HIPAA Security Risk Assessment

Compliance for Hospice Providers

April 2016

DISCLAIMER

This Compliance Guidance has been gathered and interpreted by NHPCO from various resources and is provided for informational purposes. This should not be viewed as official policy of CMS or the Medicare Administrative Contractors (MACs). It is always the provider's responsibility to determine and comply with applicable CMS, MAC and other payer requirements.

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule **requires** that covered entities (hospice providers) perform a risk assessment of their organization. **This is not an optional activity for hospice providers.** NHPCO suggests that this assessment be an activity in your quality assessment performance improvement (QAPI) program as well as your compliance program.

All e-PHI that is created, received, maintained or transmitted by a hospice provider is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic protected health information (ePHI). Risk assessment is the first step in that process[1].

Note: The Office for Civil Rights (OCR) is responsible for providing guidance on the provisions in the HIPAA Security Rule.

Purpose of Security Risk Assessment

By conducting a risk assessment, your organization:

- Will ensure it is compliant with HIPAA's administrative, physical, and technical safeguards.
- Can uncover potential weaknesses in their security policies, processes and systems.
- Will identify and address vulnerabilities, potentially preventing health data breaches or other adverse security events.

A comprehensive risk assessment process supports improved security of patient health data[2]. NHPCO has developed a compliance guide for HIPAA Security Best Practices and the Security Risk Assessment. This guide provides information and considerations when performing a risk assessment. Access this

[1] Office for Civil Rights (2010). Guidance on Risk Analysis Requirements under the HIPAA Security Rule. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

[2] Office for Civil Rights (2010). Guidance on Risk Analysis Requirements under the HIPAA Security Rule. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

resource at Security Best Practices HIPAA & Security Risk Assessment: A Compliance Guide for Hospice Providers

Documenting the Risk Assessment

A checklist will not be acceptable evidence to comply with the risk analysis requirement. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.

The Office of the National Coordinator for Health Information Technology (ONC) in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC) have developed a downloadable tool to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

Download the Security Risk Assessment tool. The tool is available for both Windows operating systems and iOS iPads.

Timing of Security Risk Assessment

The risk analysis process is continuous. While the rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process, best practice is that the assessment is ongoing. The frequency of performance will vary and hospice providers may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment. A comprehensive risk assessment and management process is proactively performed as new technologies and business operations are planned.

- Example, if the hospice provider experienced a security incident, had change in ownership, turnover in key staff or management, or is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected[3].

Resources for Hospice Providers

- Health IT.gov - Security Risk Assessment
- Health IT.gov - Guide to Privacy and Security of Electronic Health Information
- Health IT.gov - Security Risk Assessment tool
- NHPCO's Security Best Practices HIPAA & Security Risk Assessment: A Compliance Guide for Hospice Providers
- OCR - Final Guidance on Risk Assessment

[3] Office for Civil Rights (2010). Guidance on Risk Analysis Requirements under the HIPAA Security Rule. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf