Virtual Mentor
American Medical Association Journal of Ethics
March 2011, Volume 13, Number 3: 172-175.

HEALTH LAW
THE HITECH ACT—An Overview
Howard Burde, JD

Before the Patient Protection and Affordable Care Act, otherwise known as "Obamacare," or, more generally, health reform, Congress had already passed the most sweeping health care reform measures since Medicare was created nearly 45 years ago. As part of the American Recovery and Reinvestment Act (ARRA), Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH changed the nature of the relationships among health care professionals, organizations, patients, and payors by focusing on the implementation and use of health information technology. It puts particular emphasis on privacy and security, including expanded application and enforcement. HITECH also provides incentives and subsidies for health information exchanges and education, which are outside the scope of this article.

Incentives
HITECH provides financial incentives to "eligible professionals" for the meaningful use of certified qualified electronic health records (EHRs). An eligible professional is generally a physician, though there are incentives for hospitals as well. Certified EHR technology includes those EHRs that have been certified by an authorized testing and certification body (ATCB) [1].

The incentive payments under HITECH are substantial: eligible professionals who demonstrate the meaningful use of an EHR in 2011 or 2012 will be entitled to incentive payments of $18,000 in the first year (only $15,000 after 2012); $12,000 for the second year; $8,000 for the third year; $4,000 for the fourth year; and $2,000 for the fifth year [2]. After 2015, physicians who fail to meaningfully use EHRs will be subject to reductions in Medicare and Medicaid reimbursement [2].

The criteria for meaningful use are based on a series of specific objectives, each of which is tied to a measure that allows physicians to demonstrate that they are meaningful users of certified EHR technology. The final meaningful use standards for Stage 1 (of three) were published by the Department of Health and Human Services in 2010. For Stage 1, which begins in 2011, physicians must meet 15 mandatory (core) criteria and choose 5 of the 10 "menu" criteria. Each objective was evaluated for its potential applicability to all physicians and eligible hospitals. Where it is impossible for a physician to meet a specific measure, an exclusion defined in the final rule will apply [3].

The Stage 1 standards for meaningful use focus on electronically capturing health information in a coded format, using that information to track key clinical conditions, communicating that information for care coordination purposes, and initiating the reporting of clinical quality measures and public health information. All certified EHRs should enable a physician to meet these standards [1, 2]. Examples of meaningful use in Stage 1 include entry of patient demographic and insurance information, use of drug interaction software, and e-prescribing.

Stage 2 and 3 Criteria for Meaningful Use

Stage 2 meaningful use criteria will expand upon the Stage 1 criteria in the areas of disease management, clinical decision support, medication management support for patient access to their health information, transitions in care, quality measurement and research, and bidirectional communication with public health agencies. Information exchange is a critical part of care coordination, and Stage 2 criteria are expected to support health information exchanges and health information exchange activities [3].

Stage 3 criteria are expected to address improvements in quality, safety and efficiency, focusing on decision support for national high priority conditions, patient access to self-management tools, access to comprehensive patient data, and improving population health outcomes [3].

The criteria will become more stringent over time [4].

Privacy and Security under HITECH

HITECH expands on the notions of privacy and security found in the Health Insurance Portability and Accountability Act of 1996, known as HIPAA. The HIPAA regulations, in brief, prohibit the disclosure of individually identifiable health information, otherwise known as protected health information or PHI, without the consent of the patient (or guardian or other responsible person) except for three purposes: treatment, payment, or health care operations. HIPAA applies directly to "covered entities," defined as health care payors, providers, and clearinghouses.

Under HIPAA, "business associates"—a term referring to people or entities who, on behalf of covered entities, perform tasks that necessitate access to PHI—were not directly regulated, but were bound to comply with HIPAA pursuant to mandatory written agreements with the covered entities. HITECH, by contrast, provides for direct regulation of business associates and stipulates that HIPAA's privacy and security rules apply to them.

HITECH also dramatically increases the required response to breaches of PHI and the enforcement of such requirements [5, 6].

Notification of Breach

HITECH mandates public notification of security breaches when "unsecure PHI" is disclosed or used for an unauthorized purpose. ("Secure PHI," on the other

hand, is not subject to such requirements because it is encrypted and cannot be breached [6].) These notification requirements are similar to many state and federal data breach laws pertaining to financial information.

In general, the act requires that patients be notified of any breach of their data security, whether external or internal. If a breach affects 500 patients or more, then HHS must also be notified and the name of the institution where the breach occurred will be posted on the HHS web site. Under certain conditions, local media will also need to be notified. This provision is yet another example of the act's emphasis on privacy and security concerns [4].

Electronic Health Record Access

When a health care practice or organization implements an EHR system, the act gives patients in those practices (or third parties they designate) the right to obtain their PHI in an electronic format. This requirement is similar to state laws that mandate patient access to their own paper medical records. The act specifies that charges for such requests may only cover the labor cost of fulfilling the request. Although one might presume that such a request requires a few clicks, the reality is that even practices with an EHR system already in place may not have this capability.

Penalties and Enforcement

While HITECH is a federal law, it grants both the Department of Health and Human Services and state attorneys general the authority to enforce the law. This dual enforcement authority raises the specter of politically motivated investigations of PHI disclosures by ambitious state attorneys general. As health lawyers have advised physicians for years, the investigation will do as much damage as the penalty. The key is compliance in advance.

Civil penalties are mandatory if there is a violation due to willful neglect. For example, in situations in which a person is unaware of a violation (despite due diligence), the minimum penalty is $100 per violation, with a cap of $25,000 for violations of an identical requirement during a calendar year. If the violation is due to "willful neglect," however, the minimum penalty is $10,000 per violation, with a cap of $250,000 for violations of an identical requirement during a calendar year, and the maximum penalty is $50,000 per violation, with a cap of $1.5 million [7, 8].

Conclusion

HITECH has laid the groundwork for a positive revolution in the delivery of health care. Compliance is key, and HITECH provides both positive incentives in the form of meaningful use payments and negative incentives in the form of civil penalties and the threat of prosecution at the state level.

References

1. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), part 2, subtitle C, sec 13301, subtitle B, sec 3014: Competitive grants to States and

Indian tribes for the development of loan programs to facilitate the widespread adoption of certified EHR technology.
2. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), sec 13301, subtitle B: Incentives for the Use of Health Information Technology.
3. Office of the National Coordinator for Health Information Technology. Being a meaningful user of electronic health records. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__meaningful_use_-_providers/2998. Accessed February 18, 2011
4. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13402(d): Tiered increase in amount of civil monetary penalties.
5. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13401: Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions.
6. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13402: Notification in the case of breach.
7. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13409: Clarification of application of wrongful disclosures penalties.
8. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13410: Improved enforcement.

Further Reading

Klein K. So much to do, so little time: to accomplish the mandatory initiatives of ARRA, healthcare organizations will require significant and thoughtful planning, prioritization and execution. *J Healthc Inf Manag*. 2010;24(1):31-35.

Howard Burde, JD, provides general counsel and health law advice to health information technology and health care organizations, payors, and associations such as the Health Information Management Systems Society (HIMSS), the bipartisan Pennsylvania Joint Legislative Committee on Health Reform, and the National Governors' Association e-Health Alliance. He serves on the editorial boards of health law publications, including the *BNA Health Law Reporter* and the *Journal of Health and Life Sciences Law*, and has written four books.

Related in VM

Ethical Dimensions of Meaningful Use Requirements for Electronic Health Records, March 2011

Reassessing "Minor" Breaches in Confidentiality, March 2011