criticality Analysis* policies and procedures and are subject to sanctions for noncompliance.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented its *Applications and Data Criticality Analysis* procedures as part of and in support of the risk analysis review process. Our organization’s Security Official is responsible for ensuring that our three *Contingency Plans—Data Backup Plan*, *Disaster Recovery Plan*, and *Emergency Mode Operation Plan*—are appropriate and effective for sustaining during normal operations and recovery during an emergency or disaster the confidentiality, integrity, and availability of our organization’s electronic protected health information as well as proprietary critical applications and data pertaining to business operations. *­­­­* Our organization’s Security Official shall be responsible for ensuring that our organization can regularly create and maintain retrievable exact copies of our electronic protected health information and critical electronic applications. Our organization’s Security Official shall be responsible for ensuring that integrity and availability of critical data and applications are not impaired. Our organization’s Security Official shall be responsible for ensuring that the organization can continue to use its critical business processes, applications, and electronic protected health information should we have to operate in an emergency mode. When analyzing the capabilities of critical applications and safeguards of critical data that are components of our organization’s contingency plans, our Security Official shall document actions, responses, response times, procedural weaknesses, successes, and failures, and present those documented results, along with an evaluation of the effectiveness of the plans, during the risk analysis review process for consideration of revising the data backup, disaster recovery, and emergency mode operation procedures to increase the likelihood of successful plan implementation and effectiveness. Our Security Official is responsible for overseeing these analyses, may draw on our organization’s workforce members, business associates, and other resources to assist in that regard, and for implementing each plan analysis at least on an annual basis, and more frequently if circumstances warrant. Our Security Official is authorized to delegate any analytical functions to key workforce members, but remains responsible for ensuring that all reports are documented and retained according to the Security Rule *Documentation* standard (SR, CP.2.0).  **Note**: *A critical application for a covered entity such as a medical or dental practice or hospital and its business associates that create, receive, maintain, or transmit electronic protected health information is the continuous availability of electricity supply. Loss of electricity may be a nuisance in some businesses, but is critical in a healthcare provider environment for ensuring availability of electronic protected health information and applications for creating, receiving, maintaining, and transmitting it. Continuous electricity supply is a basic and critical application for consideration in your risk analysis review process and in each of your organization’s three contingency plans: Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan­­­­.* | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, AS 8.0** | **45 CFR 164.308(a)(8)** |
| **Key Activity**  Administrative Safeguards  **Evaluation** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> will design and implement policies and procedures for initiation of a technical and nontechnical *evaluation* of the effectiveness of our administrative, physical, and technical security safeguards in force for protecting our facilities and electronic networks, systems, applications, devices, and media that contain electronic protected health information (ePHI) that our organization creates, receives, maintains, or transmits. Our policy is to periodically perform an *evaluation* of in force policies and procedures and always perform an *evaluation* in response to changes in environmental or operational conditions or practices that may impact our protection of the confidentiality, integrity, and availability of the electronic protected health information that our organization creates, receives, maintains, or transmits. Our organization will revise its administrative, physical, or technical safeguard policies and procedures, as necessary, based on e*valuation* results. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with our organization’s e*valuation* policies and procedures and the consequences for noncompliance. Our organization shall document each *evaluation* process, results, recommendations, changes in policies and procedures, as applicable, and evaluate the effectiveness of the e*valuation* process as part of our ongoing risk analysis.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented policies and procedures for conducting a periodic technical and nontechnical *evaluation* of the effectiveness of our administrative, physical, and technical security safeguards in force, and in response to environmental or operational changes, for protecting our facilities and electronic networks, systems, applications, devices, and media that contain electronic protected health information (ePHI) that our organization creates, receives, maintains, or transmits. Our procedural objective in each *evaluation* is to ensure that our organization’s policies, procedures, and security control measures are reasonable and appropriate and that our organization always operates at an acceptable level of risk to safeguard the confidentiality, integrity, and availability of our electronic protected health information. Our organization’s Security Official is responsible for:   * Determining whether the evaluation should be performed by workforce members with appropriate technical and nontechnical expertise, or by an external third party business associate with appropriate experience and credentials; * Developing an evaluation plan, including criteria and metrics, for evaluation of all standards and implementation specifications of the Security Rule; * Initiating a periodic evaluation of in force security safeguard policies and procedures and whenever there may be an impact on them due to changes in environmental or operational conditions; * Conducting the evaluation if done internally and overseeing its conduct if performed by an external business associate. * Documenting in a written report for each evaluation all evaluation process activities, including information gathering, analysis, generating findings, preparing options and recommendations, and implementing any necessary changes in security safeguard policies and procedures. * Discussing evaluation results with key organization workforce members and training all workforce members on any changes in policies and procedures resulting from the evaluation.   Our organization’s Security Official also is responsible for documenting each *evaluation* process, results, recommendations, changes in policies and procedures, as applicable, and evaluating the effectiveness of the e*valuation* process as part of our organization’s ongoing risk analysis process. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, BA.1.0** | **45 CFR 164.312(b)(3)** |
| **Key Activity**  *Business Associate Contracts and Other Arrangements*  **Written Contract or Other Arrangement** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> shall execute a business associate agreement with a person who may create, receive, maintain, or transmit electronic protected health information on [<our behalf, if a covered entity> or <on behalf of *name of covered entity*, if a business associate>] if we obtain satisfactory assurances, in accordance with 45 CFR 164.314(a), in a business associate contract, that the person shall appropriately safeguard the information. A person means “a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private” (45 CFR 160.103). Our organization’s Security Official is responsible for managing all business associate agreements and ensuring that workforce members are trained on the responsibilities and need to validate access of any business associate to our organization’s electronic protected health information and information systems containing that information. Workforce members are subject to sanctions for noncompliance with our organization’s *business associate* policies and procedures. Our Security Official is responsible for documenting our *business associate* policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> shall execute a business associate agreement with a person who may create, receive, maintain, or transmit electronic protected health information on our behalf if we obtain satisfactory assurances, in accordance with 45 CFR 164.314(a), in a business associate contract, that the person shall appropriately safeguard the covered entity’s protected health information. Our organization’s Security Official shall be responsible for executing a business associate agreement with each such person, who may create, receive, maintain, or transmit electronic protected health information in our custody, prior to providing access to such person or its designated representative as a business associate. The business associate agreement shall be based on the *Sample Business Associate Agreement Provisions* published on January 25, 2013, by the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS), which is available online at: <http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>, and prepared in association with our organization’s attorney. The Security Official shall ensure that business associate agreements are in place and in force prior to granting access to electronic protected health information in our organization’s custody. Our Security Official shall provide ongoing training to all of our organization’s workforce members on the role of business associates to our organization, including the importance of referring any question to the Security Official pertaining to a business associate’s access to electronic protected health information in our custody. Our Security Official shall ensure that any covered entity’s use and disclosure restrictions, as applicable, are communicated downstream to business associate contractors, and in turn, by business associate contractors to business associate subcontractors, if applicable. Our Security Official shall maintain a *Business Associate Agreement Status Tracking Log* (SR, BA.1.0.F) that is an exhibit to SR, BA.1.0 that appears after the list of References. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 1.1** | **45 CFR 164.310(a)(2)(i)** |
| **Key Activity**  Physical Safeguards  **Facility Access Controls: Contingency Operations** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Contingency Operations* 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. Our procedures are outcomes of our organization’s risk analysis. Our workforce members are required to be trained on and comply with *Contingency Operations* procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these procedures in our disaster recovery and emergency mode operations plans and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a contingency plan to restore electronic systems containing ePHI in the event of a disaster or an emergency (See SR, AS.7). Our *Contingency Operations* procedures are outcomes of our risk analysis, and also are based on content from NIST Special Publication 800-34 Rev. 1 (see References). Our Security Official shall catalog types of emergencies and contingencies that our entity may experience, analyze likely impacts, prepare plans for restoring electronic systems containing ePHI, and identify and credential key workforce members and necessary outside personnel for recovering from a disaster or emergency.  **Note**: **Loss of electricity supply, even if unconnected with any other disaster or emergency, impairs access to ePHI. At a minimum, this contingency of loss of electricity supply should be a key element of your organization’s risk analysis and procedures for managing this contingency should be in place at all times.** | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 1.2** | **45 CFR 164.310(a)(2)(ii)** |
| **Key Activity**  Physical Safeguards  **Facility Access Controls: Facility Security Plan** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Facility Security Plan* policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Our policies and procedures are outcomes of our risk analysis (see SR, AS.1.1 and accompanying ***HIPAA Integrity*®** *Risk Analysis Template*). Our workforce members are required to be trained on and comply with *Facility Security Plan* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Facility Access Controls* policies and procedures to safeguard our facility and electronic systems containing ePHI. These policies and procedures are outcomes of our risk analysis (see SR, AS.1.1 and accompanying ***HIPAA Integrity*®** *Risk Analysis Template*). Our security official shall leverage assigned locations of workforce members for safeguarding the facility internally during normal business hours. Our security official shall implement an alert system that notifies the security official of unauthorized access to the facility outside of normal business hours. The security official shall ensure that the following areas (as examples) are addressed through policies and procedures, and that workforce members are aware of and understand them:   * Who has access to facility and locations therein during business and after hours * Facility opening and closing procedures for safeguarding ePHI * Who has authorized access to electronic systems containing ePHI and mode of access, and how is such authorization authenticated * What access control procedures are in place and how monitored for effectiveness * What access control mechanisms are used to control persons (e.g., badges and keys, sign-in/sign-out) and internal and external access points (e.g., locking mechanisms for doors and windows)   Who is designated for access during a disaster or emergency. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 1.3** | **45 CFR 164.310(a)(2)(iii)** |
| **Key Activity**  Physical Safeguards  **Facility Access Controls: Access Control and Validation Procedures** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Access Control and Validation Procedures* to control and validate a person’s access to facilities based on his or her role or function, including visitor control, and control of access to software programs for testing and revision. Our procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Access Control and Validation Procedures*, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these procedures and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented access controls for areas in our facility that house electronic systems containing ePHI. Our security official shall confirm that all stationary electronic systems containing ePHI are housed in physically secure locations within the facility. Our Security Official shall confirm that all portable or mobile electronic systems containing ePHI used inside or outside the facility are password protected and encrypted according to the HHS Office for Civil Rights (OCR) *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References). Our Security Official shall implement and manage all aspects of physical access control to the facility and locations with electronic systems containing ePHI (e.g., lock keys, alarm codes, etc.), establish appropriate controls and validate access for workforce members and visitors, and ensure that workforce members that resign or are terminated no longer have access. Our Security Official shall confirm that any outside person or entity requiring access does so under an in-force Business Associate Agreement, presents positive identification of appropriate credentials, and is aware of and understands our organization’s security policies and procedures. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 1.4** | **45 CFR 164.310(a)(2)(iv)** |
| **Key Activity**  Physical Safeguards  **Facility Access Controls: Maintenance Records** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Maintenance Records* policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). Our policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Maintenance Records* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented procedures relating to maintenance of a log of any repairs or modifications to the physical components of our facility related to security (see *Maintenance Records Log* Exhibit after References). Our Security Official shall validate satisfactory completion of a repair or modification within one business day of completion. Our security official shall maintain the log in print or electronic format according to the HIPAA Security Rule *Documentation* standard (see 45 CFR 164.316(b), at SR, CP.2). | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 2.0** | **45 CFR 164.310(b)** |
| **Key Activity**  Physical Safeguards  **Workstation Use** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Workstation Use* 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 workstation that can access ePHI. Our *Workstation Use* policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and to comply with our *Workstation Use* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented policies and procedures regarding appropriate workstation uses, how such uses are to be performed, and configuration of physical environments containing workstations where access to ePHI is permitted. Workstations include, but are not limited to, desktop computers, laptop computers, tablet computers, personal data assistant (PDA) or Smart Phone devices, and any other stationary, portable, or mobile electronic media that are used to create, transmit, receive, or store ePHI. Our Security Official has considered applicability of this standard to include workstation use inside or outside of our facility. Examples of procedures that our Security Official has implemented include: no food or drink proximate to a workstation; compliance with software licenses and copyright laws; maintaining current antivirus software and updating it, as appropriate; locating workstations with ePHI in controlled access locations available only to authorized users; and encrypting all ePHI on stationary, portable, and mobile workstations inside or outside of our business facility or facilities. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 3.0** | **45 CFR 164.310(c)** |
| **Key Activity**  Physical Safeguards  **Workstation Security** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Workstation Security* physical safeguards for all workstations that access ePHI, to restrict access to authorized users.Our *Workstation Security* physical safeguards are outcomes of our risk analysis. Our workforce members are required to be trained on and to comply with our *Workstation Security* physical safeguards, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these safeguards and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented physical safeguards to restrict access to authorized users. For example, these include controlled access to workstation locations; username/password access to electronic systems containing ePHI; periodic training on physical safeguard measures and sanctions for their circumvention; requiring written permission for any workforce member to take a portable or mobile electronic device or media outside of the facility, and only when the ePHI is encrypted according to NIST encryption standards specified in the HHS Office for Civil Rights (OCR) *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References); and validating authorized system access of any representative of a Business Associate. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 4.1** | **45 CFR 164.310(d)(2)(i)** |
| **Key Activity**  Physical Safeguards  **Device and Media Controls: Disposal** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Disposal* policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.Our policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Disposal* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Disposal* policies and procedures that are consistent with the disposal provisions in the HHS Office for Civil Rights (OCR) *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References):  “(b) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:   * Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction. [emphasis added] * Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation*, such that the PHI cannot be retrieved.”   Our Security Official is responsible for ensuring that our electronic system vendors are aware of and understand disposal methods in National Institute of Standards and Technology (NIST), *Guidelines for Media Sanitation* (see References); that appropriate methods for final disposition of ePHI and the hardware or electronic media on which it is stored are provided in plain language in the written procedures for disposal; and that workforce members and representatives of our organization’s business associates are trained on those disposal methods. Our Security Official shall ensure that each instance of sanitization shall be recorded and maintained according to the Security Rule *Documentation* standard, using the *Log for Disposal of Hard Copy and Electronic Media Containing Protected Health Information (PHI)*, which is the Exhibit (SR, PS.4.1.F) after References to SR, PS.4.1. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 4.2** | **45 CFR 164.310(d)(2)(ii)** |
| **Key Activity**  Physical Safeguards  **Device and Media Controls: Media Re-use** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Media Re-use* procedures for removal of ePHI from electronic media before the media are made available for re-use. Our procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Media Re-use* procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented media re-use procedures based on National Institute of Standards and Technology (NIST), *Guidelines for Media Sanitation* (see References). Our Security Official shall consider content from this document in our risk analysis review and updates. Our Security Official shall verify that any ePHI is removed from electronic media “such that the PHI cannot be retrieved”. Our Security Official shall balance the cost of new electronic media against potential costs of access of ePHI by unauthorized users of improperly cleansed media for re-use. Our Security Official shall document accountability of media re-use using the *Log for Removal of Electronic Protected Health Information on Electronic Media Before Re-use*, which is the Exhibit SR, PS.4.2.F, after References. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 4.3** | **45 CFR 164.310(d)(2)(iii)** |
| **Key Activity**  Physical Safeguards  **Device and Media Controls: Accountability** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Accountability* procedures for recording the movements of information systems and electronic media and any person responsible therefor.Our procedures regarding *Accountability* are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Accountability* procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented procedures for maintaining an inventory of information systems and electronic media, a corresponding record of movement of such equipment, and workforce members responsible for each inventoried piece of equipment. The Security Official has produced two written logs, which may be electronic, to document accountability. The first log documents movements of stationary information systems and electronic media entitled: *Log of Movements of Stationary Information Systems and Electronic Media*, which is Exhibit 1 (SR, PS.4.3.F1) after References to SR, PS.4.3. The second log pertains to the use of portable electronic media containing electronic protected health information (ePHI) outside of the facility, to whom the electronic media is assigned, and to its encryption of ePHI. This log is entitled*: Log of Use of Portable Electronic Media Outside of the Facility: Assignment and Encryption*, which is Exhibit 2 (SR, PS.4.3.F2). Our Security Official shall maintain these two logs according to the Security Rule Documentation Standard. Our Security Official shall maintain an up-to-date inventory of information systems and electronic media as part of our organization’s ongoing risk analysis process (see ***HIPAA Integrity*®** SR, AS.1.1), with a copy in a secure location outside of the facility. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, PS 4.4** | **45 CFR 164.310(d)(2)(iv)** |
| **Key Activity**  Physical Safeguards  **Device and Media Controls: Data Backup and Storage** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established a policy and procedures to create a retrievable, exact copy of ePHI, when needed, before movement of equipment. Our *Data Backup and Storage* policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and comply with *Data Backup and Storage* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Data Backup and Storage* procedures. Our Security Official shall enumerate the physical safeguards of our organization’s data internally and at any backup site where our data are stored. The Security Official shall confirm that a retrievable, exact copy of ePHI is created prior to movement of stationary information systems or electronic media. Our Security Official shall periodically test our backup facilities and backed-up data for integrity and availability, with frequency of tests an output of our risk analysis. Our Security Official shall confirm that our backed-up data are encrypted and stored off-site in a secure facility, with physical safeguards in place, and that backups of data are performed and retained on a daily, weekly, monthly, and quarterly basis, along with documentation of tests and audits archived according to the Security Rule *Documentation* Standard. The Security Official shall confirm that an exact copy of ePHI is created before movement of stationary equipment in an organization’s facility by signature affirmation on the *Log of Movements of Stationary Information Systems and Electronic Media*, which is Exhibit 1 (SR PS.4.3.F1) located after References at SR PS.4.3. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 1.1** | **45 CFR 164.312(a)(2)(i)** |
| Key Activity  Technical Safeguards  **Access Control: Unique User Identification** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Unique User Identity* policies and procedures for assigning a unique name and/or number to users of its electronic networks, systems, applications, devices, and media that contain ePHI in order to identify and track user identity. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with *Unique User Identity* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented a *Unique User Identification­* program for workforce members and other designated users of our organization’s electronic networks, systems, applications, devices, and media that contain ePHI. Our Security Official has established this program based on considerations in the National Institute of Standards and Technology (NIST) document: *Digital Authentication Guideline*, Draft SP 800-63-3 (see References). Our Security Official is responsible for issuing a new username/password to each new or existing workforce member and representative of a business associate that accesses our organization’s electronic networks, systems, applications, devices, and media that contain ePHI, ensuring that each such person changes its password at a time interval determined in our risk analysis (e.g., 30, 60, or 90 days), and training and providing periodic security reminders to each such person on the appropriate use of the username/password and consequences under our organization’s sanction policy for non-compliance with *Unique User Identification* policies and procedures, especially sharing or posting of credentials. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 1.2** | **45 CFR 164.312(a)(2)(ii)** |
| **Key Activity**  Technical Safeguards  **Access Control: Emergency Access Procedure** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established its *Emergency Access* *Procedure* for obtaining necessary ePHI during an emergency. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with our *Emergency Access* *Procedure*, and are subject to sanctions for noncompliance. Our Security Official is responsible for identifying potential emergency situations as part of our organization’s risk analysis, preparing and testing the *Emergency Mode Operation Plan* (see ***HIPAA Integrity*®** SR, AS.7.3), documenting these situations and procedures for obtaining ePHI should they occur, and for evaluating the effectiveness of the Emergency Access Procedure as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has established its *Emergency Access* *Procedure* for obtaining necessary ePHI during an emergency. As part of our ongoing risk analysis, our Security Official shall catalog types of emergencies that could impair our organization’s ability to obtain its ePHI, and provide remedies for them. **Our organization recognizes that loss of its usual source of electricity in its facility is the most likely emergency scenario to impact access to its stationary electronic networks, systems, applications, devices, and media that contain its ePHI, and has implemented an alternate electricity system (e.g., generator) as an automatic backup.** Our Security Official is responsible for:   * Working with our organization’s IT vendors to establish emergency ePHI access procedures to accommodate likely emergency scenarios identified in its risk analysis. * Documenting the *Emergency Access Procedure*. * Coordinating the *Emergency Access Procedure* with the *Emergency Mode Operation Plan* (see SR, AS.7.3) and *Contingency Operations* (see ***HIPAA Integrity*®** SR, PS.1.1) provisions, including identifying a key person for authorizing the *Emergency Access Procedure* or invoking more stringent ePHI access recovery methods for supporting continuity of business operations, perhaps in another facility using backed-up ePHI. * Training workforce members and representatives of business associates on the *Emergency Access Procedure*.   Documenting emergency access, using the *Emergency Access Log*, which is the Exhibit (SR, TS.1.2F) after the list of References to SR, TS.1.2. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 1.3** | **45 CFR 164.312(a)(2)(iii)** |
| **Key Activity**  Technical Safeguards  **Access Control: Automatic Logoff** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Automatic Logoff* procedures for terminating an electronic session after a predetermined time of inactivity on its electronic networks, systems, applications, devices, and media that contain ePHI. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with *Automatic Logoff* procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has implemented procedures for terminating a session on each of our organization’s electronic networks, systems, applications, devices, and media that contain ePHI after a predetermined period of inactivity based on findings from our organization’s risk analysis. Our Security Official will work with our organization’s IT vendor(s) to set automatic logoff capabilities on each of our electronic networks, systems, applications, devices, and media, if available, or acquire such capabilities to be added on, if necessary, and monitor performance of automatic logoff operations vis-à-vis inactivity. The Security Official, in calculating automatic logoff after a predetermined time of inactivity, shall take into consideration whether electronic networks, systems, applications, devices, and media that contain ePHI are in controlled v. uncontrolled locations, high traffic areas, or used remotely. The Security Official shall install and test performance of password-protected screensaver applications that automatically prevent an unauthorized user from viewing or assessing ePHI on unattended workstations. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 1.4** | **45 CFR 164.312(a)(2)(iv)** |
| **Key Activity**  Technical Safeguards  **Access Control: Encryption and Decryption** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established *Encryption and Decryption* procedures for securing ePHI *at rest* in its electronic networks, systems, applications, devices, and media. Our Security Official shall ensure that ePHI *at rest* has been secured in our organizations databases in accordance with the encryption protocols identified in the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) online *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References). Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with *Encryption and Decryption* procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness and that of the encryption measures for safeguarding ePHI *at rest* in our databases as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has established *Encryption and Decryption* procedures for securing ePHI *at rest* in our databases in our electronic networks, systems, applications, devices, and media. Our Security Official shall ensure that all ePHI *at rest* in our organization’s electronic networks, systems, applications, devices, and media are encrypted, in accordance with OCR’s *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*. Specifically, working with our organization’s IT vendor(s), our organization’s Security Official has followed the encryption recommendations provided in the *Guidance*:  “(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by ‘the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key’ [45 CFR 164.304] and such confidential process or key that might enable description has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.  (i) Valid encryption processes for data ***at rest*** are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.” (see References)  Our Security Official shall verify with our organization’s IT vendors that our electronic network, system, application, device, and media that contain ePHI, as well as any external ePHI backup systems, have audit and data integrity mechanisms to detect unauthorized access and that ePHI *at rest* has not been deciphered. Our Security Official shall be responsible for testing, monitoring, and verifying authorized access and data integrity, and for maintaining the *Data at Rest Encryption Log* of all devices and media in the Exhibit (SR, TS.1.4F) that follows References for SR, TS.1.4. Our Security Official shall report on the effectiveness of *Encryption and Decryption* of ePHI *at rest* during our organization’s ongoing risk analysis activities, and, in consultation with our organization’s IT vendor(s), make recommendations for improvements, as necessary to safeguard the integrity of our organization’s ePHI. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 2.0** | **45 CFR 164.312(b)** |
| **Key Activity**  Technical Safeguards  **Audit Controls** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established hardware and software *Audit Controls* and related policies and procedures that require recording and examining activity in our organization’s electronic networks, systems, applications, devices, and media that contain ePHI to ensure that such activity is appropriate. Our *Audit Controls* policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and to comply with our *Audit Controls* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented hardware and software tracking mechanisms related to access of and activity in our organization’s electronic network, systems, applications, devices, and media that contain ePHI, and policies and procedures for reviewing logs of access and activity to detect unauthorized access or inappropriate activity, and taking appropriate action should such access or activity be detected. Our Security Official is responsible for determining *Audit Controls* requirements, implementing appropriate *Audit Controls*, monitoring and reviewing access and activity, detecting and reporting any unauthorized access or inappropriate activity, and invoking sanctions for such access or activity. Our Security Official also is responsible for training our organization’s workforce members and representatives of business associates on our organization’s *Audit Controls* policies, procedures, and sanctions for violations. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 3.1** | **45 CFR 164.312(c)(2)** |
| **Key Activity**  Technical Safeguards  **Integrity: Mechanism to Authenticate Electronic Protected Health Information** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented *Mechanism to Authenticate ePHI* policies and procedures to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with these policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented electronic mechanisms to ensure that our organization’s ePHI in its networks, systems, applications, devices, and media has not been altered or destroyed in an unauthorized manner. Our Security Official shall verify with our organization’s IT vendors that our electronic network, system, application, device, and media have mechanisms to detect unauthorized intrusion and data corruption and to test and verify data integrity. In the absence of such built-in mechanisms, our Security Official shall, in consultation with our IT vendors, identify reasonable and appropriate commercially available mechanisms and implement them. Our Security Official shall determine requirements for such mechanisms, implement appropriate audit control policies and procedures for reviewing logs of access and activity to detect unauthorized access or inappropriate activity, monitor and review such access and activity, and take appropriate action should such access or activity be detected. Our Security Official also is responsible for training our organization’s workforce members and representatives of business associates on our organization’s *Authentication* policies and procedures, and sanctions for noncompliance. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 4.0** | **45 CFR 164.312(d)** |
| **Key Activity**  Technical Safeguards  **Person or Entity Authentication** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established and implemented *Person or Entity Authentication* policies and procedures to verify that a person or entity seeking access to ePHI in our electronic networks, systems, applications, devices, and media is the person or entity claimed. Our *Person or Entity Authentication* policies and procedures are outcomes of our risk analysis. Our workforce members are required to be trained on and to comply with our *Person or Entity Authentication* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Person or Entity Authentication* policies and procedures for verifying that a person or entity seeking access to our organization’s electronic networks, systems, applications, devices, and media containing ePHI is the person or entity claimed. Our Security Official is responsible for identifying, evaluating, selecting, and monitoring the effectiveness of methods for authentication based on findings from our organization’s risk analysis, and for considering, as necessary, methods of remote authentication. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 5.1** | **45 CFR 164.312(e)(2)(i)** |
| **Key Activity**  Technical Safeguards  **Transmission Security: Integrity Controls** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented *Integrity Controls* security measures and related policies and procedures to ensure that our organization’s transmitted ePHI is not improperly modified without detection until it is disposed. Our Security Official shall ensure that ePHI has not been altered or destroyed without appropriate knowledge and approval and that any approved destruction of ePHI shall be carried out in accordance with the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) online *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, (see HHS, OCR *Guidance* in References). Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with these measures, policies, and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness and that of the security measures as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented electronic mechanisms to ensure that our organization’s ePHI *in motion* to and from its networks, systems, applications, devices, and media has not been modified in an unauthorized manner until the ePHI is disposed. Our Security Official shall verify with our organization’s IT vendors that our electronic network, system, application, device, and media, as well as any external ePHI backup systems, have audit and data integrity mechanisms to detect unauthorized intrusion and ePHI modification during a transmission of such data. Our Security Official shall be responsible for testing, monitoring, and verifying data integrity. Our Security Official shall report on the effectiveness of the *Integrity Controls* during our organization’s ongoing risk analysis activities, and, in consultation with our organization’s IT vendor(s), make recommendations for improvements, as necessary, to safeguard the integrity of our organization’s ePHI. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, TS 5.2** | **45 CFR 164.312(e)(2)(ii)** |
| **Key Activity**  Technical Safeguards  **Transmission Security: Encryption** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented *Encryption* security measures and related policies and procedures to ensure that our organization’s ePHI *in motion* to or from our organization’s networks, systems, applications, devices, and media is not deciphered during transmission should there be unauthorized access to the ePHI *in motion* during its transmission. Our Security Official shall ensure that ePHI *in motion* has been secured during transmission in accordance with the encryption protocols identified in the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) online *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References). Our workforce members and any other designated users, such as representatives of business associates, are required to be trained on and comply with our organization’s *Encryption* policies and procedures, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness and that of the encryption measures for safeguarding ePHI *in motion* during its transmission as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has developed and implemented *Encryption* mechanisms to ensure that our organization’s ePHI *in motion* to and from its networks, systems, applications, devices, and media is not decipherable, in accordance with OCR’s *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see HHS, OCR *Guidance* in References). Specifically, working with our organization’s IT vendor(s), our organization’s Security Official has followed the encryption recommendations provided in the *Guidance* at (1)(ii):  “Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;* 800-77, *Guide to IPsec* [Internet Protocol Security] *VPNs* [Virtual Private Networks]; or 800-113, *Guide to SSL* [Secure Sockets Layer] *VPNs;* or others which are Federal Information Processing Standards (FIPS) 140-2 validated” (see References).  Our Security Official shall verify with our organization’s IT vendors that our electronic network, system, application, device, and media, as well as any external ePHI backup systems, have audit and data integrity mechanisms to detect unauthorized access and that ePHI *in motion* during its transmission has not been deciphered. Our Security Official shall be responsible for testing, monitoring, and verifying authorized access and data integrity, and for maintaining the *Data at Motion Encryption Log* of all devices and media in the Exhibit (SR, TS.5.2F) that follows References for SR, TS.5.2. Our Security Official shall report on the effectiveness of *Encryption* of ePHI *in motion* during its transmission as a part of our organization’s ongoing risk analysis activities, and, in consultation with our organization’s IT vendor(s), make recommendations for improvements, as necessary to safeguard the integrity of our organization’s ePHI. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, CP 1.0** | **45 CFR 164.316(a)** |
| **Key Activity**  Policies and Procedures and Documentation Requirements  **Policies and Procedures** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has established and implemented *Policies and Procedures* to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, taking into account those factors specified in 45 CFR 164.306(b)(2)(i)-(iv):  i. The size, complexity, and capabilities of the covered entity.  ii. The covered entity’s technical infrastructure, hardware, and software security capabilities.  iii. The costs of security measures.  iv. The probability and criticality of potential risks to electronic protected health information [ePHI].  Our organization’s *Policies and Procedures* are outcomes of our risk analysis. Our workforce members are required to have access to, be trained on, and to comply with our organization’s policies and procedures, and are subject to sanctions for noncompliance. Our organization’s Security Official is responsible for managing our safeguard policies and procedures, and is responsible for training our organization’s workforce members and representatives of our business associates on those safeguard policies and procedures. Our Security Official is responsible for documenting these policies and procedures according to the HIPAA Security Rule *Documentation* Standard and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> has established, implemented, and documented *Policies and Procedures* to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, taking into account those factors specified in 45 CFR 164.306(b)(2)(i)-(iv) outlined in our *Policies and Procedures* policy statement. Our organization’s Security Official is responsible for its policies and procedures, namely, ensuring that they are current, based on risk analysis findings, providing in read-only format to all workforce members access to the policies and procedures, training all workforce members and representatives of our organization’s business associates on those policies and procedures, maintaining readily accessible current and archived policy and procedure documentation, and providing our organization’s workforce members a means for secure access to that documentation. Our organization uses online storage of and backs up all current and archived policy and procedures documentation. The Security Official is responsible for training all workforce members on accessing policy and procedure documentation based on Security Official assigned username/password authentication and permissions to each workforce member. Workforce members are responsible for complying with our organization’s safeguard policies and procedures and treating them as proprietary to the organization, and are subject to sanctions for noncompliance. Our Security Official is responsible for training representatives of business associates on policies and procedures pertinent to safeguarding our organization’s ePHI, based on contracted business associate responsibilities. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, CP 2.1** | **45 CFR 164.316(b)(2)(i)** |
| **Key Activity**  Policies and Procedures and Documentation Requirements  **Documentation: Time Limit** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented the required *Time Limit* implementation specification of the *Documentation* standard. Our organization retains all documentation pertaining to administrative, physical, and technical safeguard policies and procedures, and any related records of action, activity, or assessment related thereto, for 6 years from its creation or last record action, activity, or assessment. Our workforce members are required to be trained on and to comply with our *Time Limit* implementation specification of the *Documentation* standard, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> > has implemented the required *Time Limit* implementation specification of the *Documentation* standard. Our organization retains all current and archived documentation pertaining to administrative, physical, and technical safeguard policies and procedures, and any related records of action, activity, or assessment related thereto, for 6 years from its creation or last record action, activity, or assessment. Our organization uses online storage of and backs up all current and archived *documentation*. The Security Official is responsible for training all workforce members on accessing current *read-only* policy and procedure documentation based on Security Official assigned username/password authentication and permissions to each workforce member. Our Security Official is responsible for managing the *Documentation* standard and its *Time Limit* implementation specification. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, CP 2.2** | **45 CFR 164.316(b)(2)(ii)** |
| **Key Activity**  Policies and Procedures and Documentation Requirements  **Documentation: Availability** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented the required *Availability* implementation specification of the *Documentation* standard. Our organization makes administrative, physical, and technical safeguard policies and procedures available to all workforce members whose job responsibilities relate to working with or exposure to ePHI and electronic networks, systems, applications, devices, and media containing such information. Our Security Official is responsible for ensuring that representatives of business associates whose job responsibilities with our organization relate to working with or exposure to ePHI and electronic networks, systems, applications, devices, and media containing such information are trained on the safeguard policies and procedures. Our workforce members are required to be trained on and to comply with our *Availability* implementation specification of the *Documentation* standard, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our organization’s ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> > has implemented the required *Availability* implementation specification of the *Documentation* standard. Our organization retains all current and archived documentation pertaining to administrative, physical, and technical safeguard policies and procedures, and any related records of action, activity, or assessment related thereto, for 6 years from its creation or last record action, activity, or assessment. Our organization uses online storage of and backs up all current and archived *documentation*. The Security Official is responsible for training all workforce members on accessing current *read-only* policy and procedure documentation based on Security Official assigned username/password authentication and permissions to each workforce member. Our Security Official is responsible for managing the *Documentation* standard and its *Availability* implementation specification. | | |

|  |  |  |
| --- | --- | --- |
| ***HIPAA Integrity*®** | **SR, CP 2.3** | **45 CFR 164.316(b)(2)(iii)** |
| **Key Activity**  Policies and Procedures and Documentation Requirements  **Documentation: Updates** | | |
| **Policies and Procedures**  **Sample Policy**: <Name of Covered Entity or Business Associate> has implemented the required *Updates* implementation specification of the *Documentation* standard. Our organization reviews its risk analysis on a periodic basis and on special occasions if there have been operational or regulatory changes, changes in environment that create risk concerns, and in response to compliance audit or aftermath of a security incident or breach. Based on findings from a risk analysis review, administrative, physical, and technical safeguard policies and procedures are updated, as needed, to ensure an acceptable risk level for our organization. Our workforce members are required to be trained on and to comply with our *Updates* implementation specification of the *Documentation* standard, and are subject to sanctions for noncompliance. Our Security Official is responsible for documenting these policies and procedures and for evaluating their effectiveness as part of our ongoing risk analysis process.  **Sample Procedures**: <Name of Covered Entity or Business Associate> > has implemented the required *Updates* implementation specification of the *Documentation* standard. Our organization reviews annually its risk assessment, and as part of that effort, our Security Official evaluates the effectiveness of each of our administrative, physical, and technical safeguard policies and procedures for effectiveness. In the event of a security incident or breach, or any material change affecting security from an operation, regulatory (e.g., the January 25, 2013, Final Rule that required compliance by September 23, 2013), or environmental perspective, our Security Official is required to conduct such an effectiveness review as soon as possible after discovery of the event or change. Our Security Official is responsible for updating any policy or procedure, based on findings from a risk analysis review, and archiving the replaced policy or procedure on backed-up, online storage and substituting a new current policy or procedure. In addition, the Security Official is responsible for informing all workforce members and representatives of business associates about the change, and training them on it. Our Security Official is responsible for managing the *Documentation* standard and its *Updates* implementation specification. | | |