# 2013 HIPAA Omnibus Rule: What Small Providers Need To Know

By Wrally Dutkiewicz MBA CFE

# 2013 HIPAA Omnibus Rule: What Small Providers Need To Know

The new 2013 HIPAA/HITECH Act Omnibus rules poses some significant issues, challenges and penalties on all health care providers, but small providers will be disproportionately impacted because of its sweeping scope and new requirements for the management of Electronic Personal Health Information (ePHI) which will stretch the limited resources of small providers and potentially put them at the risk of being in regulatory noncompliance. The new provisions of the HIPAA Omnibus Rule take affect March 26, 2013 and all covered entities, including business partners, vendors, and associates must be compliant by September 23, 2013.

The portion of the Omnibus Rule that marks a significant change in violation enforcement was the removal of the requirement for the Department of Health and Human Services (HHS) to first employ an informal remedy for HIPAA violations. The HHS will now be required to review and investigate all complaints alleging violations and move directly to punitive regulatory and civil sanctions that will range from $100 to $50,000 per occurrence with $1.5 million as the calendar year maximum for identical violations. The Rule also broadened its scope of covered entities to include vendors and other business partners that support provider operations. This means that not only the provider can be found culpable if an EPHI security breach occurs, but its business partners can also be subject to Omnibus Rule sanctions as well.


Identity theft is a growing problem for all businesses, but has become a growing risk for smaller healthcare providers because both traditional and cyber criminals have discovered that it can be much easier to collect personal identity information from a small healthcare provider versus gaining access to a large healthcare provider database. Both large and small providers need to be mindful of the information that they receive from patients and have to ensure that they have a privacy policy in place that not only informs patients on how the information that is provided to the provider is used and managed, but also how employees are to use the information, how it is stored, and the measures that the provider has put in place to safeguard the information. However, small providers are put at a disadvantage because they are held to the same HIPAA Information Security requirements as large providers, but have less financial and administrative resources to devote to ensuring their organization is HIPAA compliant.

Collecting information from a provider can be as easy as "dumpster diving" where criminals routinely scour paper recycling bins and trash bins for copies of patient intake forms, lab reports, invoice envelops, and discarded partial photocopies that may have credit card, insurer, and other invoicing information on it. Gaining access to electronic records may involve the outright theft of laptops and USB drives while left unattended in public spaces, or the deliberate break and entering to a business and stealing desktop computers and external hard drives. Beyond the "no-tech" theft of physical equipment and materials containing personal identity information, cyber criminals have found that information can be stolen from a smaller provider through phony emails emulating patients, vendors, labs, insurers, phishing scams, and by directly hacking into a vulnerable provider website and patient database.

The end result of both "no-tech" and "cyber-thefts " is that the provider ultimately suffers the consequence of having to remediate the information theft by notifying all customers that their personal identification information may have been stolen, handling the claims of customers that have become victims of identity theft as a result of the stolen information, and managing the loss of patients' trust which ultimately affects provider revenue as the news spreads that the provider was the origin of the identity thefts. In addition to the litigation that may result, some provider will face regulatory fines from governing and regulatory fines. For all of these reasons it is critical for small providers have a well-designed and implemented HIPAA compliance policy.

After over a decade and a half since its inception, the 2013 HIPAA/HITECH Omnibus Rule represents a substantial revision and augmentation to the scope of HIPAA requirements and has far reaching challenges for small providers to ensure that their business operations remain compliant going forward.

Key provisions of the Rule that small providers should pay attention to include:

- Must have suitable safeguards in place to mitigate the risks of an ePHI breach occurring such as performing a vulnerability and risk assessment, employee training on HIPAA compliance, and the appointment of an information security officer or other designated individual responsible for overseeing HIPAA compliance within the organization and its business partners;

- Ensure all systems are HIPAA compliant including the new definitions relating to electronic media storage;

- Institute appropriate response procedures to be compliant with the "Breach Notification Rule" portion of the Omnibus Rule.

### HHS announces first HIPAA breach settlement involving less than 500 patients

The Hospice of Northern Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

Source: US Department of Human Services Health Information Privacy – *"Enforcement Results - December 2012"*

**HIPAA Information Security:**

All providers regardless of size are held to the same standard under the HIPAA Security Rule and sanctions are uniformly applied for violations. The uniformity of the application of the rule for all providers creates a challenge for smaller providers to be compliant and remain in compliance going forward. The Security Rule requires specific items to be fulfilled to be compliant such as the following critical items:

- Risk Analysis - *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*
    - It is critical for a provider to create and inventory of its information management and database assets and conduct robust vulnerability tests to determine where potential threats of breach may exist. This risk assessment must be comprehensive and be inclusive of all business partners that may receive, transmit, or store ePHI data on behalf of the provider.

- Risk Management - *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the rule]*.
    - A strong ePHI Information Security Policy should be based on a holistic view of the business and encompass all information management and database assets along with all other functional business activity of the provider's organization. The "Information Security Policy" is just one prong in a provider's overall ePHI risk management's activities. Other risk management activities would include:
        - Employee Training – ensure the ePHI Information Security Policy and HIPAA compliance requirements are communicated to employees and that the provider can evidence that this training has been provided. It has been shown that compliance training reduces the incidence of noncompliance in daily business activities.
        - Surveillance & Monitoring – having a monitoring system in place to ensure compliance with the rule can increase the likelihood that a breach may be detected at an early state rather than much after the fact;

- Sanctions Policy - *"Apply appropriate sanctions against workforce members [employees, vendors, business partners] who fail to comply with the security policies and procedures of the covered entity."*

    - It is important for the provider to communicate its willingness to enforce its ePHI Information Security Policy and HIPAA compliance program to ensure that its measures and requirements are viewed seriously by employees and that there is zero-tolerance for noncompliance.

- Supervision - *"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."*

    - Systems should be created that would provide provider management with reporting capabilities that will provide insights into employees' use of ePHI and monitor for noncompliant use activity. Measures may include:

        - Email Surveillance
        - System and Application Access Logs;
        - File Access, Transfer, Change Logs, and Export Logs;
        - Desktop Access and Use Logs;
        - Internet Use Logs

- Data Backup & Disaster Planning - *"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."*

    - Every business entity should have a detailed disaster and business continuity plan that ensures that critical business information can be replicated in the event of a disaster or in the case of a data breach or system failure. A critical element to data back up and disaster planning is to ensure that the provider's information and database asset inventory is kept current so in the event of a data breach or system failure an accurate business impact and loss assessment can be prepared.

- Facility Security Plan - *"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."*

    - Having a periodic facilities and physical asset audit would assist in ensuring that a provider has taken appropriate measures to safeguard the physical equipment and premises that ePHI information is used, stored, and accessed. Additional safeguards would include:

        - Periodic changes to logical and swipe access measures;
        - Terminating access and permissions of terminated employees promptly;
        - Conduct physical inventory audits to ensure that all equipment used to access and store ePHI are accounted for.

- Disposal of Records - *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."*

    - Providers need to ensure that its ePHI Information Security Policy addresses the manner in which both file records and equipment is disposed of:

        - In the case of the removal, deletion, and destruction of ePHI file records, a review process should be instituted where-by items are identified and matched against set compliance criteria before their destruction and then only after a final review and approval has been given, are removed from the system.

        - With respect to physical equipment such as laptops, desktops, printers, copiers, and servers, the providers retirement and disposal plan should account for the following:

            - Physical removal and deletion of data to ensure each piece of equipment leaves the provider's control clean and with the verified absence of ePHI information on its storage media;

            - If a business partner or vendor service is used for the removal and disposal of equipment then the provider should ensure that the entity conducting the service is HIPAA compliant and a protocol exists for the safe and secure return of information to the provider should it be discovered on a device delivered to the vendor for disposal.

- Breach Notification Rule – *"A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.*"

    - The Breach Notification Rule requires the provider to notify patients "*without reasonable delay"* that their personal health and identity information is no longer secure following a breach event. Separate from the timely notification to patients, the rule also requires that the provider submits a "Notice of Breach" to HHS and draws a line between the requirements for a breach affecting fewer or greater than 500 patients.

        - If <u>greater</u> than 500 patients, the providers must submit a Notice of Breach to HHS "*without reasonable delay…….but within 60 days"* from the date of discovery of the breach;

        - If <u>fewer</u> than 500 patients the provider must notify HHS annually via a separate "Notice of Breach" for each breach event that occurred during the year and such notifications are required to be filed no later than 60 days after the end of the calendar year within which the breach events occurred.

There are several other required items under the Security Rule that all providers must adhere to and address within a well formulated information security & technology plan. The key to ensuring that a provider is managing ePHI in a compliant way is through the required vulnerability and risk assessment. By conducting a thorough assessment an inventory of information assets is created and potential vulnerability issues found in manual processes and within employee technology use can be mitigated through revised written supervisory policies (WSPs) and strengthened information security management practices.