The Health Information Technology for Economic and Clinical Health (HITECH) Act

C. Stephen Redhead
Specialist in Health Policy

February 23, 2009

Congressional Research Service
7-5700
www.crs.gov
R40161

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Lawmakers incorporated the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009 (H.R. 1), the economic stimulus bill that the President signed into law on February 17, 2009 (P.L. 111-5). The HITECH Act is intended to promote the widespread adoption of health information technology (HIT) to support the electronic sharing of clinical data among hospitals, physicians, and other health care stakeholders. HIT is widely viewed as a necessary and vital component of health care reform. It encompasses interoperable electronic health records (EHRs)—including computerized systems to order tests and medications, and support systems to aid clinical decision making—and the development of a national health information network to permit the secure exchange of electronic health information among providers.

The HITECH Act builds on existing federal efforts to encourage HIT adoption and use. It codifies the Office of the National Coordinator for Health Information Technology (ONCHIT) within the Department of Health and Human Services. ONCHIT was created by Executive Order in 2004 and charged with developing and implementing a strategic plan to guide the nationwide implementation of health information technology (HIT) in the public and private health care sectors. ONCHIT has focused on developing standards necessary to achieve interoperability among varying HIT applications; establishing criteria for certifying that HIT products meet those standards; ensuring the privacy and security of electronic health information; and helping facilitate the creation of prototype health information networks.

The HITECH Act provides financial incentives for HIT use among health care practitioners. It establishes several grant programs to provide funding for investing in HIT infrastructure, purchasing certified EHRs, training, and the dissemination of best practices. It also authorizes grants to states for low-interest loans to help providers finance HIT. Beginning in 2011, the legislation authorizes Medicare incentive payments to encourage doctors and hospitals to adopt and use certified EHRs. Those incentive payments are phased out over time and replaced by financial penalties for physicians and hospitals that are not using certified EHRs. The legislation further authorizes a 100% federal match for payments to certain qualifying Medicaid providers who acquire and use certified EHR technology.

Finally, the HITECH Act includes a series of privacy and security provisions that expand the current requirements under the Health Insurance Portability and Accountability Act (HIPAA). Among other things, the legislation strengthens enforcement of the HIPAA privacy rule and creates a right to be notified in the event of a breach of identifiable health information.

The Congressional Budget Office (CBO) estimates that Medicare and Medicaid spending under the HITECH Act will total $32.7 billion over the 2009-2019 period. CBO anticipates, however, that widespread HIT adoption will reduce total spending on health care. Through 2019, CBO estimates that the HITECH Act will save the Medicare and Medicaid programs a total of about $12.5 billion. Under current law, CBO predicts that about 45% of hospitals and 65% of physicians will have adopted HIT by 2019. CBO estimates that the incentive mechanisms in the HITECH Act will boost those adoption rates to about 70% for hospitals and about 90% for physicians.

Contents

Tables

Contacts

Introduction

The American Recovery and Reinvestment Act of 2009 (ARRA; H.R. 1), which the President signed into law on February 17, 2009 (P.L. 111-5), incorporated the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act, based on legislation introduced in the 110th Congress, is intended to promote the widespread adoption of health information technology (HIT) for the electronic sharing of clinical data among hospitals, physicians, and other health care stakeholders.

HIT, which generally refers to the use of computer applications in medical practice, is widely viewed as a necessary and vital component of health care reform. It encompasses interoperable electronic health records (EHRs)—including computerized systems to order tests and medications, and support systems to aid clinical decision making—and the development of a national health information network to permit the secure exchange of electronic health information among providers. The promise of HIT comes not from automating existing practices, but rather as a tool to help overhaul the delivery of care. HIT enables providers to render care more efficiently, for example, by eliminating the use of paper-based records and reducing the duplication of diagnostic tests. It can also improve the quality of care by identifying harmful drug interactions and helping physicians manage patients with multiple conditions. Moreover, the widespread use of HIT would provide large amounts of clinical data for comparative effectiveness research, performance measurement, and other activities aimed at improving health care quality.

Relatively few health care providers have adopted HIT. The most recent estimate suggests that only about 5% of physicians have a fully functional EHR that incorporates all or most of the recommended capabilities, including electronic documentation of physicians' notes, electronic viewing of lab test results and radiological images, electronic prescribing, clinical decision support, and interoperability with other systems.[1] The most important barriers to HIT adoption include the high implementation and maintenance costs, the limited financial incentives for using HIT, and the lack of interoperability.[2]

The HITECH Act includes three sets of provisions to promote HIT adoption. First, it codifies the Office of the National Coordinator for Health Information Technology (ONCHIT) within the Department of Health and Human Services (HHS). Created by Executive Order in 2004, ONCHIT was charged with developing and implementing a strategic plan to guide the nationwide implementation of HIT in the public and private health care sectors. ONCHIT has focused its activities in the following areas: (1) developing vocabulary, messaging, and functional standards necessary to achieve interoperability among varying HIT applications; (2) establishing criteria for certifying that HIT products meet those standards; (3) ensuring the privacy and security of electronic health information; and (4) helping facilitate the creation of prototype health information networks. The goal is to develop a national capability to exchange standards-based health care data in a secure computer environment.

[1] Catherine M. DesRoches et al., "Electronic Health Records in Ambulatory Care—A National Survey of Physicians," New England Journal of Medicine, 2008, vol. 359, no. 1, pp. 50-60.

[2] Interoperability refers to the ability of IT systems to share and use electronic information. Sharing clinical data across different HIT applications depends on the use of a standardized format for communicating the information electronically.

Second, the HITECH Act through a number of mechanisms provides financial incentives for HIT use among health care practitioners. It establishes several grant programs to provide funding for investing in HIT infrastructure, purchasing certified EHRs, training, and the dissemination of best practices. It also authorizes grants to states for low-interest loans to help providers finance HIT. Beginning in 2011, the legislation provides Medicare incentive payments to encourage doctors and hospitals to adopt and use certified EHRs. Those incentive payments are phased out over time and replaced by financial penalties for physicians and hospitals that are not using certified EHRs. In addition to the Medicare incentives, the legislation authorizes a 100% federal match for payments to certain qualifying Medicaid providers for the acquisition and use of certified EHR technology.

Finally, the HITECH Act includes a series of privacy and security provisions that amend and expand the current HIPAA requirements. Among other things, the legislation strengthens enforcement of the HIPAA privacy rule and creates a right to be notified in the event of a breach of identifiable health information.

The Congressional Budget Office (CBO) estimates that the HITECH Act payment incentives (and penalties) will increase spending for the Medicare and Medicaid programs by a total of $32.7 billion over the 2009-2019 period. CBO anticipates, however, that widespread adoption of interoperable EHRs will reduce total spending on health care by decreasing the number of duplicate and inappropriate tests and procedures, reducing paperwork and administrative overhead, and eliminating medical errors. Over the 2009-2019 period, it estimates that the HITECH Act will save the Medicare and Medicaid programs a total of $12.5 billion. When savings to the Federal Employees Health Benefits program and CMS's administrative costs are factored in, CBO estimates overall that the HITECT Act will increase direct federal spending by $20.8 million.[3] Under current law, CBO predicts that about 45% of hospitals and 65% of physicians will have adopted HIT by 2019. CBO estimates that the incentive mechanisms in the HITECH Act will boost those adoption rates to about 70% for hospitals and about 90% for physicians.

This report provides a summary and explanation of the provisions in the HITECH Act. In order to provide some context for that discussion, the report first gives an overview of prior actions taken by Congress and the Administrations to promote HIT, and briefly describes efforts by the 109th and 110th Congresses to enact comprehensive HIT legislation. The report will continue to be updated to reflect administrative actions related to the implementation of the HITECH Act.

Federal Efforts to Promote HIT

HIPAA Administrative Simplification: Electronic Transactions, Security & Privacy Standards

Congress took an important first step towards promoting HIT when it enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA; P.L. 104-191). HIPAA imposed new federal requirements on health insurance plans offered by public and private employers,

[3] The CBO cost estimate for the H.R. 1 conference agreement is at http://www.cbo.gov/ftpdocs/99xx/doc9989/hr1conference.pdf.

guaranteeing the availability and renewability of health insurance coverage for certain employees and individuals, and limited the use of preexisting condition restrictions. But while HIPAA was primarily concerned with giving consumers greater access to health insurance, the legislation also contained a section, subtitled Administrative Simplification, that included provisions to promote more standardization and efficiency in the health care industry and safeguard personal health information. Under HIPAA Administrative Simplification, the HHS Secretary was required to develop standards to support the growth of electronic record keeping and claims processing in the health care system and to safeguard the privacy of patient records. The standards apply to health care providers (who transmit any health information in electronic form in connection with a HIPAA-specified transaction), heath plans, and health care clearinghouses.

Electronic Transactions and Code Sets

HIPAA instructed the Secretary to issue electronic format and data standards for nine routine administrative and financial transactions between health care providers and health plan/payers. Those transactions include claims and encounter information, payment and remittance advice, and claims status inquiry and response. The electronic transactions standards include several Accredited Standards Committee X12 (ASC X12) standards, as well as a number of code sets (e.g., International Classification of Diseases, 9th Edition, Clinical Modification, or ICD-9CM) used to identify specific diagnoses and clinical procedures that pertain to a patient encounter. HIPAA does not mandate that providers submit transactions electronically, though health plans/payers increasingly require it. However, if a health care provider chooses to submit one or more of the HIPAA-specified transactions electronically, then he or she must comply with the standard for that transaction. In 2001, Congress enacted the Administrative Simplification Compliance (P.L. 107-105), which, among other things, requires Medicare providers to submit claims electronically.

Unique Health Identifiers

HIPAA further required the Secretary to issue national identification numbers for health care providers, health plans, employers, and individuals (i.e., patients) for use in standard transactions. Unique identifiers for providers and employers have been adopted, while the health plan identifier is still under review. The requirement that HHS develop a unique patient identifier has proven too controversial because of privacy concerns and is on hold. Beginning in FY1999, Congress each year has included language in the annual appropriations bill for the Departments of Labor, HHS, and Education prohibiting the use of funds for the development of a unique individual identifier.

Health Information Security

HIPAA's Administrative Simplification provisions also instructed the Secretary to issue security standards to safeguard individually identifiable health information in electronic form against unauthorized access, use, and disclosure. The security rule (45 CFR Parts 160, 164) specifies a series of administrative, technical, and physical security procedures for providers and plans to use to ensure the confidentiality of electronic health information. Administrative safeguards include such functions as assigning or delegating security responsibilities to employees, as well as security training requirements. Physical safeguards are intended to protect electronic systems and data from threats, environmental hazards, and unauthorized access. They include restricting access to computers and off-site backups. Technical safeguards are primarily IT functions used to

protect and control access to data. They include using authentication and password controls, and encrypting data for storage and transmission.

The HIPAA security standards are flexible and scalable, allowing covered entities (i.e., health plans, health care providers, and health care clearinghouses) to take into account their size, capabilities, and the costs of specific security measures. The standards are also technology neutral. They do not prescribe the use of specific technologies, so that covered entities will not be bound by particular systems and/or software.

Health Information Privacy

Finally, HIPAA set a three-year deadline for Congress to enact health information privacy legislation. If, as turned out to be the case, lawmakers were unable to pass such legislation before the deadline, the HHS Secretary was instructed to promulgate regulations containing standards to protect the privacy of individually identifiable health information. The HIPAA privacy rule (45 CFR Parts 160, 164) established several individual privacy rights with respect to such protected health information (PHI). First, it established a right of access. Individuals have the right to see and obtain a copy of their own PHI in the form or format they request, provided the information is readily producible in such form or format. If not, then the information must be provided in hard copy or such form or format as agreed to by the covered entity and the individual. The covered entity can impose reasonable, cost-based fees for providing the information. Second, the privacy rule gives individuals the right to amend or supplement their own PHI. Third, individuals have the right to request that a covered entity restrict the use and disclosure of their PHI for the purposes of treatment, payment, or other routine health care operations. However, the covered entity is not required to agree to such a restriction unless it has entered into an agreement to restrict, in which case it must abide by the agreement. Finally, individuals have the right to an accounting of disclosures of their PHI by a covered entity during the previous six years, with certain exceptions. For example, a covered entity is not required to provide an accounting of disclosures that have been made to carry out treatment, payment, and health care operations.

In addition to patient privacy rights, the HIPAA privacy rule placed certain limitations on when and how covered entities may use and disclose PHI. Generally, health plans and health care providers may use and disclose health information for the purpose of treatment, payment, and health care operations without the individual's authorization and with few restrictions. In certain other circumstances (e.g., disclosures to family members and friends), the rule requires plans and providers to give the individual the opportunity to object to the disclosure. The rule also permits the use and disclosure of health information without the individual's permission for various specified activities (e.g., public health oversight, law enforcement) that are not directly connected to the treatment of the individual. For all uses and disclosures of health information that are not otherwise required or permitted by the rule, plans and providers must obtain a patient's written authorization.

The privacy rule incorporates a minimum necessary standard. Whenever a covered entity uses or discloses PHI or requests such information from another covered entity, it must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use or disclosure. There are a number of circumstances in which the minimum necessary standard does not apply; for example, disclosures to or requests by a health care provider for treatment purposes. The rule also permits the disclosure of a "limited data set" for certain specified purposes (e.g., research), pursuant to a data use agreement with the recipient. A limited data set, while not meeting the rule's definition of de-identified information (to which the privacy

protections do not apply), has most direct identifiers removed and is considered by HHS to pose a low privacy risk.

Under the HIPAA privacy and security standards, health plans and health care providers may share PHI with their business associates who provide a wide variety of functions for them, including legal, actuarial, accounting, data aggregation, management, administrative, accreditation, and financial services. A covered entity is permitted to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will not use or disclose the information other than as permitted or required by the contract or as required by law, and that the business associate will implement appropriate administrative, technical, and physical safeguards to prevent unauthorized uses and disclosures. Covered entities are not liable for, or required to monitor, the actions of their business associates. If a covered entity finds out about a material breach or violation of the contract by a business associate, it must take reasonable steps to remedy the situation, and, if unsuccessful, terminate the contract. If termination is not feasible, the covered entity must notify HHS.

HIPAA authorized the Secretary to impose civil monetary penalties on any person failing to comply with the privacy and security standards. The maximum civil penalty is $100 per violation and up to $25,000 for all violations of an identical requirement or prohibition during a calendar year. The HHS Office of Civil Rights (OCR) is responsible for enforcing the privacy rule. For certain wrongful disclosures of PHI, OCR may refer the case to the Department of Justice for criminal prosecution. HIPAA's criminal penalties include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm.

Together, the HIPAA privacy and security standards have helped lay the groundwork for the development of a National Health Information Network and the widespread adoption of interoperable EHRs. Information on the HIPAA privacy rule and links to information on the other HIPAA Administrative Simplification standards is at [http://www.hhs.gov/ocr/hipaa].

Medicare Part D: E-Prescribing

Besides HIPAA, the other significant legislative action taken by Congress to promote HIT was the inclusion of electronic prescribing provisions in the Medicare Modernization Act of 2003 (MMA; P.L. 108-173), which created the Part D prescription drug benefit. The MMA established a timetable for the Centers for Medicare and Medicaid Services (CMS) to develop e-prescribing standards, which provide for the transmittal of such information as eligibility and benefits (including formulary drugs), information on the drug being prescribed and other drugs listed in the patient's medication history (including drug-drug interactions), and information on the availability of lower-cost, therapeutically appropriate alternative drugs. CMS issued a set of foundation standards in 2005, then piloted and tested additional standards in 2006. The final Medicare e-prescribing standards, which become effective on April 1, 2009, apply to all Part D sponsors, as well as to prescribers and dispensers that electronically transmit prescriptions and prescription-related information about Part D drugs prescribed for Part D eligible individuals. The MMA did not require Part D drug prescribers and dispensers to e-prescribe. Under its provisions, only those who choose to e-prescribe must comply with the new standards. However, the recently enacted Medicare Improvement for Patients and Providers Act of 2008 (MIPPA; P.L. 110-275) includes an e-prescribing mandate and authorizes incentive bonus payment for e-prescribers

between 2009 and 2013. Beginning in 2012, payments would be reduced for those who fail to e-prescribe. Information on the CMS e-prescribing standards is at [http://www.cms.hhs.gov/EPrescribing].

Anti-Kickback Statute, Stark Law

The MMA also instructed the Secretary to establish a safe harbor from penalties under the anti-kickback statute (42 U.S.C. 1320a-7b) and an exception to the Medicare physician self-referral (Stark) law (42 U.S.C. 1395nn) for the provision of HIT and training services used in e-prescribing. The anti-kickback statute prohibits an individual or entity from knowingly or willfully offering or accepting remuneration of any kind to induce a patient referral for, or purchase of, an item or service covered by any federal health care program. The Stark law prohibits physicians from referring patients to any entity for certain health services if the physician (or an immediate family member) has a financial relationship with the entity, and prohibits entities from billing for any services resulting from such referrals, unless an exception applies. Both statutes, which are intended to fight fraud and abuse, are seen as impediments to the dissemination of HIT among health care entities.

In 2006, the Secretary announced final regulations creating new safe harbors and Stark exceptions for certain arrangements involving the donation of electronic prescribing and EHR technologies and training services.[4] That would allow, for example, a hospital to provide such technologies and services to its medical staff, and Medicare Advantage plans to provide such technologies and services to pharmacies and prescribing health care providers.

CMS Grants, Demonstrations and Pay-for-Performance

CMS is administering a number of additional programs to promote HIT adoption. The MMA mandated a three-year pay-for-performance demonstration in four states to encourage physicians to adopt and use HIT to improve the treatment of chronically ill Medicare patients. Physicians participating in the Medicare Care Management Performance (MCMP) demonstration receive bonus payments for reporting clinical quality data and meeting clinical performance standards for treating patients with certain chronic conditions. They are eligible for an additional incentive payment for using a certified EHR and reporting the clinical performance data electronically.

CMS has developed a second demonstration to promote EHR adoption using its Medicare waiver authority. The five-year Medicare EHR demonstration is intended to build on the foundation created by the MCMP program. It will provide financial incentives to as many as 1,200 small- to medium-sized physician practices in 12 communities across the country for using certified EHRs to improve quality, as measured by their performance on specific clinical quality measures. Additional bonus payments will be made based on the number of EHR functionalities a physician group has incorporated into its practice.

[4] U.S. Dept. of Health and Human Services, Office of Inspector General, "Medicare and State Health Programs: Fraud and Abuse; Safe Harbors for Certain Electronic Prescribing and Electronic Health Records Arrangements Under the Anti-Kickback Statute," 71 Federal Register 45110, Aug. 8, 2006. U.S. Dept. of Health and Human Services, Centers for Medicare and Medicaid Services, "Medicare Program: Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships; Exceptions for Certain Electronic Prescribing and Electronic Health Records Arrangements," 71 Federal Register 45140, Aug. 8, 2006.

The Tax Relief and Health Care Act of 2006 (P.L. 109-432) established a voluntary physician quality reporting system, including an incentive payment for Medicare providers who report data on quality measures. The Medicare Physician Quality Reporting Initiative (PQRI) was expanded by the Medicare, Medicaid, and SCHIP Extension Act of 2007 (P.L. 110-173) and by MIPPA, which authorized the program indefinitely and increased the incentive that eligible physicians can receive for satisfactorily reporting quality measures. In 2009, eligible physicians may earn a bonus payment equivalent to 2.0 percent of their total allowed charges for covered Medicare physician fee schedule services. The PQRI quality measures include a structural measure that conveys whether a physician has and uses an EHR.

The Deficit Reduction Act of 2005 (P.L. 109-171) authorized Medicaid Transformation Grants to states totaling $150 million over two years. The purpose of the grants is to support adoption of innovative methods to improve effectiveness and efficiency in providing medical assistance under Medicaid. In 2007, CMS awarded Medicaid Transformation Grants to 33 states, the District of Columbia, and Puerto Rico. Most of the funds are being used for HIT-related initiatives.

Office of the National Coordinator for Health Information Technology

On April 27, 2004, President Bush announced a commitment to the promotion of HIT by calling for the widespread adoption of interoperable EHRs within 10 years. That same day he signed Executive Order 13335 creating ONCHIT to develop, maintain, and direct a strategic plan to guide the nationwide implementation of HIT in the public and private health care sectors. Within three months, ONCHIT published a strategic framework in which it outlined four major goals for HIT: (1) informing clinical practice by accelerating the use of EHRs; (2) interconnecting clinicians allowing them to exchange health information in a secure environment; (3) personalizing health care by enabling consumers to participate more actively in their own care; and (4) improving population health through improved public health surveillance and by accelerating research and its translation into clinical practice.

In fall 2004, ONCHIT solicited public input on a series of questions on whether and how a National Health Information Network should be developed. The questions addressed such topics as organization and business framework, legal and regulatory issues, management and operational considerations, interoperability standards, and privacy and security. Based on the detailed and coordinated responses that it received from a broad array of stakeholders in the health care sector, ONCHIT has undertaken a series of activities to address several important challenges to the nationwide implementation of a HIT infrastructure.

In 2005, the Secretary created the American Health Information Community (AHIC), a public-private advisory body, to make recommendations to the Secretary on how to accelerate the development and adoption of interoperable HIT using a market-driven approach. AHIC and its workgroups have proven to be extremely important in creating a forum to seek input and guidance from a broad range of stakeholders on key HIT issues and policy implications. The AHIC charter required it to provide the Secretary with recommendations to create a successor entity based in the private sector. AHIC Successor, Inc. was established in July 2008 to transition AHIC's accomplishments into a new public-private partnership. That partnership, the National eHealth Collaborative (NeHC), was launched on January 8, 2009.

Developing standards and a process to certify HIT products and services as meeting those standards is a key priority. ONCHIT awarded a contract to the American National Standards Institute (ANSI) to establish a public-private collaborative, known as the Healthcare Information Technology Standards Panel (HITSP), to harmonize existing HIT standards and identify and establish standards to fill gaps. To date, the Secretary has recognized over 100 harmonized standards, including many that need to be used for interoperable EHRs. To ensure that these standards are incorporated into products, a second contract was awarded to the Certification Commission for Healthcare Information Technology (CCHIT), a private, nonprofit organization created by HIT industry associations, which establishes criteria for certifying products that use recognized standards. CCHIT has certified over 150 ambulatory and inpatient EHR products. In August 2006, the President issued Executive Order 13410 committing federal agencies that purchase and deliver health care to require the use of HIT that is based on interoperability standards recognized by the Secretary.

The National Health Information Network (NHIN) is envisioned as a "network of networks"; that is, a nationwide, Internet-based architecture that interconnects state and regional health information exchanges (and other networks). It will be built on a secure platform using a shared set of standards and policies to permit interoperable health information exchange among providers, consumers, and others involved in supporting health care. To facilitate the development of the NHIN, ONCHIT awarded several contracts to develop models of how nationwide electronic health information might work. Each contractor was asked to develop a prototype architecture for the NHIN and to interconnect three communities as a demonstration of the architecture. The initial phase of the project has since been expanded and now involves health information exchanges across the country working cooperatively to identify and implement best practices for health information exchange.

Ensuring the privacy and security of electronic health information is critical to the success of the NHIN and the widespread adoption of interoperable EHRs. ONCHIT has undertaken the development of a national privacy and security framework, using HIPAA as its foundation, to incorporate the needs of health care consumers and build public trust in the new e-health environment. To this end it has awarded a contract to RTI International, which in turn has subcontracted with 33 states and one territory that make up the Health Information Security and Privacy Collaboration (HISPC). HISPC is leveraging input from a broad range of public and private stakeholders in health information exchange to assess the variations in current privacy and security practices and policies. The goal is to identify both best practices and challenges, and develop consensus-based solutions for interoperable electronic health information exchange that protect the privacy and security of health information. Information on ONCHIT's activities and programs is at [http://www.hhs.gov/healthit].

Agency for Healthcare Research and Quality

Within HHS, the Agency for Healthcare Research and Quality (AHRQ) is the principal source of federal HIT grant money. Since 2004, AHRQ has awarded $260 million to support and stimulate investment in HIT. This translates into almost 200 projects in 48 states. AHRQ-funded projects, many of which are focused on rural and underserved populations, cover a broad range of HIT tools and systems, including EHRs, personal health records (PHRs),[5] e-prescribing, privacy and

[5] Unlike an EHR, which is created and controlled by one or more health care providers who populate it with clinical data, a PHR is controlled by the patient. A PHR does not contain the same depth of information as an EHR, and (continued...)

security, quality measurement, and Medicaid technical assistance. In addition, AHRQ created the online National Resource Center for Health IT to disseminate research findings and best practices, facilitate expert and peer-to-peer collaboration, and foster the growth of online communities who are planning to implement HIT. Information on AHRQ's HIT activities and programs is at [http://healthit.ahrq.gov].

Other Federal Agencies

Other federal agencies that purchase health care are also involved in efforts to further the development and broad adoption of HIT. The Department of Defense (DOD), the Department of Veterans Affairs (VA), and the Office of Personnel Management (OPM) have worked with HHS to adopt health information standards for use by all federal health agencies. As part of the Consolidated Health Informatics Initiative, more than 20 federal agencies have agreed to endorse standards that enable information to be shared among agencies and that can serve as a model for the private sector. Over the past few years, OPM has encouraged Federal Employees Health Benefits (FEHB) health benefits plans to increase their use of HIT.

The VA and DOD are both extensive users of HIT. For several years, the VA has used an EHR—the Veterans Health Information Systems and Technology Architecture, or VistA—in providing care to U.S. military veterans. According to the VA, VistA has improved the efficiency of its health care delivery and the quality of the care it provides. DOD has developed and is in the process of implementing an EHR—known as AHLTA (Armed Forces Health Longitudinal Technology Application)—for its health care system. DOD is also working with the VA to develop a way by which health information can be transmitted seamlessly and instantaneously between the two agencies.

HIT Legislation in the 109th and 110th Congresses

109th Congress

The 109th Congress was the first to consider comprehensive HIT legislation. On November 18, 2005, the Senate, by unanimous consent, passed the bipartisan Wired for Health Care Quality Act (S. 1418, S.Rept. 109-111). On July 27, 2006, the House passed the Health Information Technology Promotion Act (H.R. 4157, H.Rept. 109-603) on a vote of 270-148. The bills, which contained several important differences, were not conferenced. Both bills included comparable provisions establishing ONCHIT, but contained competing language addressing the responsibilities and composition of AHIC and its role in the adoption of interoperability standards. Only the Senate bill addressed certification. S. 1418 also would have authorized grants for health care providers, grants for implementing regional HIT plans, and a state loan program to facilitate HIT adoption. H.R. 4157 included a single HIT grant program for integrated health care systems. Both measures would have authorized a demonstration program, but for different

(...continued)

typically includes information from multiple sources, including data on insurance claims. Individuals and other authorized clinical and wellness professionals use the PHR to help guide and make health decisions and manage the patient's care. Many health plans and some employers offer PHRs. Other leading IT companies, including Google and Microsoft, also offer a PHR product.

purposes. The House measure also included provisions that would have established an anti-kickback safe harbor and Stark exception for the donation of HIT and related support or training services, as well as provisions to expedite updating and modifying the HIPAA electronic transactions and codes standards. The Senate version contained no such provisions.

110th Congress

The Wired for Health Care Quality Act (S. 1693) was reintroduced on June 26, 2007, and ordered reported (as amended) by the Committee on Health, Education, Labor, and Pensions (HELP) on August 1, 2007 (S.Rept. 110-187). In the House, H.R. 6357, the PRO(TECH)T Act of 2008, was introduced by Representatives Dingell and Barton on June 24, 2008, and ordered reported (as amended) by the Committee on Energy and Commerce on September 11, 2008 (H.Rept. 110-837). No further legislative action was taken on either measure. Like the Senate bill, H.R. 6357 would have codified ONCHIT and authorized grants and loans to promote the adoption of EHRs and the development of health information exchange networks. Unlike S. 1693, however, the House measure also included extensive privacy and security provisions to strengthen the HIPAA rules. A second House bill, H.R. 6898, the Health-e Information Technology Act of 2008, was introduced by Representative Stark on September 15, 2008, and referred to the Committees on Energy and Commerce, Science and Technology, and Ways and Means. Broadly similar to the PRO(TECH)T Act, H.R. 6898 also included Medicare incentive payments to encourage EHR use by hospitals and physicians, as well as financial penalties for providers that failed to adopt HIT.

HITECH Act: Explanation of Provisions

Lawmakers incorporated the HITECH Act in the American Recovery and Reinvestment Act of 2009 (ARRA; H.R. 1, H.Rept. 111-16), the economic stimulus bill that the President signed into law on February 17, 2009 (P.L. 111-5). The HITECH Act is an amalgam of the two House bills from the 110th Congress. It contains three sets of provisions that are expected to boost HIT adoption among health care providers in the coming years. First, it codifies ONCHIT and establishes a process for the development of interoperability standards that support the nationwide electronic exchange of health information among doctors, hospitals, patients, health plans, the federal government, and other health care stakeholders. It also establishes a voluntary certification process for HIT products. The National Institute of Standards and Technology (NIST) is to provide for the testing of such products to determine if they meet national standards that allow for secure electronic information exchange. After the adoption of an initial set of standards by the end of 2009, the National Coordinator must make an EHR available at a nominal fee, unless it is determined that the needs and demands of providers are being adequately met by the marketplace.

Second, the HITECH Act authorizes funding for several grant programs to support HIT infrastructure, EHR adoption, training, dissemination of best practices, telemedicine, and inclusion of HIT in clinical education. Funds also are provided to states for low-interest loans to help health care practitioners finance HIT. In addition, the legislation provides financial incentives through the Medicare and Medicaid programs to encourage doctors, hospitals, health clinics, and other entities to adopt and use certified EHRs. Medicare incentive payments are phased out over time and replaced with financial penalties for providers that are not using EHRs.

Finally, the HITECH Act expands the HIPAA privacy and security standards. Among other things, it establishes a breach notification requirement for health information that is not encrypted, strengthens enforcement of the HIPAA standards by increasing penalties for violations and provides greater resources for enforcement and oversight activities, places new restrictions on marketing activities by health plans and providers, and creates transparency by allowing patients to request an audit trail showing all disclosures of their electronic health information.

The HITECH Act appears in two separate ARRA titles, each of which is described in the tables below. **Table 1** provides a summary of the HITECH Act provisions in Division A, Title XIII of the economic stimulus bill. Those provisions include ONCHIT and the development and adoption of standards, the grant and loan programs, and the privacy and security requirements. **Table 2** summarizes the HITECH Act's Medicare and Medicaid provisions, which are in Division B, Title IV of the stimulus bill. For each provision, as appropriate, the tables include additional information on existing federal requirements and other relevant administrative activities. Each mention of the Secretary in the tables refers to the Secretary of Health and Human Services. Note: **Table 2** does not include two miscellaneous Medicare provisions added to the HITECH Act, which are unrelated to HIT.[6]

HIT Appropriations in ARRA

In addition to the mandatory funding that would become available to health care providers under the HITECH Act's Medicare and Medicaid provisions, the emergency appropriations provisions in ARRA Division A include $2 billion in discretionary funds for ONCHIT to invest in HIT architecture; provide grants to hospitals, physicians, and other health care providers; and support training programs. In addition, $85 million is appropriated to the Indian Health Service (IHS) for HIT and telehealth, to be allocated at the discretion of the IHS Director.[7]

[6] Those provisions are at the end of Division B, Title IV: (i) Section 4301, Moratoria on Certain Medicare Regulations; and (ii) Section 4302, Long-Term Care Hospital Technical Corrections.

[7] For more details, see CRS Report R40181, *Selected Health Funding in the American Recovery and Reinvestment Act*, coordinated by C. Stephen Redhead.

Table 1. HITECH Act: Standards Development and Adoption; Grants and Loans; Privacy and Security

American Recovery and Reinvestment Act of 2009 (P.L. 111-5): Division A, Title XIII

Topic	Summary of Provision	Current Requirements and Activities
Office of the National Coordinator for Health Information Technology (ONCHIT): Standards Development and Adoption (Subtitle A, Part 1)		
ONCHIT: Purpose and Duties	The Act establishes within HHS the Office of the National Coordinator for Health Information Technology (ONCHIT). The National Coordinator is appointed by the Secretary and report directly to the Secretary. ONCHIT's purpose is to promote the development of a national HIT infrastructure that allows the electronic use and exchange of information, in order to improve health care quality, reduce health care costs and health disparities, improve public health, facilitate research, and promote prevention and management of chronic diseases, among other things. The National Coordinator is charged with the following duties: (1) review and determine whether to endorse standards, implementation specifications, and certification criteria recommended by the HIT Standards Committee (see below); (2) coordinate HIT policy and programs within HHS and with those of other federal agencies and act as a liaison among the HIT Policy and Standards Committees (see below) and the federal government; (3) update and republish the Federal Health IT Strategic Plan (as of June 3, 2008) to include specific objectives, milestones, and metrics with respect to the electronic exchange and use of health information, the utilization of an EHR for each person in the United States by 2014, the incorporation of privacy and security protections for the electronic exchange of an individual's health information, strategies for using HIT to improve health care quality, and plans for ensuring that populations with unique needs, such as children, are appropriately addressed in the technology design, among other things; (4) maintain and update a website to post relevant information about the work related to efforts to promote a nationwide HIT infrastructure; (5) in consultation with the National Institute of Standards and Technology (NIST), keep or recognize a program or programs for the voluntary certification of HIT as being in compliance with applicable certification criteria adopted by the Secretary; (6) prepare several reports, including a report on any additional funding or authority needed to evaluate and develop HIT standards; a report on lessons learned from HIT implementation by major public and private health care systems; a report on the benefits and costs of the electronic use and exchange of health information; an assessment of the impact of HIT on communities with health disparities and in medically underserved areas; and a report estimating the resources needed annually to achieve nationwide adoption of EHRs by 2014, including the resources needed to establish a sufficient HIT workforce; (7) establish a national governance mechanism for the national health information network; and (8) appoint a Chief Privacy Officer of the Office of the National Coordinator to advise the National Coordinator on privacy, security, and data stewardship.	ONCHIT was created by Executive Order 13335, signed by President Bush on April 27, 2004. The National Coordinator was instructed to develop, maintain, and direct a strategic plan to guide the nationwide implementation of interoperable HIT in the public and private health care sectors.

Topic	Summary of Provision	Current Requirements and Activities
HIT Policy Committee	The Act establishes an HIT Policy Committee to make policy recommendations to the National Coordinator relating to the implementation of a nationwide HIT infrastructure, including recommending areas in which standards are needed for the electronic exchange and use of health information, and recommending an order of priority for the development of such standards. The Committee is required to provide recommendations in at least the following eight areas: (1) technologies that protect the privacy and security of electronic health information; (2) a nationwide HIT infrastructure that enables electronic information exchange; (3) nationwide adoption of certified EHRs; (4) EHR technologies that allow for an accounting of disclosures; (5) using EHRs to improve health care quality; (6) encryption technologies that render information unusable, unreadable, and indecipherable to unauthorized individuals; (7) the use of electronic systems to collect patient demographic data (consistent with the evaluation of health disparities data under Sec. 1809 of the Social Security Act); and (8) technologies and design features that address the needs of children and other vulnerable populations. The Act describes other areas that the committee might consider, including using HIT to reduce medical errors, and telemedicine. The National Coordinator must take a leading role in the establishment and operations of the HIT Policy Committee. Committee members—appointed by the Secretary, Congress, and the Comptroller General (as specified in the Act)—must represent a balance among various health care sectors so that no one sector unduly influences the Committee's recommendations. The Committee must ensure the participation of outside advisors. The Secretary must publish in the *Federal Register* and post online all of the Committee's recommendations. The provisions of the Federal Advisory Committee Act (FACA) apply to the HIT Policy Committee.	In 2005, the Secretary created the American Health Information Community (AHIC), a public-private advisory body, to make recommendations to the Secretary on how to accelerate the development and adoption of interoperable HIT using a market-driven approach. The AHIC charter required it to provide the Secretary with recommendations to create a successor entity based in the private sector. AHIC Successor, Inc. was established in July 2008 to transition AHIC's accomplishments into a new public-private partnership. That partnership, the National eHealth Collaborative (NeHC), was launched on January 8, 2009.

Topic	Summary of Provision	Current Requirements and Activities
HIT Standards Committee	The Act establishes an HIT Standards Committee to recommend to the National Coordinator standards, implementation specifications, and certification criteria for the electronic exchange of health information. Duties of the HIT Standards Committee include the development, harmonization, and pilot testing of standards, and serving as a forum for the participation of a broad range of stakeholders to provide input on the development, harmonization, and recognition of standards. Not later than 90 days after enactment, the HIT Standards Committee is to outline a schedule (to be updated annually) for assessing the policy recommendations developed by the HIT Policy Committee. In addition, the Committee is to conduct open public meetings and develop a process to allow for public comment on this schedule. The National Coordinator must take a leading role in the establishment and operations of the HIT Standards Committee. Committee members must represent a balance among various health care sectors so that no one sector unduly influences the Committee's recommendations. The Committee must ensure a similar balance in developing procedures for conducting its activities. The Committee must ensure the participation of outside advisors. The Secretary must publish in the *Federal Register* and post online all of the Committee's recommendations. The provisions of the Federal Advisory Committee Act (FACA) apply to the HIT Standards Committee.	ONCHIT awarded a contract to the American National Standards Institute (ANSI) to establish a public-private collaborative, known as the Healthcare Information Technology Standards Panel (HITSP), to harmonize existing HIT standards and identify and establish standards to fill gaps. To date, the Secretary has recognized over 100 standards, including many for interoperable EHRs. To ensure that these standards are incorporated into products, a second contract was awarded to the Certification Commission for Healthcare Information Technology (CCHIT), a private, nonprofit organization created by HIT industry associations, which establishes criteria for certifying products that use recognized standards. CCHIT has certified over 150 ambulatory and inpatient EHR products.
Adoption of Standards, Implementation Specifications, and Certification Criteria	The Act requires the Secretary, within 90 days of receiving from the National Coordinator a recommendation for HIT standards, implementation specifications, or certification criteria, to determine whether or not to propose adoption of such measures. Adoption is to be accomplished through notice-and-comment rulemaking, whereas a decision not to adopt is to be conveyed in writing to the National Coordinator and the HIT Standards Committee. The Secretary must adopt, through notice-and-comment rulemaking, an initial set of standards by December 31, 2009. The initial standards may be issued as an interim final rule.	
Use of Standards by Private Entities	Nothing in the Act requires (or gives a federal agency new authority to require) a private entity to adopt a standard or implementation specification developed under the Act.	
Federal EHR Technology	The Act requires the National Coordinator to support the development and routine updating of qualified EHR technology and to make such technology available unless the Secretary determines that the needs and demands of providers are being substantially and adequately met through the marketplace. The National Coordinator may charge providers a nominal fee to purchase this technology, taking into account the financial circumstances of smaller and rural providers.	
Open Source HIT Systems	The Act requires the Secretary, in consultation with other federal agencies, to study and report to Congress by October 1, 2010, on the availability and cost of open source HIT systems to federal safety net providers, including smaller and rural providers and those that provide a significant amount of care to the uninsured.	

Topic	Summary of Provision	Current Requirements and Activities
Transitions	Upon enactment, all functions, personnel, assets, liabilities, and administrative actions of the existing ONCHIT are transferred to the new ONCHIT established by the Act. Nothing in the Act prohibits AHIC Successor, Inc., doing business as the National eHealth Collaborative, from modifying its charter, duties, membership, and any other functions to be consistent with the provisions of this subtitle in a manner that would permit the Secretary to recognize it as the HIT Policy Committee or the HIT Standards Committee.	
Relations to HIPAA Privacy and Security Rules	The Act specifies that its provisions may not be construed as having any effect on the authorities of the Secretary under HIPAA privacy and security law.	
Application and Use of Adopted Health Information Technology Standards (Subtitle A, Part 2)		
Federal Agencies	The Act requires federal agencies that implement, acquire, or upgrade HIT systems for the electronic exchange of health information to use HIT systems and products that meet the standards adopted by the Secretary under this Act. The President must ensure that federal activities involving the collection and submission of health information are consistent with such standards within three years of their adoption.	In August 2006, President Bush issued Executive Order 13410 committing federal agencies that purchase and deliver health care to require the use of HIT that is based on interoperability standards recognized by the Secretary.
Federal Contractors	The Act requires health care payers and providers that contract with the federal government to use HIT systems and products that meet the standards adopted by the Secretary under this Act.	
Reports	The Act requires the Secretary: (1) within two years and annually thereafter, to report to Congress on efforts to facilitate the adoption of a nationwide system for the electronic exchange of health information; (2) to conduct a study that examines methods to create efficient reimbursement incentives for improving health care quality in federally qualified health centers, rural health clinics and free clinics, and to report to Congress within two years; and (3) to conduct a study of matters relating to the potential use of new aging services technology to assist seniors, individuals with disabilities and their caregivers throughout the aging process, and to report to Congress within two years.	
Testing of Health Information Technology (Subtitle B)		
NIST Testing	The Act requires NIST, in coordination with the HIT Standards Committee, to test HIT standards, as well as support the establishment of a voluntary testing program by accredited testing laboratories.	ONCHIT is working with NIST on testing HIT standards. NIST is assisting with the HITSP standards harmonization process and with CCHIT's certification activities.

Topic	Summary of Provision	Current Requirements and Activities
Research and Development Programs	The Act requires NIST, in consultation with the National Science Foundation (NSF) and other federal agencies, to award competitive grants to universities (or research consortia) to establish multidisciplinary Centers for Health Care Information Enterprise Integration. The purpose of the Centers is to generate innovative approaches to the development of a fully interoperable national health care infrastructure, as well as to develop and use HIT. The National High-Performance Computing Program must include federal research and development programs related to HIT.	
Grant, Loan, and Demonstration Programs (Subtitle C)		
HIT Infrastructure Grants	The Act instructs the Secretary to invest in HIT so as to promote the nationwide use and exchange of electronic health information. The Secretary must invest funds through the different HHS agencies with relevant expertise to support the following: (1) HIT architecture to support the secure electronic exchange of information; (2) EHRs for providers not eligible for HIT incentive payments under Medicare and Medicaid; (3) training and dissemination of information on best practices to integrate HIT into health care delivery; (4) telemedicine; (5) interoperable clinical data repositories; (6) technologies and best practices for protecting health information; and (7) HIT use by public health departments. The Secretary must ensure, to the greatest extent practicable, that funds are used to acquire HIT that meets applicable standards adopted by the Secretary.	Since 2004, AHRQ has awarded $260 million to support and stimulate investment in HIT. AHRQ-funded projects, many of which are focused on rural and underserved populations, cover a broad range of HIT tools and systems including EHRs, PHRs, e-prescribing, privacy and security, quality measurement, and Medicaid technical assistance. In addition, the Federal Communication Commission's Universal Service Rural Health Care Program has provided $417 million to rural health care providers for telecommunications services, including broadband, to improve health care quality.
HIT Implementation Assistance	The Act requires the National Coordinator, in consultation with NIST, to establish an HIT extension program to assist providers in adopting and using certified EHR technology. The Secretary also must create an HIT Research Center to serve as a forum for exchanging knowledge and experience, providing technical assistance to health information networks, and learning about using HIT in medically underserved communities. Finally, the Secretary must fund the creation and operation of HIT Regional Extension Centers, affiliated with nonprofit organizations, to provide assistance to providers in the region. Priority will be given to assisting public, nonprofit, and critical access hospitals, community health centers, individual and small group practices, and entities that serve the uninsured, underinsured, and medically underserved individuals. Regional centers are permitted to receive up to four years of funding, to cover up to 50% of their capital and annual operating and maintenance expenditures. Each center that receives financial support must be evaluated biennially. Within 90 days of enactment, the Secretary must publish in the *Federal Register* a detailed explanation of the program, procedures to be followed by the applicants, and the maximum support levels expected to be available to centers under the program.	

Topic	Summary of Provision	Current Requirements and Activities
State Planning and Implementation Grants	The National Coordinator is authorized to award planning and implementation grants to states or qualified state-designated entities to facilitate and expand electronic health information exchanges. To qualify as a state-designated entity, an entity must be a nonprofit organization with broad stakeholder representation on its governing board and adopt nondiscrimination and conflict-of-interest policies. In order to receive an implementation grant, a state or qualified state-designated entity must submit a plan describing the activities to be carried out to facilitate and expand electronic health information exchange according to nationally recognized standards and implementation specifications. The Secretary annually must evaluate the grant activity under this section and implement the lessons learned from each evaluation in the subsequent round of awards in such a manner as to realize the greatest improvement in health care quality, decrease in costs, and the most effective and secure electronic information exchange. Grants require a match of at least $1 for each $10 of federal funds in FY2011, at least $1 for each $7 of federal funds in FY2012, and at least $1 for each $3 of federal funds in FY2013 and each subsequent fiscal year.	
State Loan Programs	The Act authorizes the National Coordinator to award competitive grants to states or Indian tribes to establish loan programs for health care providers to purchase and upgrade certified EHR technology, train personnel in the use of such technology, and improve the secure electronic exchange of health information. To be eligible, grantees must: (1) establish a qualified HIT loan fund; (2) submit a strategic plan, updated annually, describing the intended uses of the funds and providing assurances that loans will only be given to health care providers that submit required reports on quality measures and use the certified EHR technology supported by the loan for the electronic exchange of health information to improve the quality of care; and (3) provide matching funds of at least $1 for every $5 of federal funding. Loans are repayable over a period of up to 10 years. Each year, the National Coordinator must provide a report to Congress summarizing the annual reports submitted by grantees. Awards are not permitted before January 1, 2010.	
Clinical Education Demonstration	The Act authorizes the Secretary to create a demonstration program for awarding competitive grants to medical, dental, and nursing schools, and to other graduate health education programs to integrate HIT into the clinical education of health care professionals. To be eligible, grantees must submit a strategic plan. A grant may not cover more than 50% of the costs of any activity for which assistance is provided, though the Secretary has the authority to waive that cost-sharing requirement. The Secretary annually must report to designated House and Senate Committees on the demonstrations, with recommendations.	
Medical Informatics Education Grants	The Act requires the Secretary, in consultation with the NSF, to provide financial assistance to universities to establish or expand medical informatics programs.	

Topic	Summary of Provision	Current Requirements and Activities
Reports and Evaluation	The Secretary may require grantees, within one year of receiving an award, to report on the effectiveness of the activities for which the funds were provided and the impact of the project on health care quality and safety. The National Coordinator annually must evaluate the grant activities under this subtitle and implement the lessons learned from each evaluation in the subsequent round of awards in such a manner as to realize the greatest improvement in the quality and efficiency of health care.	
Authorization of Appropriations	The Act authorizes the appropriation of such sums as may be necessary for each of FY2009 through FY2013 to fund the grant, loan, and demonstrations programs.	
HIPAA Privacy and Security Standards (Subtitle D)		
Definitions	The Act defines the following privacy and security terms, in most cases by reference to definitions in the HIPAA Administrative Simplification standards: breach, business associate, covered entity, disclose, electronic health record (EHR), health care operations, health care provider, health plan, National Coordinator, payment, personal health record (PHR), protected health information (PHI), Secretary, security, state, treatment, use, and vendor of personal health records. The term breach means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security and privacy of such information, but does not include (1) any unintentional acquisition, access, or use of PHI by an individual acting in good faith and under the authority of a covered entity of business, provided the information is not further acquired, used, or disclosed, and (2) any inadvertent disclosure from an individual who is otherwise authorized to access PHI, provided the information received as a result of the disclosure is not further acquired, used, or disclosed without authorization.	
Application of Security Provisions and Penalties to Business Associates	The Act applies the HIPAA security standards and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to covered entities. It also requires the Secretary, in consultation with industry stakeholders, to issue annual guidance on the most effective and appropriate technical safeguards, including the use of encryption standards recommended by the HIT Policy Committee, for protecting electronic health information.	The HIPAA civil and criminal penalties apply to covered entities. As previously discussed, covered entities are not liable for, or required to monitor, the actions of their business associates. If a covered entity finds out about a material breach or violation of the contract by a business associate, it must take reasonable steps to remedy the situation, and, if unsuccessful, terminate the contract. If termination is not feasible, the covered entity must notify HHS.

Topic	Summary of Provision	Current Requirements and Activities
Notification of Information Breach: HIPAA Covered Entities	In the event of a breach of unsecured PHI that is discovered by a covered entity, the covered entity must notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach. For a breach of unsecured PHI under the control of a business associate, the business associate upon discovery of the breach must notify the covered entity. All breach notifications have to be made no later than 60 days after their discovery. Notification may be delayed, in the same manner as provided in Section 164.528(a)(2) of the HIPAA privacy rule, if it would impede criminal investigation or damage national security. The provision specifies the methods by which individuals must be notified and the contents of the notification. Notice of the breach must be provided to prominent media outlets serving a particular area if more than 500 individuals in that area are impacted. Covered entities also must immediately notify the Secretary of breaches of unsecured PHI involving 500 or more individuals. If the breach impacts fewer than 500 individuals, the covered entity involved has to maintain a log of such breaches and annually submit it to the Secretary. The Secretary is required to list on the HHS website each covered entity involved in a breach that impacts more than 500 individuals. The Act defines unsecured PHI as information that is not secured through the use of a technology or methodology identified by the Secretary as rendering the information unusable, unreadable, and undecipherable to unauthorized individuals. Within 60 days, and annually thereafter, the Secretary is required to issue guidelines specifying such technologies and methodologies, including the use of encryption standards recommended by the HIT Policy Committee. If the Secretary fails to meet those deadlines, PHI will be considered unsecure if not secured by a technology standard rendering it unusable, unreadable, or indecipherable to unauthorized individuals that was developed or endorsed by a standards development organization accredited by ANSI. The Act requires the Secretary annually to report to Congress on the number and type of breaches, actions taken in response, and recommendations made by the National Coordinator on how to reduce the number of breaches. Within 180 days of enactment, the Secretary is required to issue interim final regulations to implement this section.	The privacy and security rules do not require covered entities to notify HHS or others of a breach of the privacy, security, or integrity of PHI. However, business associate contracts must include a provision requiring business associates to report to covered entities if they become aware of any security incident or any use or disclosure of PHI that is not provided for by the contract.
Privacy Education	The Secretary is required to designate a privacy advisor in each HHS regional office to offer education and guidance to covered entities and business associates. Within 12 months of enactment, OCR must develop and maintain a national education program to educate the public about their privacy rights and the potential uses of their PHI.	The privacy rule requires each covered entity to designate a privacy official for the development and implementation of its policies and procedures.

Topic	Summary of Provision	Current Requirements and Activities
Application of Privacy Provisions and Penalties to Business Associates	Business associates are only permitted to use or disclose PHI if such action is in compliance with the contract. The current provisions regarding a covered entity acting on its knowledge of a material breach or violation by a business associate apply equally to a business associate gaining such knowledge. In the case of a business associate violating the privacy contract requirements in this section, the Act applies the civil and criminal penalties to that business associate in the same manner as they apply to covered entities. Any additional privacy requirements under this subtitle that are made applicable to covered entities also apply to business associates and have to be incorporated into the contract.	The HIPAA civil and criminal penalties apply to covered entities. As previously discussed, covered entities are not liable for, or required to monitor, the actions of their business associates. If a covered entity finds out about a material breach or violation of the contract by a business associate, it must take reasonable steps to remedy the situation, and, if unsuccessful, terminate the contract. If termination is not feasible, the covered entity must notify HHS.
Patients' Privacy Rights	The Act gives individuals the right to receive an electronic copy of their PHI, if it is maintained in an EHR, and direct the covered entity to transmit such copy to an entity or person clearly designated by the individual. It also requires a health care provider to honor a patient's request that the PHI regarding a specific health care item or service not be disclosed to a health plan for purposes of payment or health care operations, if the patient paid out-of-pocket in full for that item or service. Further, individuals have the right to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment, and health care operations during the previous three years, if the disclosures were through an EHR. Within 6 months of adopting standards on accounting of disclosures, the Secretary must issue regulations on what information shall be collected about each disclosure, taking into account the administrative burden of accounting for such disclosures.	As previously discussed, the privacy rule establishes several federal privacy rights, including the right of access to one's own PHI, the right to amend or supplement one's PHI, the right to request that a covered entity restrict the use and disclosure of one's PHI for the purposes of treatment, payment, or other health care operations, and the right to an accounting of PHI disclosures (other than for treatment, payment, or health care operations, or pursuant to an authorization).
Minimum Necessary	Covered entities must limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. This requirement holds until the Secretary issues guidance on what constitutes minimum necessary. In addition, the Act clarifies that the entity disclosing the PHI (as opposed to the requester) makes the minimum necessary determination. The HIPAA privacy rule's exceptions to the minimum necessary standard continue to apply.	As previously discussed, the privacy rule incorporates a minimum necessary standard. There are a number of circumstances in which the minimum necessary standard does not apply; for example, disclosures to or requests by a health care provider for treatment purposes. The rule also permits the disclosure of a "limited data set" for certain specified purposes (e.g., research), pursuant to a data use agreement with the recipient. A limited data set has most direct identifiers removed and is considered to pose a low privacy risk.
Sale of Patient Information	The Act prohibits the sale of PHI by a covered entity or business associate without patient authorization except in certain specified circumstances, including: (1) public health activities (as described in 45 CFR 164.512(b)); (2) research (as described in 45 CFR 164.512(i)); (3) treatment of the individual; and (4) providing the individual with a copy of his or her PHI. Within 18 months of enactment, the Secretary must issue regulations governing the sale of PHI.	Unless expressly permitted or required under the rule, the disclosure of PHI to a third party is prohibited without patient authorization.

Topic	Summary of Provision	Current Requirements and Activities
Marketing	The Act clarifies that a marketing communication by a covered entity or business associate about a product or service that encourages the recipient to purchase or use the product or service may not be considered a health care operation, unless the communication is for a health care-related product or service, or relates to the treatment of the individual. Further, such a communication about a health-care related product or service may not be considered a health care operation if the covered entity receives payment for the making the communication, unless (1) the communication describes only a drug or biologic that is currently being prescribed for the recipient and the payment is reasonable (as defined by the Secretary), (2) the covered entity obtains authorization from the recipient, or (3) in the event the communication is made by a business associate on behalf of a covered entity, the communication is consistent with the contract. Fundraising communications must, in a clear and conspicuous manner, provide an opportunity for the recipient to opt out of further communications.	Generally, a covered entity may not use or disclose health information for its own marketing activities without authorization. However, communications made by a covered entity (or its business associate) to encourage a patient to purchase or use a health care-related product or service are excluded from this definition and, therefore, do not require the patient's authorization, even if the covered entity is paid by a third party to engage in such activities.
Notification of Information Breach: PHR Vendors and Other non-HIPAA Covered Entities	PHR vendors and entities offering products and services through a PHR vendor's website, upon discovery of a breach of security of unsecured PHR health information, must notify the individuals impacted and the Federal Trade Commission (FTC). The previously described requirements for the content and timeliness of notifications apply also to this provision. Unsecured PHR health information means PHR health information that is not protected through the use of a technology or methodology specified in guidance issued by the Secretary. If the Secretary fails to issue guidance, then PHR health information will be considered unsecure if not secured by a technology standard rendering it unusable, unreadable, or indecipherable to unauthorized individuals that was developed or endorsed by a standards development organization accredited by ANSI. The FTC must notify HHS of any breach notices it receives and has enforcement authority regarding such breaches of unsecured PHR health information. Within 180 days, the FTC must issue interim final regulations to implement this section. The provisions in this section will no longer apply if Congress enacts new legislation establishing breach notification requirements for non-HIPAA covered entities.	The privacy and security rules apply to covered entities (i.e., health plans and providers) and, through written contracts, to their business associates. As already noted, however, the privacy and security rules do not require covered entities to notify HHS or others of a breach of the privacy, security, or integrity of PHI. However, business associate contracts must include a provision requiring them to report to covered entities if they become aware of any security incident or any use or disclosure of PHI that is not provided for by the contract.
Business Associate Contracts	The Act requires organizations that contract with covered entities for the purpose of exchanging electronic PHI (e.g., Health Information Exchanges, Regional Health Information Organizations (RHIOs), and PHR vendors) to have business associate contracts with those entities.	
Criminal Penalties	The Act amends HIPAA to clarify that criminal penalties for wrongful disclosure of PHI apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not.	In July 2005, the Justice Department's Office of Legal Counsel addressed which persons may be prosecuted under HIPAA and concluded that only a covered entity could be criminally liable.

Topic	Summary of Provision	Current Requirements and Activities
Civil Penalties	The Act amends HIPAA to permit OCR to pursue an investigation and the imposition of civil monetary penalties against any individual for an alleged criminal violation of the HIPAA standards if the Justice Department had not prosecuted the individual. In addition, it amends HIPAA to require a formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect. The Secretary must issue regulations within 18 months to implement those amendments. The Act also requires that any civil monetary penalties collected be transferred to OCR to be used for enforcing the HIPAA privacy and security standards. Within 18 months of enactment, GAO is required to submit recommendations for giving a percentage of any civil monetary penalties collected to the individuals harmed. Based on those recommendations, the Secretary, within three years of enactment, must establish by regulation a methodology to distribute a percentage of any collected penalties to harmed individuals. The Act further amends HIPAA by replacing the existing civil monetary penalties with four tiers of penalties, the highest of which would impose a fine of $50,000 per violation and up to $1,500,000 for all such violations of an identical requirement or prohibition during a calendar year. It preserves the current requirement that a civil fine not be imposed if the violation was due to reasonable cause and was corrected within 30 days. Finally, state attorneys general are authorized to bring a civil action in federal district court against individuals who violate the HIPAA privacy and security standards. Nothing in the section prevents OCR from continuing to use corrective action without a penalty in cases where the person did not know, and by exercising reasonable diligence would not have known, about the violation.	As noted above, HIPAA authorized the Secretary to impose civil monetary penalties on any person failing to comply with the privacy and security standards. Civil monetary penalties may not be imposed if: (1) the violation is a criminal offense under HIPAA's criminal penalty provisions; (2) the person did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not to willful neglect, and was corrected within 30 days. OCR has not levied a single penalty against a HIPAA-covered entity. Instead, it has focused on working with covered entities to encourage voluntary compliance through corrective action. For certain wrongful disclosures of PHI, OCR may refer the case to the Department of Justice for criminal prosecution. HIPAA's criminal penalties include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm.
Compliance Audits	The Secretary is required to perform periodic audits to ensure compliance with the HIPAA privacy and security standards and the requirements of this subtitle.	The Secretary is authorized to conduct compliance reviews to determine whether covered entities are complying with HIPAA standards.
Preemption of State Law	The Act applies the HIPAA preemption provisions to the above privacy requirements and preserves the HIPAA privacy and security standards to the extent that they are consistent with those requirements. The Secretary is required by rulemaking to amend the HIPAA standards as necessary to make them consistent with the Act's privacy and security provisions. The Act does not waive any health privacy privilege otherwise applicable to an individual.	The HIPAA security standards preempt any contrary provision of state law, with certain specified exceptions (e.g., public health reporting). However, the privacy rule does not preempt a contrary provision of state law that is more protective of patient medical privacy.
Effective Date	Except as otherwise specifically provided, the above privacy and security provisions take effect 12 months after enactment.	

Topic	Summary of Provision	Current Requirements and Activities
Studies, Reports, Guidance	The Secretary is required annually to provide Congress with a compliance report containing information on (1) the number and nature of complaints of alleged violations and how they were resolved, including the imposition of civil fines, (2) the number of covered entities receiving technical assistance in order to achieve compliance, as well as the types of assistance provided, (3) the number of audits performed and a summary of their findings, and (4) the Secretary's plan for the following year for improving compliance with and enforcement of the HIPAA standards and the provisions of this subtitle. In addition, the Secretary is required, within one year and in consultation with FTC, to study the application of health information privacy and security requirements (including breach notification) to non-HIPAA covered entities and report to Congress. The Secretary also is required, within one year of enactment and in consultation with stakeholders, to issue guidance on how best to implement the HIPAA privacy rule's requirements for de-identifying PHI. Finally, the Secretary may, by regulation, revise the definition of psychotherapy notes to include test data that are part of a mental health evaluation. The Act requires GAO, within one year, to report on best practices related to the disclosure of PHI among health care providers for the purpose of treatment. The report must include an examination of practices implemented by states and other entities, such as health information exchanges, and how those practices improve the quality of care, as well as an examination of the use of electronic informed consent for disclosing PHI for treatment, payment, and health care operations. GAO is further required, within five years, to report to Congress and the Secretary on the impact of the Act on health insurance premiums, health care costs, EHR adoption, and improvement in health care quality.	Any person who believes a covered entity is not complying with the privacy rule may file a complaint with HHS. HIPAA does not require the Secretary to issue a compliance report. The privacy and security standards apply to health plans, health care providers, and health care clearinghouses. They do not apply directly to other entities that collect and maintain health information, including Health Information Exchanges, RHIOs, and PHR vendors, unless they are acting as providers or plans. The HIPAA standards are intended to protect individually identifiable health information; de-identified information is not subject to the regulations. Under the privacy rule, health information is de-identified if 18 specific identifiers (e.g., name, social security number, address) have been removed, or if a qualified statistician, using accepted principles, determines that the risk if very small that the individual could be identified. Generally, plans and providers may use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual's authorization. Covered entities may, but are not required, to obtain an individual's general consent to use or disclose PHI for treatment, payment, or health care operations. Psychotherapy notes (i.e., notes recorded by mental health professionals during counseling) are afforded special protection under the privacy rule. Almost all uses and disclosures of such information require patient authorization.

Source: Table prepared by the Congressional Research Service, based on P.L. 111-5 (Division A, Title XIII), signed by the President on February 17, 2009.

Table 2. HITECH Act: Medicare and Medicaid Payments

American Recovery and Reinvestment Act of 2009 (P.L. 111-5): Division B, Title IV

Topic	Summary of Provision	Current Requirements and Activities
Medicare Incentive Payments and Penalties (Subtitle A)		
Physicians	The Act authorizes incentive payments over a five-year period through Medicare Part B to physicians (as defined in Section 1861(r) of the Social Security Act) who are meaningful users of certified EHR technology. Meaningful use is defined as: (1) demonstrating to the satisfaction of the Secretary the use of certified EHR technology in a meaningful manner (including e-prescribing), including for the purpose of exchanging electronic health information to improve health care quality; and (2) using such certified EHR technology to report clinical quality measures, as selected by the Secretary. The incentive payments equal 75% of the allowed Part B charges during the reporting year. However, the total amount that a physician could receive is capped and decreases over time. Beginning in 2011, eligible physicians will receive up to $15,000 in the first payment year, $12,000 in the second year, $8,000 in the third year, $4,000 in the fourth year, and $2,000 in the fifth, and final, year. Early EHR adopters whose first payment year is 2011 or 2012 will receive up to $18,000 (instead of $15,000) for that year. Eligible physicians first becoming meaningful EHR users after 2013 will be subject to lower caps, and those who do not adopt EHRs until after 2014 will receive no bonus. For eligible physicians practicing in health professional shortage areas, the incentive payment amounts are increased by 10%. No incentive payments will be made after 2016. Incentive payments are not available for hospital-based physicians. Eligible physicians who are not meaningful users of certified HIT systems by 2015 will see their Medicare payments reduced by the following amounts: 1% in 2015, 2% in 2016, 3% in 2017 and in each subsequent year. For 2018 and each subsequent year, if the proportion of eligible physicians who are meaningful EHR users is less than 75%, the payment reduction will be further decreased by one percentage point from the applicable amount in the previous year, though the reduction cannot exceed 5%. The Secretary may, on a case-by-case basis, exempt eligible physicians (e.g., rural physicians that lack sufficient Internet access) from the payment reduction if it is determined that being a meaningful EHR user would result in significant hardship. Such exemptions may not be granted for more than five years. Generally, the physician incentive payments are not available to Medicare Advantage (MA) plans. However, the Act provides for the application of the EHR bonus payments and penalties to certain eligible physicians affiliated with MA organizations that function as an HMO. To avoid duplication of payments, if a physician is both an MA-affiliated provider and eligible for the maximum incentive payment under the fee-for-service (FFS) program, then the payment is to be made only under the FFS program. If the physician is eligible for less than the maximum incentive payment, then the payment is to be made only to the MA organization.	As previously discussed, CMS is administering a number of programs to promote HIT adoption among health care providers. They include the five-year EHR demonstration, the physician incentive payments for e-prescribing, and the Physician Quality Reporting Initiative (PQRI), under which physicians can earn a bonus for satisfactorily reporting quality measures, including using an EHR.

Topic	Summary of Provision	Current Requirements and Activities
Hospitals	The Act authorizes incentive payments over a four-year period through Medicare Part A to eligible acute-care hospitals that are meaningful users of certified EHR technology. Meaningful use is defined as: (1) demonstrating to the satisfaction of the Secretary the use of certified EHR technology in a meaningful manner, including for the purpose of exchanging electronic health information to improve health care quality; and (2) using such certified EHR technology to report clinical quality measures, as selected by the Secretary. Beginning in FY2011, eligible hospitals would receive a base amount ($2 million), plus an additional $200 per discharge for the 1,150th through the 23,000th discharge. All payments would be adjusted by the hospital's Medicare share, the value of which takes into account the level of charity care provided (i.e., the more charity care, the higher the Medicare share value). Hospitals would receive the full incentive payment amount in the first fiscal year, 75% in the second fiscal year, 50% in the third fiscal year, and 25% in the fourth, and final, fiscal year. Hospitals that do not become eligible until after FY2015 will receive no payments. Beginning in FY2015: (1) eligible hospitals that failed to report required RHQDAPU quality data would see their market basket (MB) update reduced by one-quarter (i.e., 25%); and (2) eligible hospitals that are not meaningful users of certified EHR systems would see the other three-quarters of their MB update reduced by 33% in FY2015, 67% in FY2016, and 100% in FY2017 and each subsequent fiscal year. The Secretary may, on a case-by-case basis, exempt eligible hospitals (e.g., rural hospitals that lack sufficient Internet access) from the payment reduction if it is determined that being a meaningful EHR user would result in significant hardship. Such exemptions may not be granted for more than five years.	Medicare pays acute care hospitals using a prospectively determined payment for each discharge. These payment rates are increased annually by an update factor that is established in part by the projected increase in the hospital market basket (MB) index. Under the Reporting Hospital Quality Data for Annual Payment Update (RHQDAPU) program, hospitals that do not submit required quality data have the applicable MB percentage reduced by two percentage points. Currently, Medicare's payments to acute care hospitals under the inpatient prospective payment system are not affected by the adoption of EHR.
	Critical access hospitals (CAHs) that are meaningful users of certified EHR technology are eligible for reasonable cost-based reimbursement for the purchase of such technology, based on an enhanced Medicare share that equals the Medicare share calculated for acute-care hospitals for EHR bonuses (see above), including the charity care adjustment, plus an additional 20 percentage points, except the enhanced Medicare share may not exceed 100%. CAHs that are meaningful EHR users may expense these costs in a single payment year and receive prompt interim payments, rather than receiving reimbursement over a multiyear depreciation schedule. Beginning in FY2011, if a CAH is a meaningful EHR user, they are eligible for four consecutive years of payments, except that a CAH cannot get bonuses after FY2015. Beginning in FY2015, CAHs that are not meaningful EHR users would have their Medicare reimbursement rate reduced as follows: for FY2015, 100.66%; for FY2016, 100.33%; and for FY2017 and each subsequent fiscal year, 100%. CAHs are eligible for the same hardship exemption as acute-care hospitals.	Critical access hospitals (CAHs) are limited-service facilities in rural areas that offer 24-hour emergency care, have no more than 25 acute care inpatient beds, and have a 96-hour average length of stay. Generally, CAHs receive 101% reasonable, cost-based reimbursement for inpatient care provided to Medicare beneficiaries.
	The EHR payment incentives and penalties also apply to hospitals that are under common corporate governance with a qualifying MA organizations and serve enrollees in an MA plan offered by the organization.	

Topic	Summary of Provision	Current Requirements and Activities
Hold Harmless, Implementation Funding	The Medicare EHR incentive payments are not to be taken into account when calculating Part B premiums or payments rates for MA plans. Monies in the Medicare Improvement Fund may be used to adjust Part B payments to protect against projected shortfalls due to any increase in the conversion factor used to calculate the Part B fee schedule. The Act appropriates $100 million for each of FY2009 through FY2015, and $45 million for FY2016, to implement the above Medicare provisions. The amounts appropriated are to be available until expended.	
HIT Incentive Payment Study	The Secretary is required to conduct a study, and report to Congress by June 30, 2010, on whether EHR payment incentives should be made available to health care providers who are receiving minimal or no payment incentives or other funding under this Act. The study must include an examination of the adoption rates and clinical utility of EHR technology by such providers, and the potential costs and benefits of making payment incentives to such providers, among other things.	

Topic	Summary of Provision	Current Requirements and Activities
Medicaid Funding (Subtitle B)		
EHR Adoption and Operation Payments	The Act authorizes a 100% federal match for payments to certain qualifying Medicaid providers to encourage the adoption and use of certified EHR technology. The 100% federal match applies to 85% of the net average allowable EHR technology costs of a physician, dentist, nurse mid-wife, nurse practitioner, or physician assistant (practicing in a rural clinic of federally qualified heath center led by a physician assistant): (1) who is not hospital-based and has at least a 30% Medicaid patient volume; or (2) who practices predominantly in a federally qualified health center or rural clinic and has at least a 30% Medicaid patient volume. Pediatricians need only a 20% Medicaid patient volume to be eligible. The 100% federal match also applies to EHR-related payments to children's hospitals, and to other acute-care hospitals with at least a 10% Medicaid patient volume, up to a maximum amount. The state must provide assurances to the Secretary that all allowable costs are paid directly to the provider without any deduction or rebate; that the provider is responsible for payment of the other 15% of EHR technology costs; and, that for costs not associated with purchase and initial implementation, the provider demonstrates meaningful use of certified EHR technology. The Secretary may deem that the establishment of meaningful EHR use for the purpose of Medicare incentive payments is sufficient to qualify as meaningful use under this section. In order to receive Medicaid EHR payments, a provider must waive any right to Medicare EHR incentive payments. For physicians, dentists, nurse mid-wives, nurse practitioners, and qualifying physician assistants who are not hospital-based, the net average allowable costs are to be determined by the Secretary, based on studies submitted by states, but may not exceed: (1) $25,000 in the first year of payment (which may not be later than 2016), intended to cover the purchase and initial implementation of EHR technology; and (2) $10,000 a year thereafter, for a period of up to five years, to cover the costs of EHR operation, maintenance and use. Eligible pediatricians may receive up to two-thirds of those amounts. Allowable costs for children's hospitals and acute-care hospitals are based on the Medicare EHR incentive payment formula, with some modifications. Hospital EHR technology payments may not be made after 2016, unless the provider received a payment for the previous year, and may not be made over a period of more than six years. The Secretary must ensure coordination of the various HIT payment programs for the different types of providers, as well as the HIT payments provided under Medicare and Medicaid, to assure no duplication of funding. The Act authorizes a 90% federal match for payment to the states to administer the EHR technology payments. The Act further requires that the Secretary periodically submit reports to Congress on the status, progress and oversight of payments to Medicaid providers for EHR technology adoption and operation. The Act appropriates $40 million for each of FY2009 through FY2015 and $20 million for FY2016, to remain available until expended, for administering the EHR technology payments.	The federal government pays a share of every state's spending on Medicaid services and program administration. The federal match for administrative expenditures does not vary by state and is generally 50%, but certain functions receive a higher amount. The Medicaid statute authorizes a 90% match for expenditures attributable to the design, development, or installation of mechanized claims processing and information retrieval systems—referred to as Medicaid Management Information Systems (MMISs)—and a 75% match for approved MMIS operations. A 50% match is available for non-approved MMISs. States are required to have an MMIS that meets specified requirements and that the Secretary has found (among other things) is compatible with the claims processing and information retrieval systems used in the administration of the Medicare program.

Source: Table prepared by the Congressional Research Service, based on P.L. 111-5 (Division B, Title IV), signed by the President on February 17, 2009.

Author Contact Information

C. Stephen Redhead
Specialist in Health Policy
credhead@crs.loc.gov, 7-2261

Acknowledgments

Jim Hahn, Sibyl Tilson, Rich Rimkunas, and Paulette Morgan contributed to this report.

Key Policy Staff

Area of Expertise	Name	Phone
HIT policy, ONCHIT, standards, grants, privacy	C. Stephen Redhead	7-2261
Medicare physicians	Jim Hahn	7-4914
Medicare hospitals	Sibyl Tilson	7-7368
Medicare Advantage	Paulette C. Morgan	7-7317
Medicaid	Richard Rimkunas	7-7334