feature focus

Managing risks when implementing the new EHR disclosure accounting requirements of ARRA

By Cornelia M. Dorfschmid, PhD and Michael Maffeo, JD, MPH

Editor's note: Cornelia M. Dorfschmid is Executive Vice President with Strategic Management, Alexandria, VA and Michael Maffeo is Senior Associate, Integrity Management Services, LLC, Alexandria, VA. Ms. Dorfschmid may be contacted by e-mail at cdorfschmid@strategicm.com or by telephone at 703/683-9600 ext. 419. Mr. Maffeo may be contacted by e-mail at mmaffeo@strategicm.com or by telephone at 703/683-9600 ext. 415.

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009, a critical measure to stimulate the economy.[1] Among all of the important provisions that make up this Act, the new law provides major opportunities for the Department of Health and Human Services (DHHS), its partner agencies, and each state to improve the nation's health care system through the use of health information technology (HIT) and the promotion of the meaningful use of electronic health records (EHR) via financial incentives. The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of ARRA in Title XIII include improvements to HIPAA privacy and security provisions, which are specified in Section 13400 et. seq. ARRA brings significant changes to the HIPAA Privacy and Security Rules, which have been in effect since the final HIPAA rules became enforceable in 2003 and 2005, respectively. HIPAA enforcement has been sporadic since the rules' compliance dates, and recently, HIPAA Security enforcement has been consolidated with Privacy and moved from the Center of Medicare & Medicaid Services (CMS) to the Office of Civil Rights (OCR). ARRA provides for stricter enforcement and institutes increased tiered civil monetary penalties for violations of privacy and security measures.

Over the past several years, many organizations shifted their prime attention to matters other than HIPAA, such as the Medicare Recovery Audit Contractors (RACs), physician arrangements, clinical research compliance, and electronic health records (EHR). ARRA moves HIPAA back to the forefront. It brings changes meant to further strengthen safeguards against unauthorized use, disclosure, or access of identifiable health information. The expansion of HIPAA provisions through ARRA provides both an opportunity and a challenge for compliance staffs and security and privacy officers that will require revisiting their organization's security posture and assessing the effectiveness of the protected health information (PHI) safeguards currently in place.

ARRA did not change the floor of protection of the HIPAA rules and implementation specifications to safeguard PHI; rather, it broadens the federal protection. Penalties will increase and enforcement will be strengthened. Business associates (BAs) will be covered more directly under the law and, to a large degree, be treated similarly to the covered entities. The new federal breach notification provisions that strengthen patients' rights go into effect on September 18, 2009, (i.e., prior to other ARRA provisions). Although ARRA does not go so far as to establish a patient's right of action, it allows individuals to receive notice of breaches as well as a portion of the monies and penalties collected through government enforcement actions.[2] Most ARRA provisions will be effective one year after the date of ARRA's enactment, February 17, 2010. However, some provisions will take effect after the publication of appropriate regulations as noted in the statute. For example, DHHS is directed by the statute to issue interim final regulations on the breach notification provisions within 180 days of enactment (interim final regulations were published on August 24, 2009 in 45 CFR Parts 160 and 164). Also, the provision of accounting for disclosures will take effect no earlier than January 1, 2011 and is subject to future rule making.

What is yet to be determined – Rules and implementation specifications

From a technology perspective with focus on EHR, two aspects of risk driven by ARRA are of particular interest. First, there will be a higher level of protection related to disclosures when made through

Timeline

Provision	Key Dates
Accounting for disclosures	January 1, 2014 – Compliance date for current EHR users as of January 1, 2009
	January 1, 2011 – Compliance date for new EHR users after January 1, 2009
Breach notification	Interim final rules were published August 24, 2009 (effective September 23, 2009)
"Minimum necessary" standard	HHS will issue guidance on "minimum necessary" standard by August 17, 2010
Tiered civil monetary penalties	Effective immediately (February 17, 2009)

an EHR. The accounting of any and all disclosures of certain PHI that are made through an EHR must be implemented (i.e., there will be no exemption for treatment, payment, and health care operation-related disclosures). Second, there are also opportunities in ARRA (i.e., the financial incentives beginning in January 2011) for eligible professionals who are meaningful EHR users. Organizations that do not carefully consider now the possible Health IT factors and rewards gained by meeting the qualification criteria for EHR, however speculative they may be currently, may potentially lose millions downstream as they implement EHR. The risk of not meeting the qualification criteria for incentives (i.e., meeting specified HIT standards, policies, implementation specifications, time frames, and certification requirements), must be considered now.

CMS generally expects that under Medicare, "meaningful EHR users" would demonstrate each of the following:

- meaningful use of a certified EHR,
- the electronic exchange of health information to improve the quality of health care, and
- reporting on clinical quality and other measures using certified EHR technology.

Compliance and Health IT departments need to collaborate on both issues and include them in their risk management efforts to stay proactive. Given the broad impact that some of the ARRA provisions may have, such a risk analysis is best integrated into an enterprise-wide risk management effort (ERM) that includes a multi-disciplinary and multi-divisional approach.

Some of the key provisions and definitions of interest here are outlined below, with a few practical steps for managing risks when accounting for disclosures while implementing a new EHR.

What is new – The basics

Definitions

Some of the new definitions of ARRA include:

- **Electronic health record (EHR):** an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."[3]
- **Breach:** "the unauthorized acquisition, access, use, or disclosure of protected health information 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."[4]
- **Personal health record (PHR):** "an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[5]
- **Meaningful use:** Definition forthcoming. ARRA initially describes "meaningful use" to include the use of a certified EHR with e-prescribing capability, the ability to report on clinical quality measures, and the use of EHR technology that allows electronic exchange of patient health information.

Requirements

Some of the main new requirements include:

- **Accounting for disclosures**

ARRA expands an individual's right to receive an accounting of disclosures of PHI. It requires a covered entity to account for all disclosures of PHI, including those for treatment, payment, and health care operations (TPO), when these disclosures are made through an electronic health record. HIPAA's exception for TPO no longer applies if the covered entity maintains an "electronic health record." DHHS will release regulations on these new accounting provisions within 18 months. For covered entities that acquire an EHR after January 1, 2009, the compliance date is January 1, 2011. Entities that already have an EHR as of January 1, 2009 have more time to modify procedures and systems to comply by January 1, 2014.

- **Minimum necessary standard**

The HIPAA Privacy Rule requires that only the minimum necessary amount of PHI be released to accomplish the purpose of a permitted

Continued on page 32

 ...continued from page 29

use or disclosure. DHHS is to release new guidance to further clarify how this standard should be implemented by August 17, 2010. Beginning on February 17, 2010 and until the issuance of the DHHS guidance, the covered entity may only use, disclose, or request a limited data set as defined under the HIPAA Privacy Rule. If the limited data set is not sufficient for the purpose, then the covered entity must comply with the minimum necessary standard.

Meaningful use

ARRA introduces incentives to hospitals for the adoption of certified health information technology by developing a standard of "meaningful use" that hospitals must follow to ensure maximum Medicare reimbursement. Hospitals that meet the criteria established for meaningful users will be eligible for a proportional incentive to their Medicare reimbursement for up to four years. However, starting in 2016, hospitals that do not meet the "meaningful use" standard will receive a reduction in their Medicare reimbursement. DHHS has charged a Health Information Technology Policy Committee to provide more guidance on the definition of meaningful use under ARRA. This group released their initial recommendations on June 16, 2009.

ARRA also requires DHHS to conduct an audit if a preliminary investigation of the facts surrounding the complaint shows that the violation is due to willful neglect. Noncompliant entities will be subject to mandatory penalties by DHHS if these violations are due to willful neglect. This provision will go into effect in February 2011, with regulations issued by DHHS before August 2010. ARRA also gives DHHS the responsibility to periodically conduct audits of covered entities and business associates (BAs).

What providers can do now

Gap analysis, workgroups, and configuration issues

Regardless of the final detail in forthcoming rule making that will clarify further how the Act might be implemented, health care providers can begin preparing for ARRA and upgrade their HIPAA compliance now. Communication and internal assessment is crucial right now. To do that, providers may want to set up a special ARRA task force or work group to tackle the new provisions and conduct a gap analysis, once the final rules are promulgated. That group can begin discussing and planning which departments, including Compliance and IT, will be affected and may need to seek outside assistance for assessments, prepare requests for proposal (RFPs), or add resources. Compliance departments should start by orienting their internal staff on ARRA components, then educate and gain feedback from the special work group or task force assigned to map out a plan for ARRA. As a result of these measures, it would then be advisable to develop educational materials and training venues for the general workforce and the physician community.

When assessing HIPAA privacy and security policies for gaps, providers should review the BA inventory as well as the BA agreement language and marketing policies. They should also look at "minimum necessary" procedures, which typically have been a struggle for health care organizations since the HIPAA Privacy Rule became effective. As mentioned earlier, DHHS is in the process of preparing guidance to clarify what elements constitute the minimum necessary for purposes of treatment. HIM departments will need to mind the "minimum necessary" provisions of HIPAA—which state that only the information necessary for a specific purpose to be carried out can be disclosed. Furthermore, providers should be concerned that it is not easily technically possible to track every access to every patient record in addition to what has been accessed or extracted. Disclosures made through an EHR by clinicians to other clinicians for purposes of treatment now have to be documented. Current EHR technologies were not designed for this need. Providers are concerned that all of that accounting and logging could slow down access to records and systems, and take away time that could be spent treating patients.[6] The physician community needs to be aware of this significant change, especially those that implement new EHR. These physicians have less time to implement a compliant version. Those with existing EHR should carefully weigh the technical complications and risks that the new minimum necessary standards bring to their practice, along with tracking and accounting of all disclosures through the EHR.

When assessing system implementation risks and configuration issues, the limitations of current technology also complicate an ARRA provision that requires providers to give patients electronic copies of their electronic health records upon request. HIPAA required providers to furnish a copy of a patient's record in the format requested, but only if documents are "readily producible" in that format. ARRA removes the "readily producible" language and requires outright any facility using an EHR to provide an electronic copy of a patient's health record. Many current EHR systems cannot directly produce an electronic copy of a record by burning it onto an electronic medium such as a disk, CD, memory stick, etc.[7] Those providers who implement new EHR should build extraction and reporting capabilities into their requirements analysis to assist in complying with this measure. Along with disclosure tracking, many capabilities of the EHR should be reviewed, such as:

- the EHR's reporting and extraction capabilities to accommodate electronic copies to the patient,

- the physical and technical access controls, encryption, and techniques and methodologies that render PHI unusable,
- past track record of timelines for handling notices and breaches or violations, and
- consistency of safeguards across various facilities or organizational units.

At a minimum, an organization should take stock of its current status and attempt a feasibility study to overcome major technical and procedural gaps.

Many covered entities may be operating in a transition phase and have both paper-based and electronic health records. This complicates compliance further and creates risk.[8] As these entities review the restrictions and requirements for an efficient and compliant EHR, they should simultaneously assess how access, retrieval, printing, and forwarding/transmission of all relevant information from a patient's hybrid record would be handled. A risk analysis may benefit from various scenarios of record requests and disclosures across clinicians, patients/clinicians, and patients/providers, as well as cover how these communications impact workflow.

The monetary incentives (i.e., upside risk or opportunity that ARRA provides for the adoption and "meaningful use" of certified EHR systems) also warrant close collaboration of Health IT, Compliance, and medical staff. Early adopters gain the highest rewards. An eligible professional can receive $44,000 in incentives beginning in 2011. After several years, that opportunity can turn into risk. In 2015, eligible providers who are not meaningful EHR users will begin receiving reduced Medicare reimbursement. Reductions will reach 97% of the fee schedule in 2017. There is still little to go by as to what constitutes a "meaningful user" and certification seems to be pass/fail, rather than by degree or level. DHHS will publish a rule establishing the criteria which eligible professionals and hospitals must meet in order to qualify for the EHR incentive payments, including defining meaningful EHR users. The rule will also explain how to apply for those incentives. In spite of these uncertainties, it is clear that millions of dollars can be at stake if certification for EHR systems is missed and providers cannot qualify for meaningful use.

The interoperability criteria for meaningful use[9] initially can be expected to include submission of quality datasets, e-prescribing, and clinical summary exchange. The considerations related to qualifying for the incentive monies are best included in the organization's strategic plans and overall risk strategy. Recent recommendations by the Health IT Policy Committee, adopted from its Meaningful Use Workgroup, indicate that the certification process may be opened to the market and not limited to the Certification Commission for Health Information Technology (CCHIT), which is currently the only certification body.[10]

Enterprise risk management & auditing and monitoring

Larger providers already accustomed to COSO-compliant ERM approaches[11] may want to go further and declare ARRA a risk area entirely of its own and analyze it through formal probability and impact scoring of risk events. Risk events could be related to such topics as BA agreements, potential breaches at certain facilities, specific software applications, security posture loopholes, minimum necessary concerns, notice delays, currency or organizational maintenance of HIPAA, and IS-related policies and procedures. Requirement analysis and configuration or re-configuration of EHR should be on a Compliance department's risk list. As part of its auditing efforts, the organization should plan or initiate a HIPAA risk analysis that covers both privacy and security compliance, including a technical vulnerability analysis to assess the information security posture.

Special attention should be given to encryption features of software applications with PHI data at rest and data in motion (i.e., in use during transmission, reporting, and download capabilities). If internal expertise is limited, the organization should consider outside subject matter expertise to gain familiarity with NIST guidelines[12] related to encryption and methodologies to secure PHI. Furthermore, the Compliance department should initiate a review of contracts of software vendors and service companies. As contract negotiations and renewals of software licenses arise, it will be important to understand the vendors' system capabilities with respect to audit logs, reporting, access control configuration, and encryption features. ■

1 For the full bill, go to: http://www.hhs.gov/recovery/overview/index.html. For a brief overview, see Julienne Landsdown and Peggy Bodin: "HIPAA Changes in the American Recovery and Reinvestment Act of 2009." **Compliance Today**, May 2009.
2 California state law, for example, already has much stronger protections for individuals than federal HIPAA protection. A helpful comparison between ARRA and California state law is provided by Deven McGraw in "The Impact of Federal Stimulus Efforts on the Privacy and Security of Health Information in California." California HealthCare Foundation." ISSUE Brief, May 2009.
3 Pub. L. 111-5 § 13400
4 Pub. L. 111-5 § 13400
5 Pub. L. 111-5 § 13400
6 Kevin Heubusch: "ARRA Privacy Provisions Present IT Challenges." Journal of AHIMA, August 2009. Available at http://journal.ahima.org/2009/08/01/arra-privacy-provisions-present-it-challenges/
7 See Heubusch.
8 AHIMA: "The Complete Medical Record in a Hybrid EHR Environment: Part I, II, and III, 2003." Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021582.hcsp
9 Carrie Vaughn: "The Meaning of Meaningful Use." HealthLeaders, June 2009, p 51
10 Diane Manos: "Federal Panel's Meaningful Use, Certification Guidance Sparks Criticism." Healthcare IT News, August 14, 2009. Available at http://www.healthcareitnews.com/news/federal-panels-meaningful-use-certification-guidance-sparks-criticism
11 See www.coso.org for Committee of Sponsoring Organizations (COSO) standards.
12 See www.nist.gov for National Institute of Standards and Technology (NIST) publications.