

Legal Challenges: Compliance & Implementation of EHR

By Steven J. O'Doriso, William H. Fischer and Matthew Weber

Executive Summary

On February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA or the Stimulus Package), a law that is poised to revolutionize parts of the healthcare industry. Among the most significant objectives of ARRA is the widespread implementation of electronic health records (EHR) by 2014 without compromising patient privacy. To meet this objective, ARRA provides incentives for the implementation of EHR—which are eventually replaced by penalties for failing to do so—and significantly modifies the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In addition to complying with new obligations arising under ARRA, providers must understand existing federal fraud and abuse laws that relate to EHR implementation. These laws include the federal physician self-referral law (Stark), the federal anti-kickback statute (AKS), and the Internal Revenue Service's (IRS's) EHR guidelines.

This article will discuss each of the legal challenges providers must understand and overcome to successfully implement EHR.

American Recovery and Reinvestment Act

Incentives

Starting as early as 2011, ARRA makes over \$17 billion of increased Medicare or Medicaid payments available to healthcare providers who demonstrate to the satisfaction of the Secretary of Health and Human Service (HHS) that the provider is a 'meaningful user' of 'certified EHR technology.'

Certified EHR technology must include patient demographic and clinical health information (such as history and a problem list), and have capacity to provide clinical decision support, support physician order entry, capture and query information relevant to healthcare quality, and exchange health information with and integrate information from other sources.

The definition of 'meaningful use' is currently the subject of discussion and debate and is not a settled issue.

Nevertheless, ARRA provides that using certified EHR technology in a meaningful manner must include (1) interconnection that provides for the electronic exchange of health information to improve quality such as promotion of care coordination, and (2) submission of information on clinical quality measures in a manner specified by HHS. Note that meaningful use by a hospital does not include electronic prescribing.

Payments under the Medicaid incentive program can begin later than under the Medicare incentive program and can continue past deadlines established in the Medicare incentive program. The Medicaid deadline for satisfying meaningful use can also be later than the deadline under Medicare, and therefore, Medicaid incentives should be evaluated as an alternative to incentives under the Medicare program. In either case, it is not likely that either Medicare or Medicaid incentives will cover the entire cost of conversion to EHR technology. Still, they

can provide a way to reduce a provider's out-of-pocket cost for conversion and avoid penalties in the future.

In sum, the compliance challenges relating to ARRA incentives include: (1) determine whether to seek incentives under Medicare or Medicaid; and (2) identifying and complying with requirements to demonstrate meaningful use of certified EHR technology.

HITECH Changes to HIPAA

Title XIII of ARRA, called the Health Information Technology for Economic and Clinical Health Act (HITECH), significantly modifies HIPAA arguably making it the most comprehensive federal information security and privacy law ever enacted in the United States. Specifically, HITECH:

- Expands the obligations of business associates.
- Establishes data breach notification requirements.
- Expands individual rights.
- Further restricts the use of protected health information for purposes relating to marketing, fundraising, or sales.
- Calls for additional guidance on limited data sets or the minimum necessary requirements.
- Bolsters enforcement, in part, by increasing penalties.

Business Associates

Effective February 17, 2010, business associates will be directly subject to certain provisions of HIPAA regulations, such as requiring them to implement

administrative, technical, and physical safeguards described in the HIPAA security rule, as well as comply with use and disclosure restrictions described in the HIPAA privacy rule. In addition, business associates will be required to maintain policies, procedures and documentation and will be subject to civil or criminal penalties for violating the obligations described above.

All additional privacy and security requirements created for covered entities under HITECH also apply to business associates and must be incorporated into business associate agreements. Finally, the definition of business associates now includes vendors that contract with covered entities (or with business associates) to provide data transmission services or personal health records.

“The definition of ‘meaningful use’ is currently the subject of discussion and debate and is not a settled issue.”

Before HITECH, business associates were only accountable to covered entities via contract. Now that certain HIPAA security and privacy obligations apply directly to business associates, business associates must implement information security and privacy compliance programs similar to those of covered entities. Most providers will need to revise business associate agreements and other vendor agreements relating to EHR implementation to reflect the new requirements. They will also need to monitor business associate and vendor compliance more closely.

Data Breach Notification

HITECH requires covered entities to notify individuals whose ‘unsecured protected health information’ (PHI) has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of a privacy or security breach. Unsecured PHI is PHI that is not secured through the use of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. On April 17, 2009, HHS published guidance stating that such technologies and methodologies

consist of encryption or destruction.¹ Because a breach only occurs when the PHI is unsecured, the implementation of these technologies and methodologies is an obvious way to prevent triggering the data breach notification requirements (thus creating a safe harbor against the notification requirement).

If notification is required, it must be made “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.” Under HITECH, ‘discovery’ is deemed to have occurred when the covered entity or business associate (or any employee of either) knows or should reasonably have known of the breach. In addition to notifying individuals, covered entities will also be required to notify HHS of all data

breaches. If a breach involves unsecured PHI of 500 or more individuals, then the covered entity must notify prominent media outlets and the covered entity’s name will be listed on the HHS website. HITECH sets forth the content requirements for such notices.

Providers and business associates will need to review and revise their incident response plans to ensure:

- Employees properly notify the company upon the discovery of a potential breach.
- Notification procedures are in place to respond appropriately to a breach.

Individual Rights

HITECH expands the rights of an individual to access and control PHI pertaining to that individual. For example, an individual can prohibit healthcare providers from disclosing PHI to the individual’s health plan if the individual pays for the healthcare treatment or services out-of-pocket in full. Also, under certain circumstances, an individual may request an accounting of disclosures of PHI by a covered entity



for treatment, payment, and healthcare operations when the covered entity uses or maintains an electronic health record with respect to that PHI.

Providers and business associates will need to review and revise policies and procedures relating to:

- Requests by individuals for disclosure of EHR.
- Accounting of disclosures for treatment, payment, and healthcare operations.
- Privacy notices that explain individual rights.
- Requests by individuals to restrict disclosure of certain PHI to a health plan because the individual pays for certain services out-of-pocket.

A provider must design its EHR solution to help address each of these requirements described above.²

Use of PHI for Marketing, Fundraising or Sale

HITECH places additional restrictions on covered entities’ marketing and fundraising efforts. In addition, if no exception applies, HITECH generally prohibits covered entities and business associates from directly or indirectly selling PHI of an individual without the individual’s prior authorization. HHS is required to issue final rules regarding the sale of PHI by August 17, 2010. These restrictions could create challenges for providers who rely on PHI for generating revenue.

Limited Data Sets; Minimum Necessary

HITECH requires covered entities to limit their use and disclosure of PHI to limited data sets, if possible. When disclosure cannot be limited to a limited data set,

¹ HHS is seeking comments on the subject, and therefore, may identify other technologies and methodologies to make PHI secure.

² Providers may have to segregate information it sends to payors from information contained in the medical record that is used for treatment.

the disclosure must satisfy the minimum necessary standard. Additional guidance on the minimum necessary standard should be issued no later than August 17, 2010, at which point the limited data set requirement sunsets.

Enforcement & Penalties

HITECH significantly revises the approach to enforce HIPAA by:

- Requiring HHS to audit covered entities regarding HIPAA privacy and security compliance.
- Requiring HHS to formally investigate a covered entity upon receipt of a complaint.
- Increasing civil penalties for HIPAA violations (based on different levels of intent).
- Expanding the reach of criminal penalties to individuals.
- Providing state Attorneys General with the power to bring civil actions in federal court for violations that pose a threat to or harm one or more residents of their state.

Providers and business associates will need to review and revise policies and procedures relating to (a) auditor or regulator requests for information, (b) conducting internal investigations, and (c) working with law enforcement and regulators. A provider must design its EHR solution to help address each of these requirements described above.³

Fraud & Abuse

To promote the adoption of electronic health records technology consistent with the goal of achieving fully interoperable EHR and prescribing transactions, agencies within HHS promulgated special rules relating to EHR and electronic prescribing (e-prescribing). These regulations serve as guidelines for implementing EHR technology within the confines of Stark and AKS.

Stark

The physician self-referral law (Stark), prohibits a physician from making referrals for certain designated health services (DHS) payable by Medicare to an entity with which he or she (or

an immediate family member) has a financial relationship (ownership interest, investment interest or compensation arrangement), unless an exception applies; and prohibits the entity from submitting claims to Medicare or billing the beneficiary or third party payor for those referred services, unless an exception applies.

Effective February 17, 2010, business associates will be directly subject to certain provisions of HIPAA regulations.

The Stark EHR exception permits physicians to receive non-monetary compensation (donations) in the form of services and interoperable software that contains e-prescribing capabilities and is necessary and used predominantly to create, maintain, transmit, or receive EHR. Specifically, permitted donations include:

- Software packages that include other functionality directly related to the care and treatment of individual patients (e.g., patient administration, scheduling functions, billing, and clinical support).
- Interface and translation software.
- Rights, licenses, and intellectual property related to electronic health records software.
- Connectivity services, including broadband and wireless internet services.
- Clinical support and information services related to patient care (but not separate research or marketing support services).
- Maintenance services.
- Secure messaging (e.g., permitting physicians to communicate with patients through electronic messaging).
- Training and support services (i.e., access to help desk services).

- EHR system operating within ASP (application service provider) model.
- Patient portal software.
- Donations that are *not permitted* within the Stark EHR exception include:
 - Hardware (and operating software that makes the hardware function),
 - Storage devices.
 - Software with core functionality other than electronic health records (e.g., human resources or payroll software).
 - Items or services used by a physician primarily to conduct personal business or business unrelated to the physician's practice.
 - Unnecessary software and services (i.e., those recipient already has).
 - Reimbursement for previously incurred expenses.
 - Provision of office staff.

Depending on the situation, other Stark exceptions relating to implementation of EHR may include the e-prescribing exception, community-wide health information system exception, non-monetary compensation exception, fair market value exception and incidental benefit exception. Each exception has its own criteria and will likely be selected after careful consideration of all the facts relating to a provider's EHR implementation effort.

Anti-Kickback Statute

The federal anti-kickback statute (AKS) provides criminal penalties for individuals or entities that knowingly and willfully offer, pay, solicit, or receive remuneration in order to induce or reward the referral of business reimbursable under any of the Federal health care programs. The types of prohibited remuneration specifically include, without limitation, kickbacks, bribes, and rebates, whether made directly or indirectly, overtly or covertly, in cash or in kind. Prohibited conduct includes not only the payment of remuneration intended to induce or reward referrals of patients, but also the payment of remuneration intended

³ Providers may have to ensure audit logging capabilities are in place to accurately reconstruct events that took place involving PHI.

to induce or reward the purchasing, leasing, or ordering of, or arranging for or recommending the purchasing, leasing, or ordering of any good, facility, service, or item reimbursable by any Federal health care program.

AKS safe harbors set forth conditions under which the provision of technology and services by hospitals, group practices, and prescription drug plan (PDP) sponsors and Medicare Advantage (MA) organizations to certain prescribing health care professionals, pharmacies, and pharmacists would be protected. The AKS EHR safe harbor is similar, but not entirely identical to the Stark EHR exception discussed above. For example, two significant differences exist: (1) compliance with an AKS EHR safe harbor is not the only way to avoid liability under AKS (for instance, there is also a defense available based on lack of intent, since AKS is a criminal statute), whereas compliance with the Stark exception discussed above is required; and (2) AKS applies to all health care providers, whereas Stark applies generally to physicians.

Tax Exemption

In order to protect their non-profit status, non-profit providers, such as some hospitals, may need to consider the EHR implementation guidelines provided by the IRS. These IRS guidelines state that the IRS will not treat the benefits a hospital provides to its medical staff physicians in implementing EHR systems as impermissible private benefit or inurement in violation of section 501(c)(3) of the Internal Revenue Code if the following safe harbor elements are met:

- The arrangements between the medical staff physicians and the hospital required the parties to comply with Stark and AKS rules (described above).
- The hospital is able to access medical records created by physicians pursuant to the subsidized EHR arrangement (to the extent permitted by law).
- The subsidized EHR software and services are available to all medical staff physicians.

- The hospital provides the same level of subsidy to all its medical staff physicians or varies the level of subsidy by applying criteria related to meeting the healthcare needs of the community.

“HITECH expands the rights of an individual to access and control PHI.”

Failure to meet these IRS safe harbor elements previously listed does not constitute a violation; rather, in those situations, the IRS will consider the facts and circumstances of the specific arrangement.

Other Considerations

In addition to the federal law discussed above, providers looking to implement EHR must also consider relevant state law and EHR implementation efforts, EHR standards and certification, and specific contract provisions. This section will briefly discuss each of these items.

State Law and EHR Implementation Efforts

While much of this article has focused on the federal laws and regulations affecting EHR implementation, providers will need to be aware of state laws and EHR implementation efforts. For example, some state laws may expressly require the retention of the paper record or they may imply a requirement to retain the paper records by requiring the healthcare entity to provide the “original” to the patient or other healthcare professional or entity. Other potentially relevant state laws include state information security, medical privacy, and data breach notification laws, which may impose specific obligations not covered by HIPAA (even after the changes from HITECH become effective).

In addition to laws, providers should monitor efforts in their states by governmental and health information exchange organizations. Such efforts may include opportunities for training and assistance with achieving interoperability.

Standards & Certification

EHR technology implemented through ARRA must conform to standards

which will be adopted by HHS by the end of 2009. These standards will provide a framework to help providers demonstrate ‘meaningful use’ of ‘certified EHR technology’ (see discussion above regarding incentives). After the standards

have been established, efforts will likely shift to determining how such technology will be certified. At this time, only the Certification Commission for Healthcare Information Technology (CCHIT) has been recognized by HHS as a certification body. Certification currently provides a presumption of interoperability under Stark and AKS (discussed above), but will eventually provide a presumption of meaningful use.

Providers should monitor progress in the development of standards and certification in order to maximize chances of successful EHR.

Pulling It All Together

As you can see, there are plenty of compliance challenges involved with implementing EHR. But with proper planning, each of these challenges can be overcome. The following is a short list of items to consider when implementing EHR:

- Pay attention to new rules and guidance coming from the ARRA (i.e., data breach notification, minimum necessary, etc.).
- Review business associate agreements and vendor contracts carefully to ensure they support compliance with the obligations discussed above.
- Conduct due diligence on all vendors and contractors before entering into a contract for products or services.
- Develop incident and data breach response capabilities.
- Monitor developments in standards and certification of EHR.
- Monitor efforts in the states by governmental and health information exchange organizations.

- Revise HIPAA-required documents (privacy notices, authorizations, policies, etc.) to be compliant with revised HIPAA requirements.
- Conduct an audit on all other policies and procedures to ensure they support compliance with the obligations discussed above.
- Select appropriate Stark exceptions and AKS safe harbors and determine whether the IRS EHR safe harbors are applicable.
- Design the EHR solution to ensure interoperability.
- Conduct employee training about the compliance obligations discussed above. **NP**

Authors



Steve O'Doriso is Associate for Holland & Hart's Denver office. Mr. O'Doriso's practice includes working with healthcare providers and other businesses to address the challenges of information management and technology. He has worked for a global management consulting and technology services company where he led teams specializing in various areas of information security, including compliance, auditing and remediation, monitoring and incident response, and access control. He is a Certified Information Privacy Professional (CIPP). He can be reached at: sjodoriso@hollandhart.com, or by phone at (303)-295-8168.



William H. Fischer, of Counsel for Holland & Hart's Denver office. Mr. Fischer's practice focuses on the general corporate and transactional representation of healthcare providers and high tech and biotech businesses. Mr. Fischer currently serves as the practice group manager for Holland and Hart's healthcare group. Mr. Fischer can be reached at: whfischer@hollandhart.com, and by phone at (303)-295-8338.



Matthew G. Weber is a Partner for Holland & Hart's Denver office. Mr. Weber has earned a national reputation as an effective advocate in the areas of healthcare fraud and abuse, healthcare finance, public healthcare programs, and commercial litigation. He is a frequent speaker at healthcare association conferences across the country. Mr. Weber is admitted to practice in the federal and state courts of Colorado and the District of Columbia, as well as the United States Supreme Court. He may be reached at: mweber@hollandhart.com, or by phone at (303)-295-8565.

Conflicts of Interest — continued from page 7

of interest can do to their reputations do so at their own risk. Compliance Officers, Risk Managers and Internal Auditors should study the issues discussed here, and take measures to protect their institutions and the industry as a whole. **NP**

William Sacks has over thirty years' experience in health care management as a consultant, medical practice manager and faculty practice plan director. Mr. Sacks has consulted to hospitals, medical groups and academic medical centers on compliance training and education. In 1998 he estab-

lished Health Care Compliance Strategies, Inc. (HCCS), which develops computer-based training and management tools for hospitals, Medical Schools, physician groups and payers. HCCS offers a tool to help organizations manage Conflicts of Interest. Bill may be reached at bsacks@hccs.com.