HHS Report: IG Vital to a Cyber-secure Future in Healthcare

Save to myBoK

By Kristi Fahy, RHIA

The Department of Health and Human Services' (HHS) Health Care Industry Cybersecurity Task Force released their long-awaited "Report on Improving Cybersecurity in the Health Care Industry" on June 2. The report addresses information governance (IG) as a concept that will help the healthcare industry to address cybersecurity concerns.

The US healthcare industry includes countless types of organizations ranging from large health systems to small provider practices to vendors and medical device sales companies. All of these organizations have ramped up their IT efforts to stay connected in the healthcare realm, but—according to HHS—this vast electronic network needs to ensure privacy and security for all users, especially patients. HHS says that the susceptibility of healthcare information to cyber threats has become very evident in the last few years with identity theft, ransomware, and targeted nation-state hacking becoming more frequent and extensive.

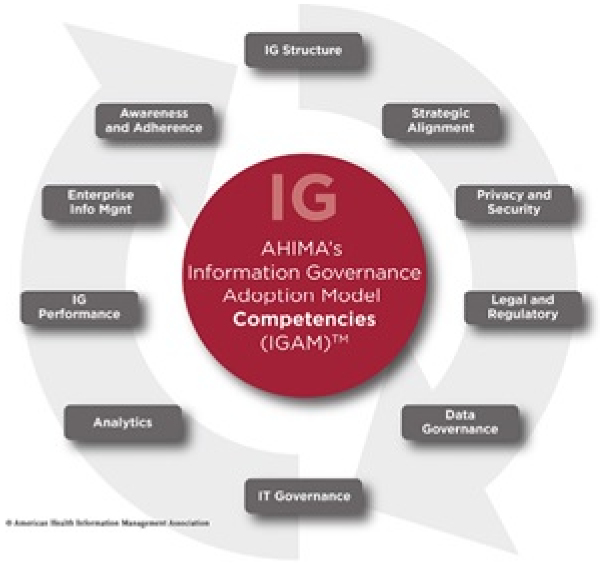
On top of the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, HHS says that the need for greater alignment and harmonization across all levels of government is absolutely necessary. **Information governance** is the answer. The report includes information governance definitions as a way to advance privacy and security practices.

> **HHS' Statement on Information Governance**
>
> "*Information governance is a relatively new concept in the industry and should include not just IT and security stakeholders, but also information stakeholders. Governance structures should also include clinical and non-clinical leaders. Governance of information shifts from technology to people, processes, and the policies that generate, use, and manage the data and information required for care.*"
>
> **AHIMA's Definition of Information Governance**
>
> *"An organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, **regulatory**, **legal**, **risk**, and environmental requirements."*

AHIMA has expressed the importance of information governance as an important initiative that ensures the integrity, reliability, security, and protection of data and information throughout all phases of its lifecycle and throughout all business units of an organization. AHIMA's Information Governance Adoption Model (IGAM™) includes ten competencies of information governance. Three of these competencies are Privacy and Security, IT Governance, and Regulatory and Legal. In many of the recommendations and action items across all sections of the report, the task force describes these information governance competencies as necessary for cybersecurity. Organizations that implement AHIMA's IGAM™ will see risk reduction and prevention from cyber threats and other threats through an organized, IG-focused approach to managing information.

Kristi Fahy (kristi.fahy@ahima.org) is an information governance analyst at AHIMA.

Original source:
Fahy, Kristi. "HHS Report: IG Vital to a Cyber-secure Future in Healthcare" (Journal of AHIMA website), June 22, 2017.



Driving the Power of Knowledge