

## **The American Recovery and Reinvestment Act (HR 1)**

### **Highlights of New Funds for the Department of Health and Human Services (HHS)**

- \$2 billion to the Office of the National Coordinator for Health Information Technology (ONC): of which \$300 million is to support regional or sub-national efforts toward health information exchange; \$20 million is for technical standards analysis and conformance testing by the National Institute of Standards and Technology (NIST); and \$5 million may be used for the administration of funds
- \$1.5 billion to the Health Resources and Services Administration (HRSA) for construction, renovation and equipment, and the acquisition of HIT systems for PHS health centers
- \$1.3 billion to the NIH National Center for Research Resources (NCRR), of which \$1 billion is intended for construction, renovation and repair of non-Federal facilities and \$300 million to support shared instrumentation and other capital research equipment
- \$8.2 billion to the Office of the Director of NIH, of which \$7.4 billion is transferred to the Institutes and Centers of NIH to support research
- \$1 billion to the Secretary of HHS for prevention and wellness programs, of which \$300 million goes to the CDC for immunization programs, \$650 million is to be used to carry out evidence-based clinical and community-based prevention and wellness strategies to address chronic diseases, and \$50 million is to be provided to States to carry out activities to reduce healthcare-associated infections
- \$1.1 billion for comparative effectiveness research [see the next heading]

### **Comparative Effectiveness Research (CER)**

- The ARRA provides \$1.1 billion for CER, divided into \$300 million to the Agency for Healthcare Research and Quality (AHRQ), \$400 million to the Office of the Director of NIH, and \$400 million to the Secretary of HHS
- CER funds are to: 1) conduct, support or synthesize research that compares the clinical outcomes, effectiveness and appropriateness of items, services, and procedures that are used to prevent, diagnose, or treat diseases, disorders, and other health conditions; and 2) encourage the development and use of clinical registries, clinical data networks, and other forms of electronic health data that can be used to generate or obtain outcomes data
- The Institute of Medicine (IOM) is to submit a report to Congress and the Secretary by June 30, 2009 making recommendations on national priorities for CER

- A 15-member Federal Coordinating Council for CER made up of senior representatives of AHRQ, CMS, FDA, ONC, VA, and other Federal agencies is established within 30 days; this Council reports to the President and Congress by June 30, 2009 regarding current Federal activities and recommendations regarding future CER
- Conference report language: The conferees do not intend for the CER funding to be used to mandate coverage, reimbursement, or other policies for any public or private payer. The funding shall be used to conduct or support research to evaluate and compare the clinical outcomes, effectiveness, risks, and benefits of two or more medical treatments and services that address a particular medical condition. Further, the conferees recognize that a “one-size-fits-all” approach to patient treatment is not the most medically appropriate solution to treating various conditions and ensures that subpopulations are considered when research is conducted or supported with these funds. None of the reports or recommendations of the Federal Coordinating Council for CER shall be construed as mandates or clinical guidelines for payment, coverage, or treatment.

### **Title XIII – Health Information Technology (the HITECH Act)**

- Provides a definition of a “qualified” EHR as containing demographic and clinical health information and having the capacity to provide clinical decision support, physician order entry, capture and query information relevant to health care quality, to exchange electronic health information with, and integrate such information from, other sources, etc.
- Establishes (codifies) ONC and gives the National Coordinator the task of performing various duties “in a manner consistent with the development of a nationwide health information technology infrastructure that allows for electronic use and exchange of information...”
- Sets a goal of EHR availability for all citizens by 2014, and stipulates that the Coordinator, in consultation with NIST, shall develop a program for voluntary certification of HIT
- The Coordinator is to estimate resources needed to reach the goal of EHR availability by 2014, including “resources needed to establish a health information technology workforce sufficient to support [this goal] including education programs in medical informatics and health information management”
- Establishes the position of Chief Privacy Officer within ONC, to advise the Coordinator on privacy, security and data stewardship issues
- Establishes the HIT Policy Committee which shall make recommendations to the Coordinator regarding standards, implementation specifications and certification criteria, as well as recommendations regarding new privacy and security technologies, including for the use of limited data sets and methodologies for new accounting for disclosures

requirements; makes this Committee subject to the Federal Advisory Committee Act (FACA). (In a great example of what some would call assuming facts not in evidence, the Committee is to look at “technologies that protect the privacy of health information and promote security in a qualified EHR, *including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns...*”)

- Establishes an HIT Standards Committee that recommends to the Coordinator standards that have been developed, recognized or harmonized; and provides for testing of such standards by NIST; same membership and FACA requirements as the Policy Committee.
- The HITECH Act stipulates that not later than 12/31/09 the Secretary shall adopt an initial set of HIT standards, implementation specifications and certification criteria; use of such standards is voluntary for the private sector.
- The HITECH Act directs that the Secretary shall make qualified EHR technology available at a nominal fee, unless the Secretary determines through an assessment that the needs and demands of providers are being substantially and adequately met through the marketplace.
- Regarding testing of HIT, the HITECH Act provides for testing of standards by NIST, and supports the establishment of a conformance testing infrastructure, including the development of technical test beds.
- NIST, NSF and other Federal agencies shall establish a program of assistance to develop multi-disciplinary Centers for Health Care Information Enterprise Integration, with grants to institutions being awarded by NIST
- Provides grants, loans, incentives on the order of \$300 million to support regional or sub-national efforts toward health information exchange; and provides for grants to States to facilitate or expand the electronic movement and use of health information, with loans that can be used to facilitate the purchase of certified EHR technology, enhance utilization, etc.
- Provides for a demonstration program to integrate information technology into clinical education – this is for graduate level education
- Sec. 3016 provides assistance to educational institutions “to establish or expand medical health informatics educations programs, including certification, undergrad and masters degree programs for both health care and information technology students...”, with priority given to existing education and training programs and programs designed to be completed in less than six months.

- Approximately \$17.2 billion for HIT funding will be distributed through Medicare and Medicaid payment incentives to “meaningful EHR users” among physicians and hospitals; with meaningful EHR users including those who do at least e-prescribing and information exchange to improve health care quality.
- Looking at physicians specifically, Medicare incentive payments can be as much as: \$18,000 in year 1, \$12,000 in year 2, \$8,000 in year 3, \$4,000 in year 4 and \$2,000 in year 5 – making a total of as much as \$44,000 in incentive payments over 5 years for physicians who are meaningful users as of 2011 or 2012; for physicians who become meaningful EHR users in 2013 the year 1 payment is \$15,000 instead of \$18,000; and for physicians who become meaningful EHR users after 2014 (presumably 2015 and beyond) there are no incentive payments at all – **the first ‘payment year’ will be no earlier than 2011**. Similar payment incentives are made to hospitals that are meaningful users of EHRs, based on their number of discharges.
- These incentive amounts are increased by 10 percent for physicians practicing in shortage areas
- Meaningful EHR use includes e-prescribing and quality reporting, and may be demonstrated by attestation, survey response, appropriate claims or quality reporting, or such other manner as the Secretary specifies.
- Using the stick as well as the carrot, the bill stipulates that Medicare fees are reduced for ‘non-EHR physician users’ by 1% in 2015, 2% in 2016 and 3% in 2017 and beyond; and the Secretary has the authority to reduce payments by up to 5% in 2018 and beyond if less than 75% of physicians are meaningful users at that time.

#### **Subtitle D – Privacy**

- In 55 pages the bill makes dozens of changes to the existing HIPAA regulatory structure.
- Sec. 13400 (Definitions) clarifies that an EHR is “created, gathered, managed, and consulted by authorized health care clinicians and staff” while a PHR (personal health record) is “managed, shared, and controlled by or primarily for the individual”.
- A key definition is that of “breach” – which includes all “unauthorized acquisition, access, use, or disclosure of” protected health information; very limited exceptions to this definition apply if an employee unintentionally accesses PHI and there is no further access or disclosure; inadvertent disclosures, on the other hand, fall within the definition of a breach, unless the disclosure is made to another employee in the same facility
- Sec. 13401 provides that business associates (BAs) of covered entities will now be directly subject to provisions of the Security Rule in the same way that covered entities are, and that recognition of the administrative, technical and physical safeguards, and other applicable security procedures, must be incorporated in the BA agreement between the BA and the CE.

- Sec. 13402 lays out breach notification obligations for CEs who must notify individuals and BAs who must notify CEs; regarding breaches, no ‘harm’ standard is included – that is, individuals must be notified of any unauthorized acquisition, use, disclosure, etc. of their information whether or not such breach could or has resulted in any harm to the individual; notice to the individual must be made without unreasonable delay and in no case later than 60 days.
- Covered entities must notify the Secretary immediately of breaches that involved the information of 500 or more individuals, and annually of all breached that involve less than 500 individuals; the Secretary then posts on an HHS website a list that identified each CE that has had a breach incident involving 500 or more individuals
- Breach notice provided to the individual must include: the date of the breach, the date of the discovery by the CE, the steps the individual should take to protect themselves from potential harm, the steps the entity is taking, etc.
- In regard to breach, there is a ‘safe harbor’ for PHI that is encrypted or otherwise rendered unusable, unreadable, etc. to an ANSI standard.
- Interim final regulations regarding breach reporting are to be issued by the Secretary within 180 days, with an effective date 30 days later.
- As with the Security Rule, Sec 13404 applies provisions of the HIPAA Privacy Rule directly to BAs and stipulates that these requirements must be included in the BA agreement; the bill also applies the Privacy Rule’s civil and criminal penalty provisions directly to BAs.
- Sec 13405 (a) says that a covered entity must restrict disclosure of PHI to a health plan for purposes of payment or health care operations at the request of the patient, if the patient self-pays for a service; among the implications is that there could be ‘holes’ in a database maintained by a Blue Cross Blue Shield plan or a Kaiser health system for such purposes as quality assurance activities, care coordination, provider credentialing, underwriting, fraud and abuse monitoring, customer service, and the like.
- Sec 13405 (b) requires CEs to use a limited data set to the extent practicable or, if necessary, the minimum necessary when making a use or disclosure; the Secretary is to issue guidance on minimum necessary within 18 months. The practical import of this provision, which confounds a mechanism intended for research – a limited data set cannot include direct identifiers such as name, social security number, email address, medical record number, account number, etc. – with a principle meant to govern information management is unclear, but there could be huge implementation costs if CEs are required to create and use limited data sets for a wide range of TPO activities. Within 18 months the Secretary shall issue guidance on what constitutes “minimum necessary” and the limited data set guideline will then sunset.

- Sec 13405 (c) provides that a CE must account for all non-oral disclosures of PHI related to treatment, payment and health care operations (TPO) for a period of 3 years, if the PHI is maintained in an EHR; if the EHR is in place as of January 2009, the effective date for this requirement is 2014; if the EHR is deployed after January 2009, the effective date is either January 2011 or the date when the EHR system is acquired. In providing an accounting to individuals who request such, covered entities may describe disclosures to business associates or provide a list of all business associates, which then must provide an accounting of disclosures on request. The Secretary is to promulgate regulations on what information is to be included in the accounting within 6 months of adopting HIT technical standards on accounting; the regulations must take into account the interests of individuals and the administrative burden on CEs and BAs.
- Sec 13405 (d) prohibits the sale of electronic health records or PHI obtained from EHRs absent an authorization by the individual; and neither a CE nor a BA can directly or indirectly receive remuneration in exchange for any PHI; with exceptions for public health activities and research, but any fees exchanged related to research would be limited to only the cost of preparation and transmittal of data [see the heading below on HIPAA, Research and HR 1]. The Secretary must develop regulations relating to Sec 13405 (d) within 18 months, to be effective 6 months later.
- Sec. 13405 (e) provides individuals the right to obtain from a CE using an EHR a copy of their information in electronic format, with charges for providing such copies limited to the entity's labor costs. The individual may designate a 3<sup>rd</sup> party, such as a PHR, to receive this copy.
- Sec 13406 (a) stipulates that “a communication by a CE or BA that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation” unless the communication relates to treatment of the individual, case management or care coordination, or describes products or benefits or services provided by the individual's health plan; and, further, a CE or BA may not receive payment for making communications about products or services, unless a BA does so under its written contract with the CE, or a CE does so with a valid authorization from the individual. A covered entity may receive payment for a communication that is about a drug or biologic that has been previously prescribed (e.g., a reminder letter) if the payment received is reasonable.
- Modifying the fundraising exception to marketing, which defines fundraising by non-profits as a health care operation, Sec 13406 (b) provides that individuals must be offered the choice of opting out of any fundraising communication.
- Sec 13407 stipulates that vendors of PHRs have breach notification obligations, including notification of individuals and of the Federal Trade Commission; and ‘third party service providers’ that provide services to PHR vendors must notify the PHR vendor if there is a breach, (similar to the requirement that BAs notify CEs); the FTC must notify the

Secretary of breaches it is informed of; and there is again a 'safe harbor' for encrypted information. The FTC is to promulgate interim final regulations regarding these breach notice obligations within 180 days, to take effect 30 days after publication.

- Sec 13408 requires BA agreements between CEs and HIEs, RHIOs and any vendor that contracts with a CE to offer a PHR to patients as part of the CE's EHR.
- Sec 13409 clarifies that HIPAA's criminal penalties apply not only to CEs but to individual employees of CEs and other individuals.
- Sec 13410 strengthens HIPAA enforcement, increases the amount of civil monetary penalties under the HIPAA rules, and clarifies that State Attorney Generals can bring lawsuits to enforce HIPAA
- Sec 13424 calls for a number of studies and reports, including one by the Secretary, in consultation with the FTC, on the application of privacy and security requirements to non-HIPAA covered entities, including PHR vendors and others; within 12 months the Secretary is to issue guidance regarding de-identification of PHI; in addition, the Secretary must prepare a report regarding HIPAA complaints submitted to the Office of Civil Rights; this section also calls for a GAO report on "best practices related to the disclosure among health care providers of protected health information of an individual for treatment of such individual."

### **Research, HIPAA and the Prohibition on Sale of Electronic Health Records**

Under the Privacy Rule, covered entities such as physicians and hospitals may use or disclose protected health information (PHI) for research purposes:

- 1) With an Authorization from the individual
- 2) For activities Preparatory to Research, such as hypothesis generation or patient screening, but PHI cannot be copied or leave the covered entity
- 3) In a limited data set, from which direct identifiers have been removed, with a data use agreement in place with the researcher
- 4) With an IRB or Privacy Board waiver of authorization, under tightly delimited circumstances
- 5) For research involving the PHI of deceased individuals
  - De-identified data is not PHI and not subject to restriction

Nothing in HR 1 alters any of the above. Rather, exceptions to the sale of PHI stipulated for public health activities (which include adverse event reporting to the FDA, for instance) and research stipulated in Sec 13405 (d) mean that if PHI is being maintained in an EHR and would be disclosed for a public health activity or to a researcher (for bona fide research purposes, which have been reviewed by an IRB), then the covered entity is prohibited from charging more for the 'sale' of such PHI than the costs of the preparation and transmittal of such PHI which is to be disclosed for research purposes.