COSMOS
Navigate the Compliance Universe

Compliance Today - November 2019
Privacy and security risk assessment considerations in post-acute care

By Carol L. Amick CPA, CHC, CHPC, CCSFP

Carol L. Amick (camick@compliancepoint.com) is Manager of Health Care Services Act CompliancePoint in Duluth GA.

- https://222.linkedin.com/in/carolamick/

The writing is on the wall. The Centers for Medicare & Medicaid Services (CMS) is pushing all providers to promote electronic sharing of healthcare data between providers. In April 2018, CMS issued a request for information seeking feedback on how to increase the sharing of data.[1] Payers and acute-care providers will be working to build networks of connected providers to meet the expected requirements of the CMS Promoting Interoperability Program.

The move towards interoperability will require that post-acute care providers prove that they are capable of protecting the electronic protected health information (ePHI) entrusted to them as part of the data exchange with other providers. One of the key components of making sure you meet that standard and the legal requirements of the Health Insurance Portability and Accountability Act (HIPAA) is the performance of comprehensive and through risk assessments.

HIPAA requires all covered entities to take appropriate actions to protect the privacy and integrity of (PHI). In addition, HIPAA specifically requires healthcare providers to "conduct an accurate and through assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."[2] HIPAA also requires providers take steps to ensure the privacy and integrity of all PHI.

Post-acute care has unique challenges when it comes to completion of a comprehensive risk assessment of the risks related to PHI. Post-acute care has lagged behind acute care, physicians, and other providers in the adoption of electronic health records (EHR). CMS has indicated that their data shows that as of 2017 only 64% of skilled nursing facilities (SNFs), and 78% of home health agencies (HHA) had adopted EHRs.[3] Generally, organizations not using EHRs have been less likely to have performed risk assessments that include the HIPAA security requirements. It's possible that post-acute providers who have not yet adopted EHRs may believe that the HIPAA Security Rule does not apply to them. However, post-acute providers are required to submit to CMS standardized patient assessment data that would be considered ePHI created, transmitted, and held by the organization.

In addition, post-acute providers are less likely to have dedicated information technology (IT) staff to perform the security risk assessment and develop corrective action plans. The Healthcare Information and Management Systems Society (HIMSS) 2019 HIMSS U.S. Leadership and Workforce Survey noted that more than half of non-acute providers do not employ an information and technology leader.[4]