

**New Regulations Dramatically Affect the Use of  
Electronic Medical Records Data Test Sets  
By Joseph A. Dawson Esq.<sup>1</sup>**

**Introduction:**

New regulations, Affective in 2010 make HIPAA Compliance even tougher for those who use data test sets that contain electronic medical and personal information. These new regulations, not only make it tougher for both Entities, such as Health Care Providers, and their Business Associates to comply with the updated HIPAA Privacy Rule, it now requires Entities and Business Associates to notify individuals, as well as the secretary of the Department of Health and Human Services (HHS) and even the Media in some cases, if a breach of the HIPAA Privacy Rule occurs.

This Article will describe why the new rules apply to the use of data test sets that contain real medical or personal information, what the Privacy Rule and HITECH rules require, and the possible criminal and civil penalties that can be incurred for non-Compliance.

**Electronic Medical Records Data Test Sets (EMRDTs)**

Beginning in the late 1980's and early 1990's, Electronic Medical Records (EMRs) began to be used in large volume. These EMRs were seen as a way to improve the quality of health care, improve the efficiency of health care providers, and help increase the security of patient's personal medical information. However, the current volume of clinical data (and therefore EMRs) essential to the practice of medicine today simply cannot be processed by the unaided human mind. This is why the use of computers and IT applications have become a crucial part of controlling and maintaining EMRs in the health care industry.

Because the IT applications required for transmitting and maintaining EMRs at current technology levels are continuously evolving and increasing in size, it is often necessary to use Data Test Sets (DTSs) to test and maintain IT applications. The use of DTSs to test and maintain IT applications is especially prevalent in the health care industry, because of the sheer volume of EMRs currently in use. In addition, the health care industry's need for testing and maintaining IT applications requires a specific set of DTSs. These test sets include specific information vital to the health care industry.

Throughout this article, when I refer to DTSs, I am referring to Electronic Medical Records Data Test Sets (EMRDTs). These are DTSs specific to the health care industry. EMRDTs are used in the health care industry to perform software validation and training to avoid errors during operations. In most cases, sets of **real** data are used for testing. These real data tests sets are the types of EMRDTs that this article addresses when discussing compliance with any regulations. Finally, in the last section of the article, I will discuss how any AHIPAA compliance issues can be avoided by using synthesized EMRDTs.

---

<sup>1</sup> This article is intended to give general guidance with regard to HIPAA regulations and the use of Electronic Medical Records Data Test Sets. I recommend that Individuals or Entities seek legal council with regard to specific legal questions regarding this subject.

## HIPAA: A Brief Overview<sup>2</sup>

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed into law with the broad goals of enabling better access to health insurance, preventing the miss use of private information, and lowering the overall cost of health care in the United States. With the advent of HIPAA in 1996 and the subsequent security rule in 2003, patient privacy and compliance with HIPAA security standards has become a chief goal in the healthcare industry.

The HIPAA Privacy Rule outlined several standards for protecting any piece of health information that could be used to identify an individual. The final security rule, released in February 2003, identified standards for protection of *electronic* health information that could be used to identify an individual. The HIPAA Privacy Rule protects certain information that Entities use and disclose. This information is called protected health information (PHI), which is generally individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information.

The Privacy Rule also establishes requirements for Entities with regard to their non employee Business Associates (e.g., lawyers, accountants, billing companies, other contractors Software Providers, Integrators, vendors, etc) whose relationship with Entities requires sharing of PHI. The Privacy Rule allows a covered provider or health plan to disclose PHI to a Business Associate if satisfactory written assurance is obtained that the Business Associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the Entity comply with certain of its duties under the Privacy Rule.

## HITECH Act: A brief Overview<sup>3</sup>

In February of 2010, the HIPAA compliance regulations were updated, through Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA). The new federal law now requires Entities and Business Associates to be accountable to HHS and to individuals for proper safeguarding of the private information entrusted to their care. With regard to using EMRDTSs for testing, the new HITECH rules apply two main changes to the HIPAA Privacy Rule.

First, the new regulations make it mandatory for any “Business Associate” of an Entity to also comply with the HIPAA Security Rule.<sup>4</sup> This means that for the first time Business Associates will be regulated by the federal government, just as Entities. Section 13401 of Subtitle D (Privacy) of the HITECH Act (42 USC 17931) states that “[t]he additional requirements of this title that related to security and that are made applicable with respect to Entities shall also be applicable to a Business Associate and shall be incorporated into the Business Associate agreement between the Business Associate and the Entity.” [Public Law 111-5, p.260] In addition, penalties that apply to Entities also

---

2 This section is intended to give a brief overview of the HIPAA regulations. In a later section, I will describe the actual requirements for HIPAA compliance with regard to the use of EMRDTSs.

3 This section is intended to give a brief overview of the HETICH regulations. In a later section, I will describe the actual requirements for compliance with regard to the use of EMRDTSs.

4 In a later section, I will describe why “Business Associates” apply to entities that use or transmit EMRDTSs. For now, I will only give a summary of the new HITECH regulations, so that the reader can have a basis for later discussions.

will apply to Business Associates for noncompliance with the provisions of the Security Rule.

Second, and most importantly, the new rules call for an enforcement of Breach Notification Rules that require notifications for breaches of disclosures of unsecured protected health information discovered on or after the February 22, 2010. [74 *Federal Register* 42757, August 24, 2009]. The Breach Notification Rule applies to Entities and Business Associates, provides obligations for each regarding compilation and reporting of information pertaining to a breach by either party, and requires “incorporation [of those obligations] into the Business Associate Agreement between the Business Associate and the Entity.” [42 USC 17934]

The new regulations, developed by the HHS Office for Civil Rights (OCR), require health care providers and other HIPAA Entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require Business Associates of Entities to notify the Entity of breaches at or by the Business Associate.

### **Why the HIPAA & HITECH Rules Apply To EMRDTs**

Under HIPAA and HITECH rules, when Electronic Medical Data Test Sets (EMRDTs) have “generally individually identifiable health information,” personal information, and medical information, within the test sets AND it is transmitted by, or maintained in, electronic media or any other form or medium, it fall within the definition of the types of Person Health Information (PHI) covered under the rules. When that data is transmitted or used in the form of DTs then it also falls under the HIPAA and HITECH rules.

Entities that use and transmit EMRDTs, such as Health Care Providers, Health Care Plans, Health Care Clearinghouses, Independent Software Providers (ISPs), Integrators, Billing Companies, Billing Software Companies, or purchasers of EMR software fall within either the definition of an Entity or Business Associate, as seen from the below definitions:

Section 106.103 of Title 45 of the Code of Federal Regulations defines an Entity as: (1) A health plan; (2) A health care clearinghouse; or (3) A health care provider, who transmits any health information in electronic form.

The new HITECH rules definition of “Business Associate” is taken from Section 106.103 of Title 45 of the Code of Federal Regulations. This section defines a “Business Associate as: “ ...a person who...on behalf of such Entity...performs, or assists in the performance of...a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or ... provides, ... legal, actuarial, accounting, consulting, data aggregation ..., management, administrative, accreditation, or financial services to or for such Entity, or to or for an organized health care arrangement in which the Entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such Entity or arrangement, or from another Business Associate of such Entity or arrangement, to the person. ... an Entity may be a Business Associate of another Entity.”

5

Within the remainder of this article, when I refer to an “Entity,” I am specifically referring to an Entity that meets the above definition of either an Entity and/or Business Associate and uses or transmits PHI in the form of EMRDTs. Therefore, these Entities fall within the jurisdiction of the HIPAA and HITECH rules.

## **HIPPA Compliance**

To ensure that an Entity is not in violation of the HIPAA Privacy Rule when it uses and/or transmits EMRDTs, the Entity must know what their responsibilities are to become HIPAA compliant. This knowledge will also confirm whether there has been a breach of the HIPAA Privacy Rule that requires the Entity to perform a breach notification under the new HITECH rules.

The HIPAA Privacy Rule describes the basic ways in which an Entity can use or disclose EMRDTs for research (testing) purposes. In general, the rules allow an Entity to use EMRDTs in one of four ways<sup>6</sup>:

- 1) DE-Identifying the EMRDTs;
- 2) Seeking Authorization for use from the Individual for whom the EMRDTs is taken;
- 3) Getting a Waiver of Authorization for use of the EMRDTs from a Privacy Board or Institutional Review Board (IRB); or
- 4) Composing a “Limited Data Set” (LDS) combined with a written “Data Use Agreement” (DUA) to use the EMRDTs.

### **1) DE-Identifying EMRDTs**

Entities may use or disclose health information that is DE-identified without restriction under the Privacy Rule. Entities seeking to release this health information must determine that the

---

*Business Associate:* (1) Except as provided in paragraph (2) of this definition, *Business Associate* means, with respect to an Entity, a person who: (i) On behalf of such Entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the Entity participates, but other than in the capacity of a member of the workforce of such Entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Entity, or to or for an organized health care arrangement in which the Entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such Entity or arrangement, or from another Business Associate of such Entity or arrangement, to the person. (2) an Entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a Business Associate of other Entities participating in such organized health care arrangement. (3) an Entity may be a Business Associate of another Entity.

<sup>6</sup> There are also separate provisions for how PHI can be used or disclosed for activities preparatory to research and for research on decedents’ information but I do not feel that these provisions apply to the use of EMRDTs, so I will not discuss them in this article.

information has been DE-identified using either 1) statistical verification of DE-identification or; 2) by removing certain pieces of information from each record as specified in the Rule.

Entities may use statistical methods to establish DE-identification instead of removing certain identifiers. The Entity may obtain certification by “a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable” that there is a “very small” risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical DE-identification must document the methods used as well as the result of the analysis that justifies the determination. The Entity is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Given the sheer volume of personal information used for testing and how that information is used, it is unlikely that there would be a finding by the statistical specialist that there is a “very small” risk that the information could be used by the recipient to identify an individual. Therefore, this method for assuring compliance with the Privacy Rule, when using EMRDTs, seems impractical.

The Privacy Rule also allows an Entity to DE-identify data by removing certain elements that could be used to identify the individual or the individual’s relatives, employers, or household members, these elements are enumerated in the Privacy Rule. The Entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information. Under this method, the Privacy Rule lists 18 identifying elements, such as names, dates, telephone numbers, etc, which must be removed.<sup>7</sup> It is also important to note that if an Entity engages a Business Associate to DE-identify EMRDTs the Entity must have a written contract with the Business Associate containing the provisions required by the Privacy Rule before it provides PHI to the Business Associate.

DE-identifying EMRDTs according to Privacy Rule standards may enable some limited testing activities. However, most EMRDTs are used to test IT applications that specifically deal with this type of “identifying information” during the course of testing. Removing the 18 “identifying elements” would likely render most EMRDTs useless and, therefore, this method of compliance with the Privacy Rule would be impractical in most EMRDTs situations.

---

<sup>7</sup> The full list of all 18 elements is: 1. Names; 2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census: a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people. b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000; 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; 4. Telephone numbers; 5. Facsimile numbers; 6. Electronic mail addresses; 7. Social security numbers; 8. Medical record numbers; 9. Health plan beneficiary numbers; 10. Account numbers; 11. Certificate/license numbers; 12. Vehicle identifiers and serial numbers, including license plate numbers; 13. Device identifiers and serial numbers; 14. Web universal resource locators (URLs); 15. Internet protocol (IP) address numbers; 16. Biometric identifiers, including fingerprints and voice prints; 17. Full-face photographic images and any comparable images; 18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

## **2) Seeking Authorization for use from the Individual for EMRDTs**

One way the Privacy Rule protects the privacy of PHI is by generally giving individuals the opportunity to agree to the uses and disclosures of their PHI for setting up EMRDTs by signing an Authorization form for uses and disclosures not otherwise permitted by the Rule. The Privacy Rule establishes the right of an individual to authorize an Entity to use and disclose his/her PHI for research and testing purposes. This requirement is in addition to the informed consent to participate in research required under the HHS Protection of Human Subjects Regulations and other applicable Federal and State law. Given the sheer volume of personal and health information required to generate a useful EMRDTs, obtaining written authorization from every individual covered by the EMRDTs would be very impractical and, therefore, I will not describe the exact requirements for an individual written waiver of authorization.<sup>8</sup>

## **3) Obtaining Waiver of Authorization By a Privacy Board or Institutional Review Board (IRB)**

In most cases, testing with EMRDTs cannot be undertaken using health information that has been DE-identified. Also, it usually is not feasible for testers to obtain a signed individual Authorization for all PHI the tester needs. To address these and other situations, the Privacy Rule contains criteria for waiver or alterations of Authorizations by an Individual Review Board (IRB) or another review body called a Privacy Board.

For research and or testing uses and disclosures of PHI, an IRB or Privacy Board may approve a waiver or an alteration of the Authorization requirement in whole or in part. A complete waiver occurs when the IRB or Privacy Board determines that no Authorization will be required for an Entity to use and disclose PHI for a particular research project. An IRB or Privacy Board may also approve a request that removes some PHI, but not all, or alters the requirements for an Authorization (an alteration). The Privacy Rule states that the required documentation must indicate that the IRB followed normal or expedited procedures in reviewing and approving the waiver or alteration. Thus, an IRB's authority to act on waiver or alteration requests under the Privacy Rule is in addition to the other authorities derived from the HHS Protection of Human Subjects Regulations and other applicable statutes and regulations.

Many testing projects take place at multiple sites and/or require the use and disclosure of PHI created or maintained by more than one Entity (collectively, multi-site *projects*). Often, different IRBs are involved in multi-site project reviews. The same situation is expected to occur with Privacy Boards. In some circumstances, Privacy Boards and IRBs will coexist. Where these boards coexist, the Privacy Rule does *not* require approval of a waiver or an alteration of Authorization by both bodies because an Entity may rely on a waiver or an alteration of Authorization approved by any IRB or Privacy Board, without regard to the location of the approving party. HHS has stated (65 *Federal Register* 82692, December 28, 2000) that an Entity's responsibility is to "obtain the documentation that *one* [emphasis added] IRB or privacy board has approved the alteration or waiver of Authorization." Consequently, the Privacy Rule allows a waiver or an alteration of Authorization obtained from a single IRB or Privacy Board to be used to obtain PHI in connection with a multi-site project.

Unlike IRBs, Privacy Boards are alternative review boards authorized by the Privacy Rule to

---

<sup>8</sup> If the reader wishes to see a full explanation of the requirements for a written waiver of authorization, they can do so at the Department of Health and Human Services Website at: [www.hhs.gov](http://www.hhs.gov)

review requests for alteration or waiver of a research Authorization. If an Entity is to use or disclose PHI on the basis of a waiver or an alteration of Authorization from a Privacy Board, the Board must be established in accordance with Section 164.512(i) of the Privacy Rule. These provisions state that:

- Members must have varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on individuals' privacy rights and related interests.
- Each Board must have at least one member who is not affiliated with the Entity or with any Entity conducting or sponsoring the research and who is not related to any person who is affiliated with such entities.
- Members may not have conflicts of interest regarding the projects they review.

If an Entity has used or disclosed PHI for testing with an IRB or Privacy Board approval of waiver or alteration of Authorization, documentation of that approval must be retained by the Entity for 6 years from the date of its creation or the date it was last in effect, whichever is later. Documentation of the waiver or alteration of Authorization must include a statement identifying the IRB or Privacy Board that made the approval and the date of approval. Among other things, the documentation must also include statements that the IRB or Privacy Board has determined that the waiver or alteration of Authorization, in whole or in part, satisfies the following criteria: 1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements: a. An adequate plan to protect health information identifiers from improper use and disclosure. b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so). c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or Entity, except as required by law, for authorized oversight of the research or testing study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule. 2. The research or testing could not practicably be conducted without the waiver or alteration. 3. The research or testing could not practicably be conducted without access to and use of the PHI.

If an Entity or Business Associate chooses to comply with the Privacy Rule by seeking written approval by an IRB or Privacy Board, they must follow all instructions for seeking a waiver of authorization, document all aspects of the waiver procedure and have such documentation available for review for at least 6 years from the date of approval or last use of the waiver. Again, given the volume and complexity of EMRDTs, it may be difficult to obtain a waiver from an IRB or Privacy Board, especially if it is unclear to the board why and how the EMRDTs are being used.

#### **4) Limited Data Sets and Written Data Use Agreement**

The Privacy Rule permits an Entity, without obtaining an Authorization or documentation of a waiver or an alteration of Authorization, to use and disclose PHI included in a Limited Data Set. An Entity may use and disclose a Limited Data Set for research or testing activities conducted by itself, another Entity, or a Business Associate if the disclosing Entity and the Limited Data Set recipient enter into a data use agreement. Limited Data Sets may be used or disclosed only for purposes of research, public health, or health care operations. Because Limited Data Sets may contain identifiable information, they are still PHI.

Limited Data Sets (LDS) refer to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

A Data Use Agreement (DUA) is an agreement into which the Entity enters with the intended recipient of a Limited Data Set that establishes the ways in which the information in the Limited Data Set may be used and how it will be protected.

A Limited Data Set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule's Limited Data Set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. Sixteen "identifiers," such as names, addresses, telephone numbers, etc.<sup>9</sup> must be removed from health information if the data are to qualify as a Limited Data Set.

A data use agreement is the means by which Entities obtain satisfactory assurances that the recipient of the Limited Data Set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a Limited Data Set from an Entity is an employee or otherwise a member of the Entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the Entity and the Limited Data Set recipient. The Privacy Rule requires a data use agreement to contain the following provisions: 1) Specific permitted uses and disclosures of the Limited Data Set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the Entity, would violate the Privacy Rule); 2) Identify who is permitted to use or receive the Limited Data Set; 3) Stipulations that the recipient will not use or disclose the information other than permitted by the agreement or otherwise required by law; 4) Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the Entity any uses or disclosures in violation of the agreement of which the recipient becomes aware; 5) Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information; 6) Not identify the information or contact the individuals.

If an Entity is the recipient of a Limited Data Set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the Entity providing the Limited Data Set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the Entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the Entity must discontinue disclosure of PHI to the recipient and notify HHS; 7) Section 164.512 of the Privacy Rule also establishes specific PHI uses and disclosures that an Entity is permitted to make for research without an Authorization, a waiver or an alteration of Authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

---

<sup>9</sup> The full list of 16 identifiers is as follows: 1 Names; 2 Postal address information, other than town or city, state, and ZIP Code.; 3 Telephone numbers.; 4 Fax numbers; 5 Electronic mail addresses.; 6 Social security numbers; 7 Medical record numbers; 8 Health plan beneficiary numbers; 9 Account numbers; 10 Certificate/license numbers; 11 Vehicle identifiers and serial numbers, including license plate numbers; 12 Device identifiers and serial numbers; 13 Web universal resource locators (URLs); 14 Internet protocol (IP) address numbers; 15 Biometric identifiers, including fingerprints and voiceprints; 16 Full-face photographic images and any comparable images.

## **Not All State Laws are Preempted by Federal Regulations**

In general, the Privacy Rule overrides (or preempts) State laws relating to the privacy of health information that are contrary to the Rule. Any provision of State law that is not contrary to a provision of the Privacy Rule will remain in full force and effect, so that Entities will continue to have to follow such State laws in addition to the Privacy Rule. However, even where a State law is contrary to the Privacy Rule, there are certain exceptions where the Privacy Rule will not override the contrary State law. For example, State laws that relates to the privacy of individually identifiable health information and is both contrary to and more stringent than the Privacy Rule will continue to stand. In addition, contrary laws and procedures established under State law that provide for reporting of disease or injury, child abuse, birth or death, or for conducting public health surveillance, investigation, and intervention also are not overridden by the Privacy Rule.

## **HITECH Act Compliance with The New Rules**

As stated above, under the new HITECH Act a “Business Associate” of an Entity will now be held to the same compliance standards as an Entity when it comes to compliance with the HIPAA Privacy Rule. I believe that any Entity that uses real personal or medical information to form EMRDTs falls within the jurisdiction of the new HITECH Act compliance rules.

Breach notification regulations, issued August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring Entities and their Business Associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

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. There are three exceptions to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of an Entity or Business Associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at an Entity or Business Associate to another person authorized to access protected health information at the Entity or Business Associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the Entity or Business Associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Following a breach of unsecured protected health information Entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, Business Associates must notify Entities that a breach has occurred.

**Individual Notice:** Entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such

notices electronically. If the Entity has insufficient or out-of-date contact information for 10 or more individuals, the Entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the Entity has insufficient or out-of-date contact information for fewer than 10 individuals, the Entity may provide substitute notice by an alternative form of written, telephone, or other means. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the Entity to determine if their protected health information was involved in the breach.

**Media Notice:** Entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

**Notice to the Secretary:** In addition to notifying affected individuals and the media (where appropriate), Entities must notify the Secretary of breaches of unsecured protected health information. Entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, Entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the Entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

**Notification by a Business Associate:** If a breach of unsecured protected health information occurs at or by a Business Associate, the Business Associate must notify the Entity following the discovery of the breach. A Business Associate must provide notice to the Entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the Business Associate should provide the Entity with the identification of each individual affected by the breach as well as any information required to be provided by the Entity in its notification to affected individuals.

Entities and Business Associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. This section also requires Entities to comply with several other provisions of the Privacy Rule with respect to breach notification. For example, Entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

For breaches that affect fewer than 500 individuals, an Entity must provide the Secretary with notice annually. All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. Notifications of all breaches occurring after the effective date in 2009 must be submitted by March 1, 2010. This notice must be submitted electronically and completing all information required on a breach notification form. A separate form must be completed for every breach that has occurred during the calendar year. If an Entity that has submitted a breach notification form to the Secretary discovers additional information to report, the Entity may submit an additional form, checking the appropriate box to signal that it is an updated submission.

### **Penalties for Non-Compliance**

Consistent with the principles for achieving compliance provided in the Privacy Rule, OCR will seek the cooperation of Entities and may provide technical assistance to help them comply voluntarily with the Privacy Rule. Entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution.

The Office for Civil Rights (OCR) may impose civil money penalties on an Entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the Entity knew or should have known of the failure to comply, or whether the Entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

	<b>For violations occurring prior to 2/18/2009</b>	<b>For violations occurring on or after 2/18/2009</b>
<b>Penalty Amount</b>	Up to \$100 per violation	\$100 to \$50,000 or more per violation
<b>Calendar Year Cap</b>	\$25,000	\$1,500,000

A penalty will not be imposed for violations in certain circumstances, such as if:

- the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
- the Department of Justice has imposed a criminal penalty for the failure to comply (see below).

In addition, OCR may choose to reduce a penalty if the failure to comply was due to reasonable cause and the penalty would be excessive given the nature and extent of the noncompliance. Before OCR imposes a penalty, it will notify the Entity and provide the Entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be submitted to OCR within 30 days of receipt of the notice. In addition, if OCR states that it intends to impose a penalty, an Entity has the right to request an administrative hearing to appeal the proposed penalty.

Finally, a person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to \$50,000 and up to

one-year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Privacy Rule.

### **The Solution: Synthesized EMRDTs**

It *is* possible for a healthcare organization to implement and test an EMR system *and* comply with HIPAA Privacy and Security rules. In complying with the HIPAA standards, however, many Healthcare providers are not realizing the full potential of their EMR systems. Without the ability to exchange information securely while maintaining data integrity, the EMR systems today are no better than electronic versions of paper records. Many private practice and primary care physicians, who see the majority of patients in the country, will find it difficult to make the initial investment in the IT hardware, software, and support necessary to implement and test an EMR system. No matter the status of IT or financial resources however, compliance with HIPAA is mandatory.

In some cases in an effort to save on testing costs, Entities may use small subsets of real data for testing. If an Entity uses real data for its' EMRDTs and does not follow HIPAA Privacy Rule compliance standards it will be in breach of the regulations and this will require notification of the breach under the new rules.

One way to avoid and HIPAA compliance or breach notification issues is to use synthetic Data Test Sets. The use of synthetic EMRDTs does not fall under the jurisdiction of the HIPAA Privacy Rule and, therefore, enables the Entity to properly test its IT applications without fear of any civil or criminal repercussions.