ATTESTATION: Strengthening "Satisfactory Assurances" of the HIPAA Business Associate Agreement

BY GRANT PETERSON, J.D.

Minneapolis/St. Paul, Minnesota, U.S.A.: Today, healthcare organizations are faced with a growing trend of sharing confidential health information with vendors (business associates) in order to meet critical business needs. Yet from a risk management perspective, little if any assessment of business associate compliance is performed, leaving little assurance of sound compliance practices by the business associate handling patients' confidential health information.

New Regulations for Business Associates

Much of the concern results from sweeping changes in 2009 to the privacy and security regulations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), resulting from the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act imposes additional privacy and security rules on business associates. For example, the HITECH Act applies the administrative, physical and technical safeguard requirements of the security rule to business associates, including obligations related to policies, procedures, implementation and documentation.

In addition, new data breach notification requirements within the HITECH Act now apply to both covered entities and business associates, requiring patient notification of any unauthorized acquisition, access, use or disclosure of their unsecured protected health information. Moreover, increased civil and criminal penalties now apply to both parties for violations of HIPAA privacy and security requirements and authorize state attorneys general to bring civil actions on behalf of state residents adversely affected or threatened by such violations.

Did You Know?
Number of Business Associate Breaches for Dec 17-Jan 17

Cause of Breach	# of Business Associate Breaches
Theft	29
Unauthorized Access/Disclosure	26
Loss	18
Hacking/IT Incident	4
Unauthorized Access/Disclosure & Hacking/IT Incident	3
Improper Disposal	2

Analysis of OCR data by Health Information Privacy/Security Alert's HIPAA & Breach Enforcement Statistics (http://www.melamedia.com/HIPAA.Stats.home.html)

Studies Underscore Enhanced Due Diligence

As evidence of the potential concern for liability that may be unfolding, HIMSS Analytics, (Healthcare Information and Management Systems Society) produced a 2009 Report: *Evaluating HITECH's Impact on Healthcare Privacy and Security*. The study reported that, "…Business associates, those who handle private patient information for healthcare organizations—including everyone from billing, credit bureaus, benefits management, legal services, claims processing, insurance brokers, data processing firms, pharmacy chains, accounting firms, temporary office personnel, and offshore transcription vendors —are largely unprepared to meet the new data breach related obligations brought on by the HITECH Act. Business associates lag behind in all areas that were tested in this survey to measure awareness of the privacy requirements of the HITECH Act. Over 30 percent of business associates surveyed did not know the HIPAA privacy and security requirements have been extended to cover their organizations data breach related obligations included in the HITECH Act."

Now, a recent patient privacy and data security study underscores the significance of the problem. The Ponemon Institute, a privacy and information management research firm released its finding in December, 2011, *Second Annual Benchmark Study on Patient Privacy & Data Security*, reporting that "Despite increased compliance with the HITECH Act and other federal regulations, healthcare data breaches are on the rise… eroding patient privacy and contributing to medical identity theft. On average, it is estimated that data breaches cost benchmarked organizations $2,243,700."

In addition, a key finding from the study indicates that "96 percent of all healthcare providers say they have had at least one data breach in the last two years. Most of these were due to employee mistakes and sloppiness - 49 percent of respondents in this study cite lost or stolen computing devices and 41 percent note unintentional employee action. *Another disturbing cause is third-party error, including business associates, according to 46 percent of participants.*"

Business Associate Agreement

HIPAA requires that…" A covered entity (healthcare organization), in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains *satisfactory assurances*, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

The answer to "satisfactory assurances" has been the use of a Business Associate Agreement between the covered entity and the business

www.privacyanalytics.ca | 613.369.4313
info@privacyanalytics.ca

2

PRIVACY ANALYTICS
Nothing Personal

800 King Edward Drive, Suite 3042
Ottawa, Ontario, Canada K1N 6N5

associate, obligating the business associate to protect confidential health information. However, with the recent HITECH Act requiring business associates to meet new obligations including the HIPAA Security Standards, Data Breach Notification requirements and increased penalties, covered entities feel the need to increase their due diligence of the business associate.

While HIPAA does not require the covered entity to "monitor" or validate the business associate, nevertheless, healthcare organizations are concerned that business associates are compliant with the new HITECH Act requirements and have begun exploring new ways to strengthen the satisfactory assurances of business associate compliance.

Attestation: A Validation Tool

Attestation has served as a valuable tool to validate a process or event in a broad range of services, including legal, financial and healthcare. As a tool, attestation is flexible in design and may be customized around a set of requirements and offered as formal process using assessors or developed for self-assessment.

Attestation is currently used in the Centers for Medicare and Medicaid Services (CMS) Electronic Health Record (EHR) Incentive Programs to provide a financial incentive for the "meaningful use" of certified EHR technology to achieve health and efficiency goals. In the case of Medicare eligible professionals and hospitals, these organizations will have to demonstrate meaningful use through CMS' web-based Registration and Attestation System. The Registration and Attestation System, sets meaningful use objectives for healthcare organizations to legally attest that they have successfully demonstrated meaningful use and therefore eligible for the incentive program.

> *"To attest for the Medicare EHR Incentive Program in your first year of participation, you will need to have met meaningful use for a consecutive 90-day reporting period"*
>
> Attestation, Centers for Medicare and Medicaid, CMS.gov, (https://www.cms.gov/EHRIncentivePrograms/32_Attestation.asp)

Another example of attestation application is used within the Payment Card Industry (PCI). PCI has developed a security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help merchants proactively protect customer account data. PCI Security Standards Council offers comprehensive standards and a framework of specifications to help merchants ensure the safe handling of cardholder information. To assist merchants validate their compliance, the PCI Security Standards Council has created a self-assessment questionnaire for certain levels of merchants. The self-assessment certifies the merchants level of eligibility, validates

compliance status and an action plan for non-compliant status. Annual self-assessments are required of the merchants.

The examples above represent proven use of attestation in a variety of formats applied to large populations. Like CMS and PCI applications, HIPAA and HITECH Act standards also provide a framework of existing specifications that healthcare organizations may use to develop an attestation of compliance for self-assessment questionnaire. In other cases of business associates handling large volumes of protected health information, the healthcare organization may create an on-site audit requirement using an independent assessor. The healthcare organization would update their business associate agreements to adopt new attestation requirements.

For healthcare organizations faced with the growing trend of sharing protected health information with business associates and the desire to strengthen "satisfactory assurances" of compliance, the attestation model may be the key to proactive risk management.

Grant Peterson is a HIPAA privacy and security consultant with over 12 years of experience as a Chief Compliance Officer and consultant. Grant specializes in the HITECH Act and HIPAA privacy and security audits, implementation and attestation to healthcare organizations and business associates. Grant holds a BS degree in Public Administration from Minnesota State University, and a Juries Doctor, law degree from Hamline University School of Law.

Useful Links:

HITECH's Impact on Healthcare Privacy and Security, HIMSS Analytics, Evaluating 2009, (http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)

Second Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute , December 2011, (http://thielst.typepad.com/files/2011-ponemon-id-experts-study.pdf)

Health Information Privacy/Security Alert's HIPAA & Breach Enforcement Statistics analysis of OCR data December 17, 2011 – January 17, 2012 (http://www.melamedia.com/HIPAA.Stats.home.html)

Attestation, Centers for Medicare and Medicaid, CMS.gov, (https://www.cms.gov/EHRIncentivePrograms/32_Attestation.asp)

Summary of the HIPAA Security Rule, U.S. Department of Health and Human Services, (http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html)

www.privacyanalytics.ca | 613.369.4313
info@privacyanalytics.ca

3

PRIVACY ANALYTICS
Nothing Personal

800 King Edward Drive, Suite 3042
Ottawa, Ontario, Canada K1N 6N5