Robert E. Moffit, PhD
CHAIR

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

HIPAA Omnibus Rule

January 2014

On January 17, 2013 the Department of Health and Human Services (HHS) published the Omnibus Rule, which modifies some of the provisions of the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) governing protected health information (PHI).[1] The final rule focuses predominantly on enforcement of breach notification regulations and enhanced individual rights, which impact Business Associates (BAs).[2] The regulations go into effective on March 26, 2013, with required compliance by September 23, 2013. The following list summarizes a number of key changes made by the Omnibus Rule.[3]

BUSINESS ASSOCIATE

Under the Omnibus Rule, a BA refers to any individual or organization that provides services such as billing, administrative or data analysis support to a Covered Entity (CE), typically involving disclosure of some level of health information.[4] Health plans, patient safety organizations (PSOs), health information organizations (HIOs) and subcontractors that maintain contracts with a BA for any portion of the PHI maintenance process are also considered BAs and must be identified in a written agreement under the terms and conditions of the updated BA agreements.[5]

BA Liabilities

- Under the Omnibus Rule a BA's obligations to the CE can no longer be confined to the limitations of the BA agreement. BAs and their HIPPA-covered subcontractors are now required to comply with current HIPAA regulations and are liable for any noncompliance.

Business Associate Agreement (BAA)

- BAAs have to be reinstated within the terms detailed in the Omnibus Rule. Current BAAs between CEs will be grandfathered in and deemed viable through the September 2013 deadline. BAs must possess a written agreement with their HIPPA-covered subcontractors, which must align with the conditions of their BAA with the CE.

BREACH NOTIFICATIONS

CEs and BAs must undertake a risk management process in the event of breach or suspected breach of PHI: (1) to identify the nature and extent of the health information processed, such as social security numbers, financial information, name, addresses, test results etc., and the probability that the individual can be re-identified; (2) to evaluate the entity receiving the PHI; (3) to assess

---

[1] Protected health information (PHI) refers to individually identifiable health information (IIHI) transmitted or maintained by a medical office such as the medical history of a patient, test results, insurance information, etc. The IIHA of persons who have been deceased for fifty (50) years or fewer is also considered PHI.

[2] A BA is a person, entity or subcontractor of such person or entity using PHI to perform a function or activity on behalf of a provider/facility, health plan or clearinghouse but who is not part of the aforementioned workforce, e.g. billing, practice management, and utilization review.

[3] The Omnibus Rule is available at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html

[4] A CE is a health care provider or facility, health plan, or health care clearinghouse that transmits medical information in electronic form.

[5] BA Agreement is a written contract between a Covered Entity and a BA.

whether the PHI was acquired or reviewed; and (4) to determine the extent of risk mitigation based on how thoroughly or quickly the PHI was destroyed or recovered.

Suspected breach and the responsibility of the CE and BAs

- HHS is now required to conduct a formal investigation on any indication of possible neglect.
- The onus rests with the CE and the BA to determine if the information in question has been acquired or viewed by an unauthorized entity.
- CEs and BAs must assess at risk variables for health information being compromised following an unauthorized disclosure.

DISCLOSURE OF PHI

CEs must now receive authorization (verbal or written) from the patient prior to disclosing PHI for provision of care or operational communication to a third party for the below purposes. Communications to an individual must include a clear and conspicuous opportunity to elect not to receive any further marketing or fundraising communications at any time.

Marketing

- A communication about a product or service that encourages recipients of the communication to purchase or use the product or service in exchange for direct or indirect remuneration is considered marketing.
- Refill reminders and communications about a drug or biologic currently being prescribed for the individual, or case management/care coordination, or recommending advantageous alternative therapies, providers or settings for individual's care are generally not considered marketing.

Sale of PHI

- A sale constitutes a disclosure of PHI by a CE or BA where the Covered Entity or BA directly or indirectly received remuneration from or on behalf of the recipient of the PHI in its exchange. Exceptions apply.[6]
- An authorization permitting the sale of PHI must state that the disclosure will result in remuneration to the CE.

Fundraising

- PHI permitted to use for fundraising includes demographic information (name, address, other contact information, age, gender and date of birth); clinical, treatment and outcome information; departments and physicians providing services; and health insurance status, but not include diagnosis information.
- Individual must be informed of the purposes for fundraising and types of PHI information to be used.

[6] Sale of PHI does not include disclosures for the purposes of: (1) public health, (2) research, (3) treatment or payment, (4) sale, transfer, merger or consolidation of all or part of the Covered Entity, (5) undertaking or accepting remuneration to perform such activities by the BA or a subcontractor, (6) disclosure to an individual who is the subject of the PHI pursuant to the request to access the PHI or accounts, (7) as required by law, and (8) disclosures in accordance with the Privacy Rule if the only remuneration received by Covered Entity or BA is a reasonable, cost-based fee.

Exclusions from Authorization

- CEs are no longer required to obtain written authorization to disclose the proof of student immunization to schools. An oral agreement, from a parent, guardian or other person acting in loco parentis for the individual, or directly from the individual, if he or she is an adult or emancipated minor is still necessary. The agreement is effective until revoked.
- CEs may disclose PHI to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the individual's authorization. CEs are required to reasonably limit the amount of PHI disclosed to the minimum necessary to accomplish the workers' compensation purpose.

EXPANDED INDIVIDUAL RIGHTS

Restriction of Certain Health Plan Disclosures

- An individual may now request a CE to restrict certain uses or disclosures of PHI about treatment, payment, or health care operations.
- The Omnibus Rule requires the health care provider to agree to such request if the request is to restrict disclosures to a health plan for payment or health care operations purposes if the PHI at issue pertains to a health care item or service that was paid fully by the individual or the third party other than the health plan.
- CEs must employ methods to flag or make a notation of such PHI in the patient's record to ensure that the information is not inadvertently disclose to a health plan.

Enhanced Access to PHI

- An individual may now request to access to the individual's electronic health records maintained in one or more data sets by CEs in electronic format. CEs must provide access of individual or the third party specified by the individual, the requested data in electronic format, in addition to providing a copy of such information under the HITECH Act.
- CEs are required to upgrade the technology if the technology utilized by the CEs is not capable of providing any form of electronic copy.
- CEs must provide the requested information to the individual or the third party specified by the individual within 30 days. An additional one-time 30-day extension is permitted under certain circumstance.
- CEs are permitted to charge a reasonable cost-based fee for the copies, labor, supplies and electronic media.[7]

PHI OF DECEASED

PHI disclosure for deceased individual

- Under the Omnibus Rule, PHI is of individual is protected for fifty years after the person's death.
- Disclosure of information may be provided to a decedent's family members and others providing care or payment of care prior to death, unless inconsistent with expressed preferences of individual.

[7] Fees associated with systems maintenance, recouping capital for data access, storage and infrastructures are not considered reasonable, cost-based fees.

- The individual may express preferences regarding the retention of the PHI to the CE upon death.

NOTICE OF PRIVACY PRACTICES

Covered Entities Obligation

- CEs must update their Notice of Privacy Practices (NPP) that explains an individual's rights regarding disclosure of their PHI. These disclosures must cover the intended use of the information with a signed authorization by the individual.

Updated NPP must include the following:

- Statements to inform individuals that additional authorization will be required for the release of psychotherapy notes, the use and disclosure for marketing or sale of their PHI.
- A statement about the individual's right to limit disclosure of PHI to a payer in the instance the patient pays for health care services "out of pocket."
- Option for the individual to opt-out of receiving fundraising materials from the CE.
- Information about their individual's right to be notified in the event of a breach of their PHI.
- Communication about unauthorized disclosure and use of individual's PHI for purposes including research, sale, marketing, fundraising, or communication with an individual who has elected to not receive fundraising communications constitutes a violation of the Privacy Rule, and subjects the individual to possible criminal penalties, civil money penalties or other corrective actions.

CIVIL PENALTIES FOR VIOLATIONS

Broadened fines and reach of penalties

- Monetary fines have been increased and broadened to include BAs and subcontractors. Fees range from $100 to $1.5 million based on the level of the following prohibitive parameters: 1) knowledge of breach, 2) reasonable cause, and 3) willful neglect.[8]
- HHS reserves the authority to enforce the penalty and the amount of penalty depends on the number of occurrences or violations, nature and extent of the violation, and the number of individuals affected or harmed. Factors such as the CE's history of general compliance and HIPAA violations are also considered.

[8] Summary of HIPAA Privacy Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html