

HIPAA Templates

Security Edition Version 2.4

Compliments the following
Clayton-MacBain LLC HIPAA
Privacy Editions:

- Provider
- Health Plan
- Employee Health Benefit Plan

Contributors:

Lesley E. Berkeyheiser
Chief Editor
The Clayton Group, LLC

John Ecken, CISSP
Security Expert Reviewer
Computer Solutions & Support, LLC

Miriam Paramore
Design & Quality Control Editor
Paramore Consulting, Inc. (PCI)

Susan A Miller, J.D.
Regulatory Reviewer

Published by

THE CLAYTON GROUP, LLC
Glen Mills, PA September, 2003

Policy and Procedure Templates

Reflects February 20, 2003 Security Rule

As published in the Federal Register
Some content originated from Clayton-MacBain LLC Privacy Templates



The Clayton Group

HIPAA Security P&P Checklist

Administrative Safeguards	Have it already?	Customize Template	Refine with Team	Final Draft	Training Complete
1 General Guidelines to Safeguard Protected Health Information					
2 Risk Analysis and Ongoing Risk Management					
3 Sanctions for Violating Privacy and Security Policies and Procedures					
4 Activity Review of Information System Security					
5 Assignment of Security Responsibility					
6 Assignment and Management of Information Access Privileges					
7 Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems					
8 Training Program: Security Awareness and Training to Safeguard Electronic Protected Health Information					
9 Security Incident Procedures: Response and Reporting					
10 Contingency Planning: Response to Unexpected Negative Events					
11 Evaluation of the Security of Protected Health Information					
12 Business Associates Contracts and Other Arrangements					
13 Maintenance of Privacy and Security Policies and Procedures					
Physical Safeguards					
14 Assignment of Facility Access Controls or Privileges					
15 Polices and Guidelines on Work Station Use and Security					
16 Device and Media Controls					
Technical Safeguards					
17 Access Control					
18 Audit Controls					
19 Integrity					
20 Authentication of Person or Entity					
21 Electronic Transmission Security of PHI					
22 E-Mail and Protected Health Information					
23 Facsimile Machines and Protected Health Information					

Items in bold italics correspond to the required implementation specifications as outlined on Appendix A to Subpart C of Part 164.

SAMPLE

AUTHENTICATION OF PERSON OR ENTITY

RESPONSIBILITY: Security Official and Director of Information Systems

BACKGROUND:

Authentication is the process of proving or confirming that an entity or person is who or what it claims to be. All entities and workforce members must be authenticated prior to accessing electronic protected health information. In most cases an entity is a person, but it can be a system or a process as well.

POLICY:

1. [ENTITY] uses a combination of operational practices and technological solutions to validate or authenticate that a person or entity attempting access to electronic protected health information in [ENTITY] possession is the one claimed to be. Corroboration can be made from a compilation of:
 - a. Something workforce member/entity has (card, token, or key)
 - b. Something workforce member/entity knows (password, personal identification number)
 - c. Something related to who the workforce member/entity is (signature, iris, fingerprint)
 - d. Something where workforce member/entity is located (network address, terminal connected by hardwired line)

PROCEDURE:

The Security Official will gather all information collected for the risk assessment process relating to the authentication of a person or entity. This assures that the processes chosen to carry out the combination of policy and technical solutions for person or entity authentication are in accordance with the level of risk, priority, and importance assessed by [ENTITY].

1. The Security Official will establish a committee comprised of the following (as necessary and applicable), or their designees:
 - a. Designated Security Official (*chair*)
 - b. Designated Privacy Official
 - c. Director of Information Systems
 - d. Director of Human Resources

- e. Facilities Maintenance
 - f. Representatives from affected business areas
2. The committee is responsible to choose the [ENTITY] preferred combination of process and technical solution(s) to develop the procedures which function to reasonably safeguard [ENTITY] protected health information, and make up the authentication of person or entity by considering the following factors:
- i. Reviewing the risk assessment results and related documentation
 - ii. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
 - iii. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability
 - iv. Thoroughly considering all areas defined in the procedure as “Implementation Considerations”

Implementation Considerations Relating to Person or Entity Authentication

[ENTITY] Authentication of a person or entity is the process of corroborating, or validating through the use of information that the person or entity is the one claimed. Technical Solutions supporting such corroboration or validation may include:

Password Configuration and Usage Controls

- a. Configuration of system for password encryption
- b. Configuration of system for automatic password changes on a frequent and routine basis (every 30 days or 60 days)
- c. Password deactivation controls
- d. Single session passwords
- e. Configuration of user identification numbers consistent across organizations

Other Safeguard Controls

- a. Access Controls (establishment, modification, and termination)
- b. Audit Trails
- c. Biometric authentication- physical features, hand, finger-print, voice
- d. Cryptographic integrity mechanisms
- e. Digital systems, digital signatures
- f. Encrypted authentication protocols, Encryption technologies (secret or public key)
- g. Magnetic swipe cards with PIN
- h. Smart card tokens, soft tokens
- i. Token-based authentication systems
- j. Workforce incentives to reduce sharing of information
- k. Workforce sanctions to reduce sharing of information

- l. Workforce Training about creation of passwords (not easy to guess, use of alpha and numeric when possible)
- m. Technical controls for workforce members needing access to electronic protected health information including:
 - i. Which workforce members have access (access profiles)
 - ii. Why access to electronic protected information is permitted
 - iii. When access to electronic protected information is permitted
 - iv. When access to electronic protected information is expired
 - v. Where access to electronic protected information is permitted
 - vi. What electronic protected information is permitted access to
 - vii. How workforce members gain access

[Some organizations may find that their software application controls all or part of the authentication process. In other words, technical mechanisms to corroborate or validate person or entity attempting access to the electronic protected health information may be built into the software itself, and therefore documentation of such may be found in software application manuals.]

3. The chair of the committee will assure that all decisions related to the solution (s) chosen are well documented and retained in accordance with [ENTITY] retention policy. This includes documentation supporting “further assessment” activities in support of “Addressable” Implementation Specifications. [Note: The various draft versions of each policy may be utilized to support this documentation process. Consider adding a “Note Section” at the bottom and be sure to archive all draft/working versions of the templates.]
4. Once a process and/or technical solution is chosen, the Security Official will work with the committee to assure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process.
5. The Security Official will additionally assure that any and all related policies and procedures will be updated, including training materials.
6. To the extent that workforce functions are affected by the chosen solution, the training department will work with managers to coordinate and assure that the solution is implemented and each affected member is trained.
7. The Security Official will assure that routine monitoring of this solution is carried out on a (daily, monthly, quarterly) basis in order to continually assess the effectiveness of [ENTITY]’s ability to balance the confidentiality of the protected health information with its integrity and availability.

REFERENCE: 45 CFR § 164.312(d)