DHA PRIVACY AND
CIVIL LIBERTIES OFFICE
Defending Privacy

Person or Entity Authentication For Information System Access

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities (CEs) and their business associates (BAs) to implement person or entity authentication as part of their technical safeguards. Person or entity authentication is verifying and ensuring users seeking access to electronic protected health information (ePHI) are actually who they claim to be.

Definitions

Business Associate: A person or entity that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a CE and is not considered a member of the CE workforce

Covered Entity: Under HIPAA, this is a health plan, a healthcare clearinghouse, or a healthcare provider that conducts one or more covered transactions in electronic form

Electronic Protected Health Information: Individually identifiable health information that is transmitted by or maintained in electronic media

Implementation Specification: The specific requirements or instructions for implementing a standard

Person or Entity Authentication: Procedures to verify that a person or entity seeking access to ePHI is the one claimed

Protected Health Information (PHI): Individually identifiable health information created or received by a CE that relates to the past, present, or future physical or mental health of an individual, and is transmitted or maintained in electronic, paper, or any other form. It excludes health information in employment records held by a CE in its role as an employer. PHI does not include health information of persons deceased more than 50 years

Required: If an implementation specification is required, then a CE and BA must implement the implementation specification

Standard: A rule, condition, or requirement that describes the classification of components; specification materials, performance, or operations; or delineation of procedures for products, systems, services or practices with respect to the privacy of individually identifiable health information

Technical Safeguards: Technology and the policy and procedures for its use that protect ePHI and control access to it.

Discussion

This paper discusses the need for CEs and BAs to install and use technical procedures to verify the identity of "entities" with access to ePHI. An "entity" includes human users and other machines while transferring or requesting information. CEs and BAs may use many methods with varying degrees of assurance to satisfy this requirement. Three accepted methods of authentication are:

1. Something You Have (authentication by ownership);
2. Something You Know (authentication by knowledge); and
3. Something You Are (authentication by characteristic).

Something You Have – this can be a Common Access Card (CAC), smart token, or key and is commonly used for accessing facilities. However, a downside to this method is that the item can be tampered with, lost, or stolen.

Something You Know – this can be a CAC PIN, password, or mother's maiden name and is usually the least expensive method to implement. However, these methods are also considered the weakest because another person can gain access to this knowledge.

Something You Are – this can be a retinal scan, signature, or finger prints and is referred to as biometrics. Biometrics verify an individual by analyzing physiological attributes and behavioral traits that are unique to that individual. It is considered the most effective and accurate method for authentication, but it can also be the most expensive to implement.

For strong authentication, a combination of two or more of the above authentication methods should be used to verify an entity's identity. For example, using a CAC to verify an individual's identity to access a system should require an individual to possess a CAC (Something You Have) and know the correct PIN number (Something You Know).

Person or entity authentication is required by both the HIPAA Security Rule and DoD 8580.02-R. However, as with most of the standards and implementation specifications, the HIPAA Security Rule does not specify the technology or requisite level of robustness. CEs and BAs must balance business needs, cost of controls, and the sensitivity of the ePHI while conducting their risk assessment to determine the strength of the authentication method. There are no associated implementation specifications.

Resources/References

45 CFR 164.312(d), Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007, C4.5