



New York State Psychiatric Association, Inc.

Area II Council of the American Psychiatric Association
400 Garden City Plaza, Garden City, New York 11530
(516) 542-0077 • www.nyspsych.org

Updated January 26, 2010

NYSPA GUIDANCE DOCUMENT

Summary of the Health Information Technology for Economic and Clinical Health Act (HITECH)

This document is intended to provide NYSPA members with an overview of the health information technology provisions of the American Recovery and Reinvestment Act of 2009.

ACTION ITEMS FOR NYSPA MEMBERS WHO ARE SUBJECT TO HIPAA

- ▶ Adopt form of Notice of Breach of Unsecured Personal Health Information. The Notice of Breach must be used in connection with any unauthorized or inadvertent breaches of personal health information occurring on or after September 23, 2009. The Notice of Breach will be sufficient to comply with both the new federal requirements and New York State law on breach of personal information.
- ▶ Adopt revised Business Associate Agreement, incorporating HITECH changes to the HIPAA privacy and security rules. The revised Business Associate Agreement must be signed by all existing vendors/contractors who have access to personal health information on or before February 17, 2010, and by all new vendors/contractors at time of engagement.
- ▶ Adopt revised Notice of Privacy Practices, incorporating HITECH changes to the HIPAA privacy and security rules. The revised Notice of Privacy Practices should be distributed to all *new* patients at first date of service on or after February 17, 2010. The revised Notice should be made available to *existing* patients upon request and posted in a prominent location at the service delivery site and on the practice website, if applicable.
- ▶ Adopt revised HIPAA Policies and Procedures, incorporating HITECH changes to the HIPAA privacy and security rules. The revised Policies and Procedures are an internal practice document that should be adopted on or before February 17, 2010.

NYSPA is preparing templates for all of the above action items, which will be made available in the members' only section of the NYSPA website (www.nyspsych.org). Further

instruction will follow regarding specific steps to be taken to comply with new rules and requirements.

BACKGROUND

Signed into law in February, 2009, the American Recovery and Reinvestment Act ("ARRA") is a comprehensive economic stimulus bill that also included provisions aimed at encouraging widespread use of health information technology. ARRA incorporates the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which provides \$19 billion in federal funding in support of health information technology initiatives.

HITECH creates a new Office of the National Coordinator for Health Information Technology ("ONCHIT"), to be placed within the purview of the U.S. Department of Health and Human Services ("HHS"). ONCHIT is charged with developing and implementing a national health information technology infrastructure. HITECH also makes extensive changes and clarifications to HIPAA privacy and security regulations.

HIPAA PRIVACY AND SECURITY RULES

Unless otherwise noted, all revisions to the HIPAA privacy and security rules go into effect on **February 17, 2010**, which is one year from the HITECH enactment date. Please note that the breach notification provisions, described in Section II below, apply to breaches occurring on or after **September 23, 2009**.

I. Who is covered by HIPAA?

By way of refresher, HIPAA applies only to health care providers who transmit health information electronically. Electronic transmission means transmission via the Internet, leased lines, dial-up lines, private networks, and the use of magnetic tape, computer discs or compact disks. An electronic transaction includes hiring a billing company to submit bills electronically or having the hospital where a provider is admitted to practice submit electronic claims on the provider's behalf. Once a provider engages in at least one electronic transaction, all health information the provider maintains or transmits becomes subject to HIPAA forever, including paper and oral information.

In addition, a psychiatrist will be a covered entity if a hospital, clinic or other health care facility where the psychiatrist is employed or works as a consultant bills electronically for services under the psychiatrist's name and provider ID number, even if the facility retains the fees received for the services. However, transmitting health information via a fax machine will constitute an electronic transmission of data *only* if the information is exchanged between **two** computer systems (such as those used by a managed care company). If a psychiatrist sends a fax from a paper fax machine, it will not constitute electronic transmission of data, regardless of whom or what type of machine receives the fax.

II. Business Associates

Under current law, business associates are required only by contract to appropriately safeguard the personal health information ("PHI") they receive in the course of their work for covered entities. Now, under HITECH, all of the privacy and security provisions in the HIPAA regulations will apply directly to business associates and they will be subject to the same civil and criminal penalties that apply to covered entities. In addition, a business associate may be subject to further penalties if it becomes aware of a violation made by a covered entity and does not take action. Finally, business associates also will be subject to the new breach notification requirements described in more detail below.

HITECH also clarifies that any organization that provides data transmissions services, such as a health information exchange organization, a regional health information organization, an e-prescribing gateway or any vendor that offers a personal electronic health record to patients is to be treated as a business associate and must sign a business associate agreement.

III. New Notification Requirements

On August 24, 2009, HHS issued an interim final rule entitled Breach Notification for Unsecured Protected Health Information ("Breach Notification Rule"). The Breach Notification Rule applies to all breaches of unsecured PHI occurring on or after September 23, 2009. Yet, in the preamble to the Rule, HHS stated that it will delay enforcement of the Breach Notification Rule until February 22, 2010, to give covered entities additional time to implement the new breach notification procedures. During the interim period, HHS will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

A. Definition of Terms "Breach" and "Unsecured"

Effective September 23, 2009, covered entities are required to provide notification of a breach of "unsecured" PHI. No notice is required in the event of a breach of PHI that is "secured."

The term "breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of such information. The phrase "compromises the security or privacy of health information" means poses a significant risk of financial, reputational or other harm to the individual.

If a breach occurs and a covered entity determines that the breach poses significant harm to the individual, the covered entity must provide written notice to the individual affected as described below. In order to determine whether the breach poses significant harm to the individual, the covered entity should perform a fact-based risk assessment that includes consideration of the following factors: (i) who or what type of entity received access to the information; (ii) steps taken to mitigate harm, such as obtaining satisfactory assurances (e.g., a confidentiality agreement) from the recipient that the information will not be further used or disclosed, or will be destroyed; (iii) if the information was returned prior to it being accessed for an improper purpose; and (iv) the nature, type and amount of information used or disclosed.

As part of HITECH, Congress directed HHS to issue guidance on specific encryption technologies and methodologies to be utilized to "secure" unsecured PHI. Unsecured PHI is

defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS. In April, 2009, HHS issued a Guidance and Request for Information that identified two methods for rendering PHI unusable, unreadable or indecipherable: encryption and destruction.

Encryption is the process of transforming data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The National Institute of Standards and Technology (NIST) has identified valid encryption processes both for data at rest and data in motion. Destruction includes (i) shredding or destruction of paper, film or other hard copy media so that PHI cannot be read or otherwise reconstructed and (ii) clearing, purging or destruction of electronic media consistent with NIST guidelines.

In the April guidance, HHS indicated that use of either of these two methods to "secure" PHI creates a safe harbor that eliminates the need for covered entities and business associates to provide notice in the event of a breach. At the same time, HHS reminded covered entities and business associates to work to mitigate any collateral harmful effects resulting from the breach of "secured" information.

In addition, HHS has identified three specific exceptions to the definition of breach:

- (i) an unintentional acquisition, access or use by a workforce member or person acting under authority of a covered entity or business associate, if made in good faith and within the scope of authority;
- (ii) an inadvertent disclosure by a person at a covered entity or business associate who is authorized to access PHI to another person at the same covered entity or business associate; or
- (iii) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Finally, HHS explicitly excludes "limited data sets" from the breach notification requirement. A limited data set is PHI that excludes 16 direct identifiers, including name, address, telephone number, fax number, email address, social security number, medical record number and others. Under HIPAA, a covered entity may use or disclose a limited data set for research, public health or health care operations purposes without an authorization as long as the intended recipient signs a data use agreement. Under the Breach Notification Rule, unauthorized or inadvertent use or disclosure of a limited data set *that does not also include date of birth or zip code* will not constitute a breach that compromises the security or privacy of PHI.

B. Notification Required

1. Notice to Individuals

In the event of a breach that causes significant harm to the individual, the covered entity must notify the individual in writing. In addition, any business associate that becomes aware of a

breach must notify the covered entity of the breach and identify all individuals whose information has been accessed, acquired or disclosed.

The required notice must be sent without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. A breach will be treated as discovered by the covered entity as of the first day on which the breach is known to the covered entity or would have been known to a covered entity exercising reasonable diligence. The notice must be written in plain language and must contain the following information: (i) brief description of what happened, the date of the breach and the date of discovery, if known; (ii) the type of PHI involved in the breach; (iii) any precautionary steps the individual should take; (iv) description of what the covered entity is doing to investigate and mitigate the breach and prevent future breaches; and (v) contact information for the covered entity, including a toll-free telephone number, e-mail address, website or postal address.

The notice must be sent by first-class mail or by email, if the individual has specified a preference for communication by email. If contact information for the individual in question is insufficient or out-of-date, the covered entity may use a substitute form of notice reasonably calculated to reach the individual. In the event there is insufficient or out-of-date contact information for fewer than 10 individuals whose information was breached, substitute notice may be provided by an alternative form of written notice, telephone or other means.

In the event there is insufficient or out-of-date contact information for 10 or more individuals whose information was breached, the covered entity must post a notice on the homepage of its website for at least 90 days or post conspicuous notice in major print or broadcast media in the geographic area where the affected individuals likely reside and, in both cases, include a toll-free contact number for potentially affected individuals to use. NYSPA understands that these requirements may seem rather onerous and costly for a sole practitioner. Hopefully, when HHS issues additional guidance on these provisions, it will take these concerns into account.

Finally, if the notification is of an urgent nature because of possible imminent misuse of unsecured PHI, a covered entity may contact the individual by telephone or other means, as appropriate, in addition to the written or other forms of notice.

2. Notice to the Media

In the event of a breach affecting more than 500 residents of a State or jurisdiction, the covered entity must, without unreasonable delay and in no case later than 60 calendar days after discovery of the breach, notify prominent media outlets serving the State or jurisdiction.

3. Notice to HHS

For breaches affecting fewer than 500 individuals, a covered entity is required to maintain an annual log of such breaches and provide notice to HHS within 60 days of the end of the calendar year. For breaches affecting 500 or more individuals, a covered entity is required to notify HHS at the same time notice is provided to the individual.

4. Notice provided by Business Associates

If a business associate discovers a breach of unsecured PHI, it must notify the covered entity of such breach without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The business associate shall endeavor to include in its notice identification of each individual whose unsecured PHI was or reasonably believed to have been accessed, acquired, used or disclosed. In addition, the business associate is required to provide the covered entity with any other available information that will assist the covered entity in providing the required notice to the individual(s) affected.

5. Law Enforcement Delay

Following a breach, a covered entity or business associate is required to delay transmission of any of the required forms of notice if it is informed by a law enforcement official that such notice would impede a criminal investigation or cause damage to national security.

6. Special Rules for PHR Vendors/Service Providers

HITECH also requires vendors of personal health records (e.g., Google Health) to provide notice of a breach of security of any identifiable health information maintained in a personal health record (PHR). The vendor must provide notice (i) to each individual whose information was breached and (ii) to the Federal Trade Commission, which, in turn, must notify HHS. A notice requirement is also placed on any third party service providers who provide software support services to a PHR vendor. In the event that the third party service provider discovers a breach, it is required to notify the vendor. PHR vendors must provide notice subject to the same procedures that apply to covered entities and business associates.

C. Interaction with State Breach Notification Laws

In general, any HIPAA rule or regulation that is contrary to a provision of State law will preempt the contrary State law, unless an exception¹ applies. In order to determine whether a state law is contrary to a federal law one must determine whether "a covered entity could find it impossible to comply with both the State and federal requirements." With respect to the federal Breach Notification Rule, HHS has taken the position that "in most cases, a single notification can satisfy the notification requirements under State laws and this regulation."

The New York State law on breach of personal information is called the Information Security Breach and Notification Act.² This Act requires entities, persons or businesses doing business in New York that own or license computerized data to notify a New York resident if an individual's private information is acquired without valid authorization. Private information is defined as unencrypted personal information in combination with one of the following: (1) social security number; (2) driver's license or non-driver ID number; or (3) account number, credit card or debit

¹For example, state laws relating to the privacy of health information that are more stringent than the privacy requirements under HIPAA will not be preempted by HIPAA. However, in the preamble to the rule, HHS states that none of the exceptions to the general HIPAA preemption rule will apply in the case of the Breach Notification Rule.

² Codified at State Technology Law § 208 and General Business Law § 899-aa.

card number and security code, access code or password that permits access to an individual's financial account. Notification to the individual affected is required to be made "in the most expedient time possible and without unreasonable delay."

Under New York State law, notice may be provided in writing, by electronic notice or by telephone. In addition, if the cost of providing notice would exceed \$250,000 or more than 500,000 individuals need to be contacted, an entity may elect to use a substitute form of notice, including email notice, a posting on the entity's website, or notification in major statewide media. The notice must include contact information for the entity and a description of the breached information, including the specific data elements disclosed.

In the event of a breach, NYSPA members will be able to utilize a single form of notice to comply with both the federal Breach Notification Rule and New York State law. First, there is no apparent conflict between the timeframes required for notification. New York law requires notice to be sent in the most expedient time possible and the federal rule requires notice to be sent without unreasonable delay, but no later than 60 days from date of discovery of the breach. Notice sent as soon as reasonably practicable after discovery of the breach will comply with both the State and federal requirements. Second, there is no apparent conflict between the required content of the notice. Since the Breach Notification Rule requires more elements to be included in the notice, compliance with the federal rule automatically constitutes compliance with the State rule.

IV. Expanded Individual Rights Under HITECH

A. Restrictions on Disclosures

Under current law, individuals are entitled to request that a covered entity restrict certain uses and disclosures of their health information for treatment, payment and health care operations, but the covered entity is not required to agree to a requested restriction. Under HITECH, a covered entity *must* comply with a patient's request to restrict information if the information is to be sent to a health plan for payment or health care operations purposes and the disclosure relates to products or services that were paid for solely out-of-pocket (unless the disclosure is otherwise required by law).

B. Minimum Necessary Rule

Under current law, health care providers using, disclosing or requesting PHI are required to use, disclose or request only the minimum necessary amount of information, in other words, the least amount of information required to achieve the purpose of the use, disclosure or request. In order to clarify this term, HITECH directs HHS, within 18 months, to issue guidance on what constitutes "minimum necessary." Until such guidance is issued, covered entities may comply with the minimum necessary rule by limiting the use of PHI to a limited data set, or, if needed, to whatever is the minimum necessary to accomplish the intended purpose. As stated in Section III.A.2. above, a limited data set is PHI that excludes certain direct identifiers of the individual, such as name, address, telephone number, social security number, accounts number, and others.

C. Accounting of Certain Disclosures

Under HIPAA, patients may request that a covered entity provide an accounting of disclosures of their PHI. However, this right to receive an accounting does not apply to routine disclosures for treatment, payment or health care operations. Now, under HITECH, individuals will be entitled to receive an accounting of routine disclosures of PHI that is maintained in an electronic health records system, for the three year period prior to the date of the accounting request. For disclosures made by a business associate, the covered entity can provide the accounting itself or in the alternative provide the individual with contact information for the business associate.

For those covered entities using electronic health records systems as of January 1, 2009, the effective date of the new accounting requirement is January 1, 2014. If the covered entity began using an electronic health records system after January 1, 2009, the effective date of the new requirement will be January 1, 2011, or the date the covered entity acquires the electronic health records system, whichever is later.

D. Prohibition on Sale of Electronic Health Records or PHI

Under HITECH, covered entities and business associates will be prohibited from receiving direct or indirect remuneration in exchange for PHI, unless a valid HIPAA authorization has been signed by the patient, which includes such permission. Exceptions to the authorization requirement include sale of PHI in connection with:

- (i) public health activities;
- (ii) research;
- (iii) treatment of the individual;
- (iv) sale, transfer, merger or consolidation of the covered entity;
- (v) services provided by a business associate, pursuant to a business associate agreement;
- (vi) providing an individual with a copy of their PHI; and
- (vii) other purposes deemed necessary and appropriate by HHS.

This change will take effect six months after promulgation of final rules implementing this section of HITECH.

E. Access to Information in Electronic Format

If a covered entity maintains an electronic health record for an individual, HITECH requires that the individual be permitted to request access to the information in an electronic format or may have the information transmitted electronically to a designated recipient. Any fee charged by the covered entity for the document production cannot exceed the entity's labor costs in responding to the request.

F. Marketing and Health Care Operations

Under HIPAA, marketing means a communication about a product or service that encourages recipients to purchase or use the product or service. Normally, a covered entity is required to

obtain patient authorization prior to making a marketing communication. However, if certain conditions are met, the marketing communication will come under the umbrella of health care operations activities and may be made without patient authorization.

HITECH clarifies that marketing communications are not health care operations (and will require patient authorization) if direct or indirect payment is made in exchange for the marketing communication. However, even if payment is involved, the marketing communication may be considered to be a health care operations activity if *one* of the following three exceptions are met: (i) the communication describes a medication to be prescribed to the recipient and the payment to be made to the covered entity is reasonable in amount; (ii) the communication is made by the covered entity and a valid authorization is obtained; or (iii) the communication is made by a business associate pursuant to a valid business associate agreement.

G. Opt-Out of Fundraising

Under HITECH, the current requirement for covered entities to provide individuals with the chance to "opt-out" of receiving fundraising communications is enhanced. Now, the opt-out language must be presented in a clear and conspicuous manner and any such opt-outs will be treated as a revocation of any prior authorizations.

V. Enhanced Enforcement Activities

HITECH increases HIPAA civil monetary penalty amounts as follows:

Category	Penalty
Violations made where the person had no knowledge (and by exercising reasonable diligence would not have known)	\$100 per violation, not to exceed \$25,000 annually
Violations due to reasonable cause and not due to willful neglect	\$1,000 per violation, not to exceed \$100,000 annually
Violations due to willful neglect that are corrected within 30 days	\$10,000 per violation, not to exceed \$250,000 annually
Violations due to willful neglect but not corrected within 30 days	\$50,000 per violation, not to exceed 1,500,000 annually

In addition, HITECH grants State Attorneys General the ability to bring a civil action enjoining HIPAA violations and seeking damages of \$100 per violation (capped at \$25,000 per year), including costs and attorneys' fees. The HHS Office of Civil Rights is permitted to use corrective action without a penalty in cases where the individual in violation did not know and, by exercising reasonable diligence, would not have known about the violation. Finally, HITECH provides for the addition of criminal penalties for individuals or employees of covered entities who violate HIPAA rules.

Prepared by Rachel A. Fernbach, Esq.
 Associate Executive Director
 Prepared September, 2009

