

Hewitt Associates LLC
100 Half Day Road
Lincolnshire, IL 60069
Tel 847.295.5000 Fax 847.295.7634
www.hewitt.com

The Hewitt logo consists of the word "Hewitt" in a white, serif font, centered within a dark blue square.

May 21, 2009

Submitted electronically via the Federal Rulemaking portal @ www.regulations.gov

Attention: HITECH Breach Notification
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Dear Sir or Madam:

Subject: Request for Information Regarding the Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009

Hewitt welcomes the opportunity to submit comments on the required guidance and the breach notification provisions to the U.S. Department of Health and Human Services (HHS) to assist with the development of new rules as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

About Hewitt Associates

Hewitt Associates provides leading organizations around the world with expert human resources consulting and outsourcing solutions to help them anticipate and solve their most complex benefits, talent, and related financial challenges. Hewitt consults with companies to design and implement a wide range of human resources, retirement, investment management, health management, compensation, and talent management strategies. As a leading outsourcing provider, Hewitt administers health care, retirement, payroll, and other HR programs to millions of employees, their families, and retirees. With a history of exceptional client service since 1940, Hewitt has offices in more than 30 countries and employs approximately 23,000 associates worldwide.

I. Overview

As the health and welfare benefits administrator for more than 7.5 million Americans, Hewitt understands the need to implement strong standards to protect the privacy and security of protected health information (PHI).

The breach notification provisions outlined in the HITECH Act would place significant new obligations on covered entities and business associates that use and disclose PHI. We believe these notification requirements could lead to unnecessary concern and distrust by the public and unwarranted reputation damage for organizations trying diligently to protect their employees' information. Without distinguishing between minor infractions and those breaches that could cause more serious harm, the current breach notification standards would likely result in "notification fatigue" for individuals whose data may have been compromised. In addition, the cost of compliance would be significant. This further exacerbates the rapidly rising cost of health care at a time when both employers and Congress are working diligently to reverse this trend to make coverage more accessible to all Americans.

Hewitt has identified areas of the breach notification provisions of the HITECH Act that we believe need further clarification. We also are providing recommendations to solve the issues we have identified, including suggestions for additional technologies and methodologies HHS should consider including in its safe harbor list to secure PHI. Taken together, we believe these suggestions will make the guidelines more workable for covered entities and more effective in accomplishing their intent.

II. Comments on the Specific Technologies and Methodologies That Make PHI Secure

In response to HHS's request for comments on the guidance regarding technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, we have identified the following areas for HHS's consideration.

Additional Methodologies and Technologies for Securing PHI

The Federal Information Processing Standard (FIPS) 140-2 adds an economic and operational burden to organizations that already have existing processes and technologies that sufficiently safeguard PHI. HHS's data breach safe harbors for data in motion and data at rest rely on National Institute of Standards and Technology (NIST) and the related FIPS 140-2 cryptographic certification. In Hewitt's opinion, NIST may not be an appropriate standard for the following reasons: 1) it is primarily used by government contractors to protect national secrets, not health information; and 2) the cryptographic certification process is time-consuming, is expensive, and addresses cryptographic concerns that are not relevant in breach scenarios. For example, FIPS 140-2 addresses breaches only at the point of loss, or when data leaves a system or is exposed to unauthorized parties, but does not address loss scenarios involving virus infection or server misconfiguration. Should HHS mandate the use of NIST guidelines and FIPS certification, organizations will be required to re-implement new and costly FIPS-certified technologies that will not yield incremental protections for data. Hewitt requests that HHS consider alternative encryption technology standards in addition to FIPS 140-2 or provide specific technical security goals that organizations must satisfy in lieu of a central certification process.

Many organizations utilize leading encryption technologies including open-source and custom technologies that are not NIST/FIPS-certified, such as GNU Privacy Guard (GnuPG) and OpenSSL on Solaris. These products often offer equal protection to FIPS-certified products. GnuPG is an open-source implementation of the PGP standards but is not FIPS 140-2 certified. It is used to protect files in motion and at rest and is considered to be a secure and well-examined technology by the industry. Similarly, OpenSSL has been certified to FIPS 140-2 only on specific versions of HP-UX, Linux, and Microsoft Windows. When used on non-certified platforms to transport data with FIPS-approved algorithms, it still provides equivalent protections to the data in transit. Hewitt encourages HHS to consider adding these options to the list of identified technologies and methodologies that may be used to secure PHI.

One gap in the NIST guidelines is the failure to address controls that prevent data losses before they occur. Many organizations have made significant investments to prevent data breaches such as data masking, detailed access controls, data leakage tools, antivirus programs, and appropriately secured data centers. Hewitt encourages HHS to consider including such tools and methodologies as safe harbors to secure PHI and prevent breaches before they happen.

Limited Data Sets

As drafted, the HITECH Act requires notification for breaches involving limited data sets. First, the likelihood that misuse of PHI contained in a limited data set is extremely low because the information is so limited. In the event that this data were compromised, it would be nearly impossible for a covered entity or business

associate to meet the breach notification requirements. This is because the limited data sets are de-identified to such a high degree that an organization would not be able to identify the individual who is the subject of a breach. Therefore, Hewitt recommends that HHS either add limited data sets as a method to secure PHI for data breach purposes or no longer consider limited data sets to be PHI.

III. Comments Related to the Breach Notification Provisions

In response to HHS's request for information on areas or issues pertinent to development of the interim final regulations on breach notification, we have identified several areas for HHS's consideration.

Standard for Requiring Notification of a Breach

The HITECH Act defines a "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." However, this definition of "breach" does not set forth any evaluation of risk or threshold of harm standard.

Mitigating the risk of harm to an individual is one of the primary purposes of breach notifications. The HITECH Act recognizes this important principle in Section 13402(f)(3) and (4) by providing that a notice of breach shall include the "steps individuals should take to protect themselves from potential harm resulting from the breach" and a "brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches." Hewitt suggests that HHS provide additional guidance that allows entities to evaluate the level of risk and severity of a breach and the threshold of harm to an individual whose information is associated with or subject to the breach.

The current breach notification standard increases the likelihood that individuals will receive numerous notifications that do not reflect actual risks. The resulting "notice fatigue" will most likely de-sensitize individuals to these notices in general. They may not pay attention to more serious notifications that identify steps they should take to protect themselves from harm. Thus, Hewitt believes that the breach notification standard should reflect reasonable and balanced notification requirements, and should be limited to situations where there is a substantial risk of harm due to breach of information.

Interaction With State Breach Notification Laws

Although the HITECH Act breach notification provisions and state breach notification laws share common principles, there are some important differences. Hewitt believes these differences would make it unduly burdensome for organizations that must comply with the notification requirements, could create confusion for individuals affected by a breach, and could vastly increase the number of notifications issued.

Notification Time Frames Under State and Federal Breach Notification Laws

HHS should consider aligning the time frames for providing notices to individuals under federal and state laws, so that a covered entity or business associate can send notices to affected individuals at one time. This is especially true for large, multi-state employers where different state laws may specify different time frames for providing breach notices. In this situation, Hewitt believes that the time frames in the HITECH Act should override state laws.

Methods of Notice to Individuals in the Event of a Breach of Unsecured PHI

Individual Notice Delivery Method

Section 13402(e)(1)(A) of the HITECH Act provides that written notification of a breach of unsecured PHI shall be provided via first-class mail to the individual, or by electronic mail if specified as a preference by the individual.

Hewitt believes employers are in the best position to determine the most efficient method to deliver communications to their employees. Hewitt recommends that the interim final regulations provide that for those covered entities that utilize an electronic mail delivery system (company-issued e-mail addresses) for distribution of information to active employees, electronic mail will be deemed to be an individual's preference for notifications. The regulations could stipulate that a paper copy be provided, free of charge, upon request. Electronic mail systems provide for 1) secured and targeted delivery of communications to the intended recipients; 2) timely delivery of important information; and 3) timely notification of undelivered information (such as through return receipt or notice of undelivered electronic mail features). An entity's electronic system also may afford an individual the opportunity to specify an e-mail address (or an alternate e-mail address) where he or she would prefer to receive important communications in the future.

Media Notice

Section 13402(e)(2) of the HITECH Act provides that if the unsecured PHI of more than 500 residents of a state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during a breach, then notice shall be provided to prominent media outlets serving the state or jurisdiction.

Notification through a prominent media outlet would generate unnecessary concern and anxiety for individuals whose PHI is not the subject of the breach. Also, adding mainline media to the notification process greatly increases the chance of sensationalism of an incident. Further, the reputation risk for organizations may be out of proportion to the breach. Hewitt requests that HHS consider the duplicative nature of this media notice requirement that would apply to an organization which is already complying with the individual notice requirement. Providing notice through a prominent media outlet could potentially have a negative impact on an organization's reputation when it is diligently protecting individuals' PHI in compliance with the law.

Application of Breach Notification Provisions to Breaches 30 Days After Issuance of Interim Final Regulations and Business Associates

Since the provisions of the HITECH Act now apply to business associates directly, these business associates face significantly more issues than covered entities to ensure they comply with the new requirements. Under Section 13402(j) of the HITECH Act, the breach notification provisions will apply to breaches discovered on or after the date that is 30 days after publication of the interim final regulations. The date for compliance with the data breach notification provisions precedes the date for compliance by business associates by months. Typically, regulatory changes require compliance first followed by enforcement after a reasonable period of time. Business associates will be required to comply with the new data breach standards (which will affect the covered entities that they serve) before they have completed their compliance plans. Hewitt requests that HHS consider making the effective date of the data breach standards commensurate with business associates' compliance obligations, February 17, 2010.

Attention: HITECH Breach Notification
Page 5
May 21, 2009

Conclusion

Hewitt applauds HHS for its commitment to protecting PHI. We respectfully request further clarification on some of the breach notification guidelines and the introduction of new technology and methodologies to meet the intended objectives in a way that is less disruptive for individuals and companies. We would be pleased to provide further comments or answer any additional questions.

Sincerely,

Hewitt Associates LLC

Frances Wiet
Chief Privacy Officer
(847) 442-2852
frances.wiet@hewitt.com