Health Care Providers
HIPAA Privacy and Security Compliance
and the effects of the 2013 HIPAA Omnibus Rule

by

Paul R. Hales, Attorney at Law[1]
St. Louis, Missouri

Abbreviations used in this Summary

1. BA……means "Business Associate"
2. BAA……means "Business Associate Agreement" (referred to in HIPAA regulations as the "Business Associate Contract"
3. CIA……means "Confidentiality, Integrity and Availability"
4. CMP……means "Civil Money Penalty"
5. CMS……means "Centers for Medicare & Medicaid Services"
6. HER……means "Electronic Health Record"
7. EMR……means "Electronic Medical Record"
8. EPHI……means "Electronic Protected Health Information"
9. HCP……means "Health Care Provider" – a HIPAA defined Covered Entity
10. HHS……means "The United States Department of Health and Human Services"
11. HIPAA……means "The Health Insurance Portability and Accountability Act of 1996"
12. MU……..means "Meaningful Use" of certified EHR technology required to qualify for CMS Medicare and Medicaid financial incentive payments
13. NPP…… means "Notice of Privacy Practices"
14. PHI……. means "Protected Health Information
15. PSO…….means "Patient Safety Organization"

Introduction

The HIPAA Omnibus Rule – Effective Date: September 23, 2013

The HIPAA Omnibus Rule, published in the Federal Register on January 25, 2013, created substantial new HIPAA Privacy and Security compliance requirements authorized by 2009 amendments to HIPAA (the "HITECH" Act) that go into full force and effect

[1] This summary is prepared by an attorney for education and information purposes only. It is not a privileged communication or to be considered legal advice. Distribution of this summary may be considered attorney advertising in some jurisdictions. The choice of a lawyer is an important decision and should not be based solely upon advertisements. See Missouri Supreme Court Rule 4-7.2: Advertising

September 23, 2013. The new requirements imposed by the HIPAA Omnibus Rule will be summarized below.

HIPAA Prior to the Effective Date of the HIPAA Omnibus Rule

It is important to emphasize HIPAA compliance requirements that were in effect prior to the HIPAA Omnibus Rule and now are subject to much closer scrutiny by government regulators as a result of increased enforcement including newly mandated HHS HIPAA audits and CMS audits of HCPs that have received financial incentive payments after attesting to compliance with MU Core Objectives.

In 2012 the new HHS HIPAA audit program found widespread HIPAA Privacy and Security deficiencies among HCPs of all sizes and types even before the effective date of the much more stringent HIPAA Omnibus Rule. HCPs were cited for inadequate or no Risk Analysis and Risk Management programs, inadequate or no contingency plans, inadequate and incomplete policies, procedures, documentation and ineffective workforce training.

Compliance with the HIPAA Omnibus Rule must be built from a foundation of compliance with the basic HIPAA Rules. Accordingly, key, continuing HIPAA requirements are reviewed briefly before the 2013 Omnibus Rule requirements are explained.

Basic HCP HIPAA Compliance Requirements Not Affected by the 2013 HIPAA Omnibus Rule

1. **Comprehensive Scope of the Privacy Rule**
   All EPHI is PHI and Privacy Rule requirements apply regardless of the medium in which the PHI is created, received, maintained, or transmitted.

2. **HIPAA Security Rule Risk Analysis and Risk Management**
   2005
   The HIPAA Security Rule became effective and requires HCPs, among other things to:
   a. Conduct a HIPAA Security Rule Risk Analysis defined as an accurate and thorough assessment of the potential risks and vulnerabilities to the CIA of EPHI held by the HCP. "Risk Analysis" is often called "Risk Assessment".
   b. Implement a HIPAA Security Rule Risk Management Program of security measures including administrative, physical and technical safeguards *based on the Risk Analysis* to reduce risks and vulnerabilities to the CIA of EPHI.

   Security Rule Risk Analysis is singled here because failure to perform Risk Analysis tops the list of HIPAA compliance deficiencies and is also an MU Core

Objective. HHS officials repeatedly emphasize the importance of the Security Rule Risk Analysis as the basis for establishing an effective HIPAA compliance program. However, HHS audits confirm widespread failure among HCPs to perform a HIPAA Risk Analysis since it became mandatory in 2005. Furthermore, as of September 23, 2013 all HIPAA BAs are required by law to comply with the HIPAA Security Rule and for the first time perform a HIPAA compliant Risk Analysis.

3. **CMS – MU and HIPAA Security Rule Risk Analysis**

2011

CMS made the HIPAA Security Rule Risk Analysis and implementation of security updates necessary to correct identified security deficiencies a mandatory Core Objective of Stage 1 MU. Receipt of a CMS Medicare and Medicaid incentive payment requires an HCP to attest it has completed a HIPAA Security Rule Risk Analysis, implemented of security updates necessary to correct identified security deficiencies and fully documented the process. CMS will conduct random audits of 1 of every 20 recipients of MU incentive payments. An HCP that falsely attest to MU must not only return its financial incentive payment but also may be liable for criminal prosecution under the Federal False Claims Act or similar state laws.

2012

CMS made the HIPAA Security Rule Risk Analysis and Risk Management Process a mandatory Core Objective of Stage 2 MU.

2013

In April, 2013 CMS announced it will conduct random audits of 1 of every 20 recipients of MU incentive payments. If CMS finds that an HCP was ineligible for an MU incentive payment, the incentive payment will be recouped. False attestation of MU also may be the basis for liability under the Federal False Claims Act or similar state laws.

4. **Minimum Necessary Standard**

The Minimum Necessary Standard requires an HCP to limit the amount of PHI it uses, discloses or requests to the Minimum Necessary to accomplish the purpose and to limit the PHI available to each workforce member to the Minimum Necessary required to perform that workforce member's specific duties.

5. **Documentation Requirements**

Every task required by the HIPAA Privacy, Security, Breach Notification and Enforcement Rules must be documented and documentation maintained for

HIPAA purposes for six years. (NOTE: Other laws may require maintenance of the documentation for longer periods.)

6. **Workforce Training**
   Workforce training has always been required and essential for HIPAA Privacy and Security compliance. It is even more vital now during the complex transition to EHRs and EMRs. HCPs must be acutely aware that no EHR or EMR by itself is HIPAA compliant. HIPAA compliance, regardless of the medium in which PHI is created, received, maintained or transmitted depends on the proper use and disclosure of PHI by humans. HCP workforce must be well trained to enable the HCP to be HIPAA compliant. See HHS Guidance on HIPAA Security Administrative Standards that includes a review of the role and importance of workforce training.

HCP HIPAA Compliance Requirements
Modified or Established by the 2013 HIPAA Omnibus Rule

The 2013 HIPAA Omnibus Rule modified some HIPAA Privacy and Security Rule requirements and established new requirements. The HIPAA Omnibus Rule, like the HIPAA regulations it modifies is lengthy and written in dense government "legalese". Key HIPAA Omnibus Rule provisions including newly established requirements are summarized and explained in the following four sections:

1. Privacy Rule Modifications
2. Breach Notification Rule Finalized and Explained by HHS
3. Enforcement Rule Penalties, Categories of Violations and Defenses
4. Business Associates – Expanded Compliance Requirements and Liability

1. Privacy Rule Modifications

a. Privacy Rule Administrative Requirements

i. New BA and BAA Requirements

BAs – New BAAs Required

The liabilities and responsibilities of BAs have been increased substantially as more fully discussed in Section 4 which concludes this Summary. BAAs are required to incorporate these changes. However, HCPs and BAs dealing with Subcontractors defined as BAs under the HIPAA Omnibus Rule are well advised to perform due diligence investigations

of the BA's HIPAA compliance before determining whether to continue using a BA or before engaging a BA. HIPAA compliant BAAs in effect before January 25, 2013 may be used until September 23, 2014 if not revised earlier. However, BA compliance with the Omnibus Rule becomes mandatory on September 23, 2013. Therefore HCPs should promptly review and revise their BAAs as well as the capacity of each BA to comply with HIPAA requirements.

BA Subcontractors – BAAs Required with BA

Subcontractors of a BA that create, receive, maintain or transmit PHI on behalf of a BA are now also defined as HIPAA BAs. Therefore, downstream Subcontractors are subject to the same requirements as a BA that has a contract with an HCP. Each BA now also is required to have a HIPAA compliant BAA in place with its Subcontractors that that create, receive, maintain or transmit PHI on behalf of a BA creating a chain of responsibility for HIPAA compliance.

HCPs not Required to have BAAs with BA Subcontractors

HCPs are not required to have BAAs with Subcontractors of their BAs. Sub-BAAs are the responsibility of the BAs.

ii. New NPP Required by September 23, 2013

HCPs must adopt a new NPP as of September 23, 2013 to conform to HIPAA modifications required by the HIPAA Omnibus Rule. While increasing HIPAA enforcement, HHS also is stepping up its efforts to inform individuals of their HIPAA rights and encouraging them to read the NPP and ask questions.

Required Revisions to the NPP

1. Statements that uses and disclosures of PHI for marketing purposes, disclosures that constitute a sale of PHI and most uses and disclosures of psychotherapy notes require the individual's authorization. HCPs that do not record or maintain psychotherapy notes are not required to include a statement in their NPPs about the authorization requirement for uses and disclosures of psychotherapy notes.
2. A statement that other uses and disclosures not described in the Notice will be made only with an authorization from the individual and the individual may revoke an authorization

prospectively (uses and disclosures previously made under a valid authorization cannot be retrieved).

3. A statement that the individual has the right to opt out of receiving fundraising communications but the NPP is not required to state a mechanism for individuals to opt out of receiving fundraising communications.
4. A statement by HCPs that the individual has the right to restrict certain disclosures of PHI to a health plan regarding a health care item or service if the individual or a person on behalf of the individual pays for the health care item or service in full and out of pocket.
5. A statement of an individual's right to be notified of a breach of the individual's unsecured PHI.
6. The NPP is no longer required to include statements that the HCP may contact the individual to provide appointment reminders or information about treatment alternatives or other health related benefits and services that may be of interest to the individual. (Note that sending information about treatment alternatives or other health related benefits and services involving financial remuneration to an HCP (and/or BA) now requires written authorization by the individual.

Delivery of Revised NPP to Existing and New Patients

HCPs are not required to print and hand out a revised NPP to existing patients, however, they must post the revised NPP in a clear and prominent location in their facility, on their web site if they maintain one and have paper copies of the NPP available for all patients to take with them. HCPs are required to give all new patients a copy of the revised NPP and obtain acknowledgment of receipt of the NPP from them. HCPs may post a summary of the NPP in a prominent place in their facility as long as the full NPP is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on their part. HHS specifically warns that it is not appropriate to require the individual to have to ask a receptionist for a copy of the full NPP (Federal Register, January 25, 2913 at p. 5625).

b. Privacy Rule Regulations Regarding Uses and Disclosures of PHI
   i. PSO activities are defined as health care operations.
   ii. Genetic information is health information that may not be used or disclosed for underwriting purposes.
   iii. HCPs are permitted to disclose a decedent's PHI (not including past medical problems unrelated to the patient's death) to family members and others who were involved in the care or payment for care of a decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the HCP. This does not modify the authority of a decedent's personal representative to have a right to access the decedent's PHI relative to the personal representative's role.
   iv. HCPs may disclose proof of immunization to a school where state or other law requires it prior to admitting a student without written authorization but agreement must still be obtained and may be oral.
   v. Individually identifiable health information of a person deceased more than 50 years is no longer considered PHI subject to restrictions on its use and disclosure under the Privacy Rule.

c. Privacy Rule – Enhanced Patient Rights concerning PHI
   i. An individual has the right to request *and receive* restriction of disclosure of PHI to a Health Plan that pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the HCP in full. NOTE: This requires special medical records attention, workforce training and EHR/EMR functionality.
   ii. An individual has the right to receive access to their PHI in electronic form and generally in the electronic format of their choice if the PHI is maintained in electronic form. The HCP must respond within thirty (30) days of the individual's request and is permitted one thirty (30) day extension but must notify the individual of the extension.
   iii. An individual must give advance authorization before receiving marketing communications from an HCP or BA for which the HCP or BA receives direct or indirect financial remuneration from or on behalf of a third party whose product or service is being marketed.
   iv. HCPs must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications and an individual's choice to

opt out will be considered revocation of authorization to send fundraising communications to the individual.

v. Sale of PHI that is not de-identified by an HCP or BA is expressly prohibited without the individual's authorization. Sale of PHI is defined as disclosure of PHI for which the HCP or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

vi. An HCP may combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. These provisions would allow HCPs to combine authorizations for the use and disclosure of PHI for clinical trials and related biospecimen banking activities, as well as other scenarios that often occur in research studies. However, authorizations for use or disclosure of psychotherapy notes may not be combined with any other authorization.

2. <u>Breach Notification Rule Finalized and Explained by HHS</u>

a. Any Use or Disclosure of unsecured PHI by an HCP or BA not permitted by the Privacy Rule is presumed to be a breach unless the HCP or BA demonstrates that there is a low probability that the PHI has been compromised.

b. The probability of PHI compromise requires consideration of four factors:
   i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   ii. The unauthorized person who used the PHI or to whom the disclosure was made;
   iii. Whether the PHI was actually acquired or viewed; and
   iv. The extent to which the risk to the PHI has been mitigated.

c. A breach will be treated as discovered as of the first day on which the breach is known or should reasonably have been known to the HCP or BA.

d. An HCP must notify affected individuals without reasonable delay and within sixty (60) calendar days from discovery of the breach except for circumstances involving delay requested by law enforcement.

e. The notice of breach must provide information describing the PHI involved, steps the individual should take for protection, steps the HCP is taking to investigate, mitigate harm and prevent further breaches, contact information for individuals to learn more including a toll-free telephone number, an e-mail address, website, or postal address.

f. If the breach involves unsecured PHI of more than 500 residents of a state or jurisdiction the HCP must provide notice of the breach to prominent media outlets in the state/jurisdiction.

g. All breaches of unsecured PHI affecting fewer than 500 individuals must be reported to HHS within sixty (60) days after the end of the calendar year in which the breach was discovered.

h. HCPs must report breaches affecting 500 or more individuals to HHS immediately which generally is considered to be at the same time notification is sent to the affected individuals.

i. BAs must notify HCPs within sixty (60) days of discovery of a breach of unsecured PHI.

j. The HCP is ultimately responsible for notifying individuals of the breach. The time required for the HCP to notify individuals of a breach by a BA is within sixty (60) days of receipt of notification by the HCP of the breach from the BA unless the BA is an "agent" of the HCP in which case the discovery of the breach by the BA is the start of the sixty (60) day notification period for the HCP.

3. Enforcement Rule Penalties, Categories of Violations and Defenses

The HIPAA Omnibus Rule confirmed adoption of higher CMPs for violations of HIPAA. BAs are now directly subject to the Enforcement Rule and subject to assessment of CMPs. An HCP is also liable for violations by a BA that is legally defined as an "agent" of the HCP.

HHS is required to investigate violations if circumstances indicate a possible violation due to willful neglect. However, HHS has discretion regarding whether to review possible violations when circumstances do not indicate it was due to willful neglect and HHS has additional discretion to choose between informal resolution and formal resolution of investigations.

HHS will not impose the maximum CMP in all cases but will determine the amount of a CMP on a case-by-case basis based on the circumstances of a violation and the HCP or BA. Factors in determining the amount of a CMP include:

a. the nature of the violation;
b. the nature and extent of the resulting harm;
c. the number of individuals affected;
d. the HCP's or BA's history of prior compliance with HIPAA Privacy and Security standards; and
e. the financial condition of the HCP or BA.

The Four Categories of Violations and Corresponding CMPs for Each Category

Type of Violation	Range of Amounts of CMP for Each Violation	All Such Violations of an Identical Provision in a Calendar Year
1. Unknowing Violation An HCP or BA did not know and by reasonable diligence would not have known of the violation.	**From $100 to $50,000**	**$1,500,000**
2. Reasonable Cause An HCP or BA committed a violation due to reasonable cause not willful neglect	**From $1,000 to $50,000**	**$1,500,000**
3. Willful Neglect, Corrected An HCP or BA committed a violation due to willful neglect but corrected in a timely manner.	**From $10,000 to $50,000**	**$1,500,000**
4. Willful Neglect, Uncorrected An HCP or BA committed a violation due to willful neglect and not corrected in a timely manner.	**$50,000**	**$1,500,000**

Affirmative Defenses available under the Enforcement Rule

Violation Not Due to Willful Neglect – Corrected within 30 Days

HHS may not impose a CMP on an HCP or BA for violations occurring on or after February 18, 2009 for a violation that is not due to willful neglect and is corrected within 30 days of actual or constructive knowledge of the violation, or a longer period if HHS deems such a longer period is reasonable and appropriate.

Recommended Action Steps when Violation Not Due to Willful Neglect

An HCP or BA that discovers a violation not due to willful neglect should;

- Document the date on which it discovered the violation;
- Document the circumstances establishing lack of willful neglect;
- Correct the violation within 30 days of discovery; and
- Document all investigative and corrective actions.

Subject to Previous Criminal Penalty

Another affirmative defense to CMPs, although an unhappy one, is that HHS may not impose a CMP for a violation that previously had been subject to a criminal penalty.

4. Business Associates – Expanded Compliance Requirements and Liability

a. The Definition of BA is expanded
   i. A BA is now defined as a person or entity other than a member of the HCP's workforce that performs services for an HCP in which the BA creates, receives, maintains or transmits PHI.
   ii. Addition of the word "*maintains*" is significant and emphasized ion HHS guidance on the new rule. It confirms that a data storage company that maintains PHI on behalf of an HCP and has access to the PHI (whether digital or hard copy) is a BA, even if it does not view the information or only does so on a random or infrequent basis. There is only a very narrow "conduit" exception for entities that have only transient possession of PHI for transmission purposes such as the U. S. Postal Service and UPS or their electronic equivalents, such as internet service providers (ISPs).
   iii. Specific types of entities added to the definition of a BA are:
      1. PSOs;
      2. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to an HCP and that requires access on a routine basis to such PHI;
      3. A person that offers a personal health record to one or more individuals on behalf of an HCP; and

4. A Subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA.

b. BAs are directly liable under HIPAA
   i. BAs are subject to enforcement of HIPAA Privacy and Security law by HHS and by State Attorneys General. Previously BA HIPAA responsibility to protect PHI was based only on the BA's contractual responsibilities with the HCP. This is a change that HHS estimates will affect as many as 500,000 HIPAA BAs. Under the Omnibus Rule BAs are subject to the HIPAA Security and Enforcement Rules and parts of the HIPAA Privacy and Breach Notification Rules. BAs are liable for:
      1. impermissible uses and disclosures of PHI;
      2. failure to provide breach notification to an HCP;
      3. failure to provide access to PHI to the individual or HCP;
      4. failure to provide an accounting of disclosures;
      5. failure to disclose to HHS as required;
      6. failure to comply with the entire HIPAA Security Rule; and
      7. CMPs for HIPAA violations.

c. BAAs with Subcontractors
   A BA must have a BAA with each Subcontractor or "sub-BA" that creates, receives, maintains, or transmits PHI on behalf of the BA. This is a change that HHS estimates will affect between 250,000 and 500,000 BA Subcontractors. As stated previously, an HCP is only required to have a BAA with its BAs – not with each of its BA's Subcontractors.

d. Elements of the Privacy Rule apply to BAs
   i. A BA is not permitted to use or disclose PHI in a manner that would violate the Privacy Rule if done by the HCP including, expressly, the Minimum Necessary Standard.
   ii. A BA may not use or disclose PHI except as permitted or required by the Privacy Rule or the Enforcement Rule.
   iii. A BA may use or disclose PHI only as permitted or required by the BAA.
   iv. A BA must provide an electronic copy of PHI to an individual or the HCP as necessary to satisfy the HCP's obligations to comply with an individual's request for an electronic copy of PHI.

