



Connecting Lawyers and Communities

# Legal Lines

Legal Issues for Nonprofits

*Prepared for Community Legal Resources by  
Susan H. Patton, Butzel Long*

## NEW HIPAA REGULATIONS: OPPORTUNITIES AND BURDENS ON SMALL NONPROFIT HEALTH CARE FACILITIES

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that imposes non-discrimination and other requirements on employer-sponsored health plans. On February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA) into law. The ARRA is a stimulus package that makes significant changes to HIPAA. While these amendments impact a broad range of constituents, this article focuses on small nonprofit health facilities and how these changes affect them.

This article addresses a) obtaining federal stimulus dollars under HITECH; b) general HIPAA requirements; c) breach notification rules; d) encryptions rule; e) FTC rules for internet based businesses; and f) enforcement dates.

### **Federal Stimulus Dollars available under HITECH**

Nonprofit Health Care Providers Should Grab New Federal Money!

Nonprofit FQHCs, look-alikes, clinics, counseling services, case managers and other health care providers should act quickly, but carefully, to receive federal stimulus dollars by automating their practices with an electronic health record (EHR) system. Under the *Health Information Technology for Economic and Clinical Health* (HITECH) provisions of the ARRA legislation, the federal government is offering funding to create a network of electronic medical records (EMR) through the “acquisition of Health Information Technology (HIT) systems.” This funding can be used to support the acquisition of HIT in a number of ways including construction, renovation, equipment and software licenses.

Additional new grant dollars are available through the Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONCHIT). For example, FQHC’s can be paid up to 85 percent of “allowable costs” (as determined by HHS) for the acquisition, implementation (including training), upgrade,

maintenance, and use of a “certified electronic health record” system (certified by the Certification Commission for Health Information Technology--CCHIT).

There are also capital Improvement Program (CIP) funding opportunities. Funds range from \$250K and up. As a result of recent changes in Stark laws and the Anti-Kickback Statute, FQHCs, look-alikes, clinics, counseling services and other health care providers are able to receive money, information technology (IT) equipment, software and the services of IT staff without running afoul of prohibitions relating to referrals. Nonprofit health care providers can tap any number of public and private funding sources to help pay for these upgrades.

Nonprofit health care providers can apply for funding from either Medicare or Medicaid incentives, but not both. Medicare incentives add up to \$44,000 per physician if there is meaningful use of a qualifying electronic medical record from the earliest eligibility dates, which are 2010-2011. For Medicare, physicians are defined to include physicians, optometrists, chiropractors and dentists. For Medicaid incentives, eligible providers are more broadly defined and include certified nurse midwives, nurse practitioners and physician assistants as well as physicians.

The ARRA defines meaningful EHR use as: (1) use of certified EHR technology in a demonstrably meaningful manner, including e-prescribing; (2) use of certified EHR technology that allows for the electronic exchange of health information to improve the quality of health care, such as promoting care coordination; and (3) reporting on clinical quality measures and other measures selected by the Secretary of the U.S. Department of Health and Human Services using certified EHR technology<sup>1</sup>. A user can establish that they are a “meaningful user” by demonstrating the use of the functionality for electronic prescribing, data sharing, and clinical quality reporting.

Nonprofit health care providers should begin immediately, but carefully, to search for and implement a certified EHR, or fine-tune their existing systems to ensure qualification for the incentives. If a provider cannot show effective “meaningful use” of its EHR system, when the incentive period starts in 2011, it will forfeit additional money until meaningful use is achieved. While Medicaid currently contemplates no penalties, nonprofit health care providers that elect the Medicare incentives will have their Medicare fee schedule reduced by 1% in 2015, 2% in 2016 and 3% in 2017. Penalties will apply to hospitals that are not using and reporting by October 2014.

---

<sup>1</sup> The American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111-5, 111th Cong., 1st sess. (2009), §.4101(a) (new section 1848(o)(2)(A) of the Social Security Act (42 U.S.C. 1395w-4).

## **General HIPAA Requirements and changes**

Important new personal health information (PHI) privacy and security rules will have an enormous impact on the operations and use of technology by health care providers, health plans, health care clearinghouses and their business associates (who are now substantially, directly regulated in the same manner as covered entities). Health information privacy is a populist issue and critical to the trust required to take patient care and the health industry into the electronic age.

Breaches of trust resulting from the unauthorized use and disclosure of e-PHI will be subject to heightened enforcement efforts and stiff new penalties. Stringent new requirements will be paired with new, tiered, civil and criminal penalties, with all being serious and expensive. Especially egregious breaches can result in fines of up to \$1,500,000.00, mandatory disclosure to all individuals involved and mandatory notice to the media in the event that more than 500 individuals have e-PHI that is disclosed in situations where individuals may be harmed.

Nonprofit health care providers and business associates with access to e-PHI have until mid-February to accomplish changes in the way they do business before enforcement and penalties apply, but compliance is expected as soon as mid-September 2009.

The general requirements of the HIPAA Security Rule require that covered entities and business associates do the following:

1. Ensure the confidentiality, integrity, and availability of all the e-PHI the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
4. Ensure compliance by the workforce.

## **Breach Notification Rules for Unsecured e-PHI**

It is time to update policies and procedures, audit operations and IT to avoid strict new penalties. When the privacy of “unsecured” e-PHI is breached, new “breach notification rules” require health care providers, health plans, health care clearinghouses and their business associates to undertake an array of mandatory notifications, undertake mitigation strategies and indemnify for losses. An exception exists for “secured” encrypted information and for information that does not result in a significant risk of financial, reputational or other harm to an individual as determined

*Community Legal Resources*  
615 Griswold · Suite 1400 · Detroit · Michigan · 48226  
Phone: 313/962-3171 · Fax: 313/962-0797  
[www.clronline.org](http://www.clronline.org)

by a risk analysis in which the burden is on the covered entity or business associate to prove why breach notification is not required.

The breach notification rules are the most recent series of rules that HHS is issuing to implement new and stricter personal health information privacy and data security requirements for covered entities which were added to HIPAA under the Health Information Technology for Economic and Clinical Health (HITECH) Act. This Act was signed into law on February 17, 2009 as part of the ARRA.

The new breach notification provisions require that covered entities and their business associates undertake the following mandatory actions:

- Notice to patients of breaches within 60 days, from the date the breach was actually discovered or the date it should have been discovered by exercising reasonable diligence
- Notice to covered entities by business associates when business associates discover a breach of their own or that of a subcontractor or agent
- Notice to “prominent media outlets” on breaches of 500 individuals or more
- Notice to “next of kin” on breaches of patients who are deceased
- Notice to the Secretary of HHS of breaches of 500 or more
- Annual notice to the Secretary of HHS of breaches of less than 500 of “unsecured PHI” that pose a significant financial risk or other harm to the individual, such as financial or reputation harm.

The new rules also establish mitigation minimums and indemnification minimums. Mitigation minimums include toll free numbers, web sites, credit reporting and counseling, among other expensive actions. Exceptions to the breach notification requirements include inadvertent “peeks” and “disclosures” of e-PHI by otherwise authorized individuals in situations where the information is not disclosed further and breaches involving e-PHI secured through encryption.

### **Encryptions Rule and Technology Mandates**

Encryption is a remedy for getting a good night’s sleep. A health reform priority is increasing interoperability among healthcare stakeholders. Financial incentives and new regulations propel the drive toward making health information and data transmissible via open networks while keeping e-PHI safe from unauthorized use or disclosure. With the push is towards increased use of electronic transactions in healthcare, most covered entities and their business associates will be using open systems.

New encryption rules published on April 17, 2009 establish exactly when and how e-PHI is “secured” in its various data states: ‘data in motion’ (i.e., data that is moving through a network,

*Community Legal Resources*  
615 Griswold · Suite 1400 · Detroit · Michigan · 48226  
Phone: 313/962-3171 · Fax: 313/962-0797  
[www.clronline.org](http://www.clronline.org)

including wireless transmission); ‘data at rest’ (i.e., data that resides in databases, file systems, and other structured storage methods); ‘data in use’ (i.e., data in the process of being created, retrieved, updated, or deleted); or ‘data disposed’ (e.g., discarded paper records or recycled electronic media).

While styled as “guidance,” the encryption rules are very directive. Covered entities and their business associates should encrypt data in all data states in accordance with HHS standards found in NIST 800-111 and FIPS 140-2. Individuals and organizations that meet these encryption requirements have suitably “secured” their e-PHI and rendered it “unusable, unreadable or indecipherable to unauthorized individuals.” Breaches of “secured” e-PHI are exempt from the onerous breach notification rules described above.

Data comprising e-PHI can be vulnerable to a breach in any of the commonly recognized data states. Encryption is the new key to securing e-PHI in its various data states. In securing data by encryption, a nonprofit need not worry about data breaches requiring notification.

### **Federal Trade Commission (FTC) Rules for Internet Based Businesses**

The Federal Trade Commission protects consumers from fraudulent, deceptive, and unfair business practices and provides information to help spot, stop, and avoid them. On August 17, 2009, the Federal Trade Commission (FTC) issued a rule requiring some Internet-based businesses to notify consumers when they’ve had a breach of their PHI. The rule applies to both vendors of personal health records – which provide online repositories that people can use to keep track of their health information – and entities that offer third-party applications for personal health records. These applications could include, for example, devices such as blood pressure cuffs or pedometers whose readings consumers can upload into their personal health records. The FTC breach notification requirements are similar to those required by HIPAA and are intended to fill gap because many of these entities are not subject to the privacy and security requirements of HIPAA.

### **Enforcement Dates and Summary**

These new HIPAA rules will have a practical impact on all aspects of business operations, including the use of portable work stations, laptops, blackberries and other hand held devices, storage, transmission standards, technology upgrades business processes, encryption, passwords, physical floor plan layouts, storage and destruction of electronic protected health information e-PHI, insurance and risk management, personnel training and disciplinary actions against personnel involved in breaches of e-PHI.

*Community Legal Resources*  
615 Griswold · Suite 1400 · Detroit · Michigan · 48226  
Phone: 313/962-3171 · Fax: 313/962-0797  
[www.clronline.org](http://www.clronline.org)

The Secretary of HHS has announced a moratorium on enforcement actions for an additional period of time to give covered entities and their business associates time to comply with the new rules. By mid-February 2010, expect enforcement actions to begin.

There are new federal and state dollars available to nonprofit health care providers to help them take the leap into the electronic age. Early incentives are replaced by penalties for organizations that fail to adopt EMRs. HIPAA privacy and security rules continue to evolve in tandem with the push to the Internet. This is a time of tremendous opportunity for nonprofits to go high tech take it!

*Susan Patton is an attorney at Butzel Long P.C. in its health industry group.*

THIS PUBLICATION SHOULD BE USED AS A REFERENCE ONLY.  
**IT SHOULD NOT BE SUBSTITUTED FOR LEGAL ADVICE.**  
NONPROFIT ORGANIZATIONS ARE ENCOURAGED TO CONTACT  
COMMUNITY LEGAL RESOURCES FOR SPECIFIC LEGAL ASSISTANCE.

*Community Legal Resources*  
615 Griswold · Suite 1400 · Detroit · Michigan · 48226  
Phone: 313/962-3171 · Fax: 313/962-0797  
[www.clronline.org](http://www.clronline.org)

© 2009 Community Legal Resources