U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

What Type of Authentication is Right for you?

October 2016

Over the past years, the healthcare sector has been one of the biggest targets of cybercrime. Some of these cybercrimes resulted in breaches due to weak authentication, which has made healthcare entities take a second look at their safeguards and consider strengthening their authentication methods.

Authentication is a process used to verify whether someone or something is who or what it purports to be in the electronic context, while keeping unauthorized people or programs from gaining access to information. In the healthcare sector, healthcare entities usually use login passwords or passphrases to access information on public or private networks, internet portals, computers, medical devices, servers, and software applications. Authentication is based on specific criteria, including:

- Something you know (i.e., passwords, passphrases);
- Something you are (i.e., fingerprint, signature, voiceprint, or retina or iris pattern);
- Something you have (i.e., smart card, token).

The **Person or Entity Authentication** standard of the HIPAA Security Rule requires that covered entities and business associates implement reasonable and appropriate authentication procedures to verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed.

Covered Entities and Business Associates should:

- Conduct an enterprise-wide risk analysis that is accurate, comprehensive, and thorough. By conducting a risk analysis that identifies vulnerabilities to the ePHI in their enterprises, they can identify the vulnerabilities of their current authentication methods and practices, the threats that can exploit the weaknesses, the likelihood of a breach occurring, and how a particular type of breach (if it occurs) can impact their business and mission. This process helps entities rate the level of the risk and determine (based on their risk analysis): if the risk should be mitigated with a particular type of authentication; if they should keep the current authentication method in place and accept the risk; if they should transfer the risk by outsourcing authentication services to a business associate; or if they should avoid the risk altogether by eliminating the service or process associated with a particular authentication risk.

- Consider, based on the probability of potential risks and vulnerabilities to their ePHI, implementing a form of authentication that is reasonable and appropriate for their size, complexity, and capabilities, and their technical infrastructure, hardware, and software security capabilities.

- Consider different recommended methods of authentication, depending on the results of their risk analyses, including:

    - Single-factor authentication – A process that uses one of the three factors (i.e. something you know, are, or have) to attain authentication. For example, password is something you know and is the only factor that would be required to authenticate a person or program. This would be considered a single factor authentication.

    - Multi-factor authentication – A method that uses two or more factors to succeed authentication. For instance, a private key on a smart card that is activated by a person fingerprint is considered a multi-factor token. The smart card is something you have, and something you are (the fingerprint) is necessary to activate the token (private key).

Resources:

NIST 800-63.2 http://csrc.nist.gov/publications/PubsSPs.html (Electronic Authentication Guideline)