

HOW THE ECONOMIC STIMULUS ACT WILL AFFECT YOUR MEDICAL PRACTICE: THE GOOD, THE BAD AND THE UGLY

By: Gary Brenner, MBA, JD

When new legislation is passed by Congress, people often think it addresses a new plan or vision of where the country is headed. Many times, however, the new legislation addresses a plan that has been discussed and debated for years but lies dormant because of the lack of funding. Over time, political forces may gather with enough strength to pass legislation that will fund and implement the plan. HIPAA is an example of how this evolution occurs.

The year was 1996. Garry Kasparov defeated Deep Blue in a second chess match, the O.J. Simpson trial began, and a cloned sheep named Dolly was created. It was during this year that Congress passed an Act that was entitled “The Health Insurance Portability Accountability Act of 1996” (HIPAA). At the time, the common understanding of HIPAA was to ensure that employees would be able to carry their healthcare insurance coverage from one employer to another. However, many people did not understand that HIPAA also addressed Congress’ desire to improve the efficiency of Medicare. The Act stated, “[n]ot later than 3 months after August 21, 1996, the Secretary shall establish a program under which the Secretary shall encourage individuals to submit to the Secretary suggestions on methods to improve the efficiency of the Medicare program.” Congress delegated the task of privacy and efficiency to the Department of Health and Human Services (HHS). In addition, because health insurance coverage was required to be portable, it was foreseeable that millions of health records would be transferred among 3rd party payers through electronic means which could be subject to potential abuse by prying eyes. Since 2000, Congress has passed new laws, and HHS has issued regulations, that have addressed security, privacy, and the digital conversion of patient health records.

When the American Recovery and Reinvestment Act of 2009 (Recovery Act) was discussed and debated within the new Obama Administration and with members of Congress before it was passed, it was presumed that money would be borrowed by the federal government to pay for government programs for the purpose of stimulating the economy as well as to bring change to various aspects of our society. As it related to healthcare, the dormant plan of implementing a program that allowed for the electronic exchange and use of health information to improve the quality of healthcare, while saving the federal government substantial amounts of money, was seen as the ideal program to be funded by the Recovery Act. The Recovery Act became law on February 17, 2009. The law cobbled together supplemental appropriations for FY2009 which flowed to federal departments and agencies for a variety purposes. Incorporated into the Recovery Act is the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act attempts to support the nationwide electronic exchange and use of health information in a secure, private and accurate manner. Because the HITECH Act merges together the use of electronic records with the concern for the privacy of patient records and essentially amend HIPAA, the Act will be referred to in this article as “HIPAA 2009”.

Congress' Goals for HIPAA 2009

Three key Congressional committees collaborated to state the goals for the new program. These goals lay the foundation for HIPAA 2009 and will serve as the outline for all of the regulations that are about to be promulgated.

The Committees jointly started with the following preamble and then listed their goals:

This health information technology legislation improves and expands current Federal privacy and security protections for health information. As healthcare providers move to exchanging large amounts of health information electronically, it is important to ensure that such information remains private and secure. The bill accomplishes this by:

- *Establishing a Federal breach notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.*
- *Ensuring that new entities that were not contemplated when the Federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.*
- *Providing transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record.*
- *Shutting down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without their authorization.*
- *Requiring that providers attain authorization from a patient in order to use their health information for marketing and fundraising activities.*
- *Strengthening enforcement of Federal privacy and security laws by increasing penalties for violations and providing greater resources for enforcement and oversight activities.*

Source: Staff of the Committees on Energy and commerce, Ways and Means, and Science and Technology, January 16, 2009.

Summary of HIPAA 2009

The Good. The Department of Health and Human Services (HHS) will reimburse office-based physicians if they purchase and use an electronic health record (EHR) system. The maximum amount that each physician can receive is \$44,000.

The Bad. The EHR system must be "certified"; however, certification's standards have not been established. The physician must demonstrate that it is a "meaningful user" of its EHR

system. However, the definition of meaningful user has not been defined. There are new notification requirements for breaches of protected health information (PHI). Physicians must keep an accounting of all disclosures of PHI. Security requirements of PHI are enhanced.

The Ugly. The penalties for violating a patient's privacy by disclosing unsecured PHI have significantly increased. These new penalties became effective on February 17, 2009 (the day HIPAA 2009 was passed) even though the data breach notification regulations from HHS are not expected to become effective until September 15, 2009. In addition, a physician can be sued for damages and may be required to pay legal fees. As if this was not enough, the Attorney General for each State is authorized to share with affected patients a percentage of any civil monetary penalty that is collected from a healthcare provider. The regulations regarding this novel approach are being formulated and will be published.

There are four tiers of penalties:

- **\$100 - \$50,000** - For each violation in which the person did not know and by exercising reasonable diligence would not have known that a violation had occurred.
- **\$1,000 - \$50,000** - For each violation that was due to reasonable cause and not to willful neglect.
- **\$10,000 - \$50,000** - For each violation due to willful neglect but is corrected within 30 days.
- **\$50,000 or more** - For each willful violation that is not corrected within 30 days.

How the Incentive Works under HIPAA 2009

The Carrot. For a physician to qualify for the incentive, the physician must show that it is a "meaningful" user of an EHR system that is certified. Many people believe the certification will be performed by the not-for-profit Certification Commission on Healthcare Information Technology (CCHIT). At a minimum, expect that a certified EHR system must be able to engage in the electronic exchange of health information. More than likely, HHS will require a physician to submit information on clinical quality measures.

To receive the entire \$44,000 incentive payment, the physician must implement and use an EHR system by the year 2011 or 2012. The incentive system has the following payment schedule:

\$18,000 - year 1 (if implemented in 2011 or 2012)

\$15,000 - year 1 (if implemented after 2012)

\$12,000 - year 2

\$ 8,000 - year 3

\$ 4,000 - year 4

\$ 2,000 - year 5

The good news is that if a physician does not implement an EHR system until 2013 or 2014, the physician is still entitled to receive incentive payments but the total amount will be reduced. For example, if a physician adopts an EHR system in 2013, the physician will receive \$39,000. If a physician adopts in 2014, the physician will receive \$35,000. The last year to adopt and then receive the incentive is 2014. If a physician adopts in 2015 or thereafter, the physician will not receive any incentive payments. In all cases, the last year in which payment will be made under the plan is 2016. For example, if a physician adopts in 2014, the physician will receive incentive payments for the years 2014 through 2016.

The Stick. If a physician is not a “meaningful” EHR user starting in 2015, the physician’s Medicare reimbursements will be reduced to 99% of the Medicare fee. Each year the Medicare fee will be reduced by 1% as follows: in 2016, the physician will receive 98% of the Medicare fee; in 2017, the physician will receive 97% of the Medicare fee; and in 2018, the physician will receive 96% of the Medicare fee. Each year thereafter, the Medicare fee will be reduced by 1% until it reaches 95% of the Medicare fee.

Types of Information that Is PHI

PHI is defined as individually identifiable health information that is created, stored, transmitted or received by electronic, paper, or oral means.

Information that should be treated as PHI includes personal data that is both individually identifiable and contains Health related information. Examples of personal data that is individually identifiable are the patient’s name, address, telephone numbers, fax number, email address, birth date, social security number, identity of family members and their address, identity of employer, medical record number, vehicle identification number, web Universal Resource Locators (URLs), internet protocol (IP) address numbers, health plan beneficiary number, finger or voice prints, or any other characteristic that could uniquely identify the individual. Examples of health related information are treatment notes, patient history, family history, laboratory, and other test results, medication lists, photographs and x- rays, and allergy information.

PHI can be used as needed for the treatment of the patient, payment for healthcare services, and the operations of the healthcare provider without receiving specific consent from the patient. However, when the use of patient information is for something other than these activities, written consent from the patient is required before PHI can be disclosed.

HIPAA’s Requirement to Protect Privacy and Provide Patient Access

In a nutshell, HIPAA 2009 requires a healthcare provider to do the following: (1) Have clear privacy procedures and a designated person to manage the procedures. (2) Obtain training

in privacy procedures and ensure that everyone within the medical office follows the procedures. (3) Secure patient records containing PHI so that they are not easily available to persons who have no right to see the information. (4) Restrict the release of information to the minimum needed (regardless of the purpose of the release) so that at all times information is to be shared strictly on a “need to know” basis. (5) Obtain specific written consent from the patient for any disclosure of PHI that is outside of treatment, payment, or the operation of the medical practice. (6) Explain to patients their privacy rights, how their information may be used and by whom, and for what purpose. (7) Allow the patient to access its own health information at reasonable times and cost. (8) Understand the patient has the right to cancel its permission to allow the physician to disclose PHI to others, and this cancellation may occur at any time. (9) Require that any outside organization, which is to receive a patient’s PHI, enter into a written business associate agreement that obligates the organization to comply with privacy protection rules in the same way the medical practice is required to comply.

Further, computer screens should be protected from reading by unauthorized persons to include members of the staff. PHI files and other written records should be secure and not easily accessed by the public. PHI should be disposed of in a secure manner, such as by shredding.

In general, the health information privacy and security provisions of HIPAA 2009 will take effect on February 17, 2010 after the regulations have been published. Between now and then, expect a flurry of regulations from HHS.

Notice Is Mandatory When There Has Been a Breach of Unsecured PHI

Definition of a Breach

A “breach” is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. PHI is considered “unsecured” PHI if it is not secured by a technology standard (developed or credited by a standards organization accredited by ANSI) that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

When and How Notice Must Be Sent and to Whom

When Notice Must Be Sent. Notice of a breach must be sent without unreasonable delay and never later than 60 days following the discovery of the breach.

Notice to Individuals. Written notice must be sent to all individuals by first class mail whose information was accessed by the unauthorized person. The notice that unsecured PHI has been breached must include the following information: (1) A brief description of what happened, including the date of the breach, and the date of the discovery of the breach (if known). (2) A description of the types of unsecured PHI that were involved in the breach (such as name, social security number, date of birth, home address, account number, or disability code). (3) The steps individuals should take to protect themselves from potential harm resulting from the breach. (4) A brief description of what the healthcare provider involved is doing to investigate the breach, to

mitigate losses and to protect against any further breaches. (5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an email address, website, or postal address.

Notice to HHS. Written notice is required to be provided to HHS if the breach involved 500 or more individuals. The notice must be provided immediately. If the breach involved less than 500 individuals, the healthcare provider may maintain a log of such breach occurring and annually submit the log to HHS documenting the breaches that occurred during the year involved.

Notice to the Media. Notice shall be provided to prominent media outlets serving the State of California (or jurisdiction), following the discovery of unsecured PHI that has been acquired or disclosed which involves more than 500 residents of the State of California (or the jurisdiction).

Final Regulations Are Coming. Final regulations regarding breach notification are to be published no later than August 16, 2009. The new breach notification requirements will become effective 30 days after the date the final regulations are promulgated. The target date is September 15, 2009 as the most probable date in which regulations will go into effect, unless HHS publishes its regulations earlier.

Types of Disclosure of PHI

There are three types of disclosure of PHI, which are the following: permitted, authorized, and required. If a disclosure does not fall within one of these three categories, then it is unauthorized and considered a breach of PHI that requires reporting to the individual affected and to HHS.

Permitted disclosure is defined as any disclosure to the patient, any disclosure related to treatment, payment, or healthcare operations in compliance with 45 C.F.R. §164.506, and in certain instances disclosure to a business associate.

An authorized disclosure is the result of a valid written authorization from the patient that satisfies the requirements under 45 C.F.R. §164.508.

A required disclosure is defined as a disclosure requested by the patient, required by HHS, required by law, or required for a judicial or administrative proceedings.

Accounting for Disclosures

The terms “use” and “disclosure” are often confused. A “use” is defined as utilization of PHI within the healthcare organization and is under the direct control of the organization. For example, when a physician reviews a patient’s medical records as part of the treatment process, it constitutes a use of PHI. A “disclosure” is defined as any release of PHI that is outside of the healthcare organization (that is holding PHI). For example, if PHI is given to a consultant to render an opinion regarding a patient’s condition, it would constitute a disclosure. Under

HIPAA 2009, a patient whose PHI is held by a healthcare provider can obtain an accounting of all disclosures made by the healthcare provider (with certain exceptions) for a period of 3 years prior to the date the request is made. As a consequence, a healthcare provider is required to keep a record of all disclosures of PHI. This record keeping responsibility is called “accounting disclosure”.

Essentially, the exceptions to the requirement of providing an accounting disclosure are the following: (a) disclosure related to treatment of the patient, payment, or healthcare operations; (b) disclosure pursuant to a valid authorization; (c) disclosure for national security or intelligence purposes; (d) disclosure to persons involved in the patient’s healthcare; (e) disclosure to a correctional institution or law enforcement officials; or (f) disclosure that is part of a limited data set in accordance with 45 C.F.R. § 164.54(e).

There are two different effective dates for the accounting disclosure to be put into effect and ready for use. For healthcare providers and business associates currently using an EHR system, the effective date is January 1, 2014. For healthcare providers and business associates that require an EHR system after January 1, 2009, the effective date is the later of January 1, 2011 or the date the EHR system is acquired.

Patient’s Right to Restrict Access

If a patient requests that a healthcare provider not disclose the patient’s PHI, that request must be honored if the request is to restrict disclosure to a health plan for purposes of carrying out payment or healthcare operations (and is not for purposes of carrying out treatment), and the patient’s PHI pertains solely to a healthcare item or service for which the healthcare provider involved has been paid in full.

Enforcement of HIPAA 2009

Under the old law, if a patient wanted to seek legal enforcement of a HIPAA violation, HHS was the sole agency authorized to act on behalf of the patient. Under HIPAA 2009, the enforcement has been delegated to the Attorney General of each State. In other words, the Attorney General of each State has authority to file a civil lawsuit in U.S. District Court on behalf of the affected residents of the State to stop violations of the privacy of the PHI and to obtain damages on behalf of the affected residents of the State. HIPAA 2009 provides that an individual who is harmed by a violation may receive a percentage of any civil monetary penalty or monetary settlement that is collected. HHS is required to establish regulations regarding the methodology to calculate the percentage of the monetary penalty to be distributed to harmed individuals. Moreover, the court, in its discretion may award the cost of the lawsuit and reasonable attorney’s fees to the State in compensation for bringing the legal action.

Because of the ominous enforcement provisions of HIPAA 2009, there has been much discussion as to what is acceptable electronic security. For the first year beginning after the date of the enactment of HIPAA 2009, and annually thereafter, HHS is required to issue guidance regarding the most effective and appropriate technical safeguards for use in carrying out security standards to keep PHI secure.

Marketing Products and Services to Patients Is Severely Restricted

Under the old HIPAA rules, a use or disclosure of PHI was allowed for marketing purposes if the communication was made for the purpose of describing a health related product or services that is included in the plan of benefits, the healthcare provider was providing treatment to the recipient, or there was a recommendation for alternative treatment. This was allowed even if the healthcare provider was paid by a third party to make a communication.

Under HIPAA 2009, a healthcare provider is prohibited from making any types of communication in exchange for payment without specific authorization from the recipient unless the following conditions are satisfied: (a) the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication, and (b) the payment received by the healthcare provider for making the communication is a “reasonable amount”. HHS will define a “reasonable amount”.

Business Associates Treated the Same As Covered Entities

Under the old HIPAA rules, business associates were not governed by HIPAA regulations; instead, they were governed by a business associate contract entered into with the healthcare provider. If a business associate violated the agreement by releasing PHI, the dispute was between the healthcare provider and the business associate to be decided by civil litigation. Under HIPAA 2009, a business associate is now subject to the same regulations that apply to a healthcare provider and is subject to the same civil and criminal penalties.

Gary Brenner is a business attorney who represents clients engaged in various areas of business activity which includes healthcare services. He can be reached at 110 West C Street, Suite 1905, San Diego, CA 92101; (619) 237-8899; e-mail: gbrenner@sonic.net.