Chapter 3
Clinical Informatics Policy and Regulations

Margo Edmunds, Doug Peddicord, and David Westfall Bates

Learning Objectives

- Describe the policy development process for Health Information Technology (HIT), including the role of public and private sector agencies and organizations
- Become familiar with the major federal legislation that provides legal and regulatory frameworks for HIT
- Identify at least three policy challenges that will affect practicing clinical informaticians in the future

Core Content

- Fundamental knowledge of the organization and regulatory authority of federal and state executive branch agencies that influence the practice of clinical informatics
- Familiarity with key provisions of the main legislation that affects clinical informatics practice, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical

M. Edmunds, PhD (✉)
Evidence Generation and Translation, AcademyHealth, 1150 17th Street, NW, Suite 600, Washington, DC 20036, USA
e-mail: margo.edmunds@academyhealth.org

D. Peddicord, PhD
Washington Health Strategies Group, Washington, DC, USA

D.W. Bates, MD, MHS
Division of General Internal Medicine and Primary Care, Brigham and Women's Hospital, Boston, MA, USA

J.T. Finnell, B.E. Dixon (eds.), *Clinical Informatics Study Guide: Text and Review*, DOI 10.1007/978-3-319-22753-5_3

Health (HITECH) Act, the Patient Protection and Affordable Care Act (ACA), and the Food and Drug Administration Safety and Innovation Act (FDASIA)
- Understanding of the role of private sector organizations, including professional organizations, in the policy development process

Case Vignette

A 52 year-old man presents to establish a new primary care relationship with Dr. Carol Jones. The vital signs data collected by the medical practice assistant using an electronic blood pressure monitor reveal that his blood pressure is 155/105, and his weight is 190; the computer calculates that his body mass index is 31. The practice assistant also notes that he is currently a smoker. The patient tells Dr. Jones that he is generally healthy, but he's had more trouble keeping up at work, and that he's been urinating a lot. Physical examination is normal except for the hypertension, which is apparently new.

The concept of '**meaningful use**' was established to help ensure that providers would not only adopt electronic health records, but would use them in ways that would make care better. The electronic health record (EHR) in this instance performed several tasks that might have been overlooked in a paper world—the vital signs were electronically uploaded to the EHR with no need for data entry, and the body mass index (BMI) was automatically calculated.

When Dr. Jones logs on to the secure provider portal from home that evening, there is an auto-alert in her inbox indicating that the patient's labs are ready for review and that the blood sugar is high. The next day, Dr. Jones asks her nurse to send a secure message to the patient to set up an appointment so she can explain that he has diabetes, and when the appointment takes place, she refers him to several online materials available through the health education department to provide diet and physical activity suggestions. While the patient is still in the exam room, with only a couple of clicks, Dr. Jones will generate an appointment summary letter explaining the rest of the labs to the patient, which the patient will be able to view on his personal health record (PHR). He'll also be able to track his blood sugars and his blood pressure in his PHR, and see if he is meeting his recommended targets. Because of the newly diagnosed diabetes, his name will automatically be added to the provider and practice's diabetes registry, which will help ensure that even if he misses follow-up appointments, someone will check in with him.

The adoption of EHR systems has encouraged the development of clinical decision support, helps multiple health professionals work with the same clinical information to coordinate care, and helps engage patients in their own care. It has also promoted the flow of clinical information for population health monitoring and reporting, such as maintaining registries. Taken together, all of these technology-enabled steps should help engage the individual patient, improve the quality of care he gets, and at the same time help providers manage the myriad of tasks they need to juggle more efficiently and ensure that the whole team is involved in caring for him.

Introduction

This chapter is important to the practice of clinical informatics because health information technology (HIT) policy has had major effects on the adoption, content and use of HIT in routine care, and it is likely to have downstream effects for the foreseeable future.

The chapter begins with an overview of the public policy process in the United States and the governmental, legal, and regulatory environment for HIT. It then describes the role of public-private collaborations and private-sector organizations in driving the policy process and helping to implement health information infrastructure improvements and organizational changes that will accelerate the adoption and meaningful use of HIT in a learning health system.

The chapter highlights the major governing pieces of legislation that are fundamental to the understanding of decision-making and implementation of public and private sector policies that govern the way HIT functions within delivery systems: the Health Insurance Portability and Accountability Act (HIPAA) (1996), the Health Information Technology for Economic and Clinical Health (HITECH) Act (2009); The Patient Protection and Affordable Care Act (ACA, 2009); and the Food and Drug Administration Safety and Innovation Act (FDASIA, or FDA Safety and Improvement Act, 2012). The chapter closes with a look forward to some key policy issues that will be particularly important to practicing informaticians and the health systems in which they practice over the next several years, and that may influence their becoming involved in the policy process.

Fundamentals of the Policy Process in the United States

One of the core functions of government is to act in the public interest to protect health and safety [1]. Government policies, or public policies, are positions, statements, and courses of action that reflect the government's goals and values and that may appear in the context of legislation, regulations, budgets and program priorities, written statements, speeches, executive orders, and in other ways.

In the United States, the Constitution does not explicitly grant the federal government authority over health. The states have the majority of statutory responsibility for health, insurance regulation (including medical liability), professional licensure and credentialing, and other activities [2]. The tensions and gaps between federal and state authority for health are inherent in the design of the US system of government and are re-negotiated and re-interpreted with most new laws and regulations, particularly when new responsibilities, authority, and new agencies are created by law.

In recent years, the balance of powers has been seen clearly with the variability of state responses to the Affordable Care Act (ACA). For example, by law, states are expected to exercise enforcement authority over health insurance marketplace reform or notify the Centers for Medicare and Medicare Services (CMS) that they

lack the authority or ability to enforce these reforms. In the latter cases, CMS will work out a collaborative arrangement with the states [3]. Because the policy and political climates vary so much across the states, this approach to shared federal-state responsibility can range from cooperative to contentious and may or may not reach public awareness or become the subject of public debate.

The U.S. Constitution is based on a separation of powers, meaning that Congress has the authority to make laws; the President is commander in chief and head of the executive branch of government, with the responsibility for administering and enforcing the laws; and the judicial branch or courts interpret the laws. This chapter focuses on the legislative and executive branches.

Organization and Authority of Congress

The U.S. Congress consists of the Senate, whose 100 members serve 6-year terms, and the House of Representatives, whose 435 members serve for 2-year terms. Each branch does its legislative work through committees and subcommittees, whose chairs have the most influence in the legislative process. The most influential committees are those that deal with appropriations, and some subcommittees have special oversight responsibilities for programs and issues that cut across committee jurisdictions.

In its purest form, the legislative process begins when a "lawmaker" or individual member introduces a bill, with as many co-sponsors as possible. Whenever a bill is introduced in either the House or Senate, it is first sent to the committee of jurisdiction for consideration, which can then send it to a subcommittee, hold public hearings, "mark up" or rewrite the bill. The committee then votes on whether to send the bill to the floor for debate and further consideration. If the bill reaches the floor for a vote and is passed, it then passes to the other chamber, which develops and votes on a similar bill. The two versions are reconciled in conference and another vote is held. When the conference version is passed in both chambers, it goes to the President for signature or veto.

The Senate has 21 standing committees, and the most important for health care and public health are Finance; Health, Education, Labor and Pensions (HELP); and Appropriations. In the House, there are 20 standing committees, and the key for health issues are Ways and Means; Energy and Commerce; and Appropriations. The Senate Finance and House Ways and Means Committees have jurisdiction over Medicare, Medicaid, and the Children's Health Insurance Program (CHIP), and Senate and House Appropriations Committees have authority for agencies in the Department of Health and Human Services (HHS), including the Agency for Healthcare Research and Quality (AHRQ), Centers for Disease Control and Prevention (CDC), Centers for Medicare and Medicaid Services (CMS), Food and Drug Administration (FDA), Health Resources and Services Administration (HRSA), the National Institutes of Health (NIH), the Substance Abuse and Mental Health Services Administration (SAMHSA), and the Office of the Secretary (OS).

Congressional members and staff often have or develop individual expertise in health issues, but because of the complexity of the health sector and the absence or lag time in getting relevant information from the field, they often seek advice and information from other credible sources, such as reports from the Government Accountability Office (GAO), the Institute of Medicine (IOM), the Congressional Research Service (CRS), and professional as well as trade associations such as the American Medical Informatics Association (AMIA) Health Information and Management Systems Society (HIMSS), and College of Health Information Executives (CHIME). The information provided by professional experts such as those from these organizations to Hill staff and members can provide valuable background and context for policy issues as they are playing out around the country.

Organization and Authority of the Federal Executive Branch

The President heads the executive branch of government, which administers and implements laws by developing budgets, regulations, and programmatic guidelines and also oversees programs and provides regulatory oversight as specified by law. The executive branch is organized into 15 Cabinet-level departments, including the Department of Health and Human Services (HHS), whose FY 2015 budget totals $1 trillion in outlays [4].

HHS is the principal department for protecting the health of all Americans, and it is organized into 8 agencies or operating divisions. Virtually every one has responsibilities that affect or interface with informatics.

The **Agency for Healthcare Research and Quality** (AHRQ) has provided guidance and technical assistance for planning, implementing, and evaluating HIT since 2004, when it began providing funding for implementation projects to improve patient safety and population health [5]. Over the past decade, AHRQ created a variety of toolkits to assist and support health systems and the clinical community in developing decision support tools [6]. AHRQ continues to fund HIT research to improve the design and deployment of HIT systems, and has probably been the leading funder of applied evaluations.

The **Centers for Disease Control and Prevention** (**CDC**) provides funding to states through cooperative agreements that support information infrastructure development and data collection for heath promotion, disease prevention, and emergency preparedness, including biosurveillance and environmental health. CDC has been the federal focal point for public health informatics and sponsors regular convenings for public health informaticians to share information and tools for public and population health planning, research, and reporting [7].

The **Centers for Medicare and Medicaid Services** (**CMS**) is the regulatory and payment agency for Medicare, Medicaid, and the Children's Health Insurance Program (CHIP). CMS also oversees the Medicare and Medicaid incentive programs for the adoption and meaningful use of EHRs, in collaboration with the Office of the National Coordinator for HIT (ONC).

The **Food and Drug Administration** (**FDA**) protects the public health by assuring the safety and security of human and veterinary drugs as well as food safety. The FDA Safety and Innovation Act (FDASIA), which will be covered further below, expanded the FDA's authority to include mobile medical applications [8].

The **Health Resources and Services Administration** (**HRSA**) provides support and technical assistance for safety net providers, such as Federally Qualified Health Centers, rural hospitals, and critical access hospitals, to implement HIT systems and health information exchanges [9].

The **Indian Health Service** (**IHS**) provides funding and technical assistance to improve the quality, safety, and efficiency of health information systems used in providing health care and services for 1.9 million American Indians and Alaska Natives (AI/AN) [10]. IHS maintains a database of best practices (evidence-based practices) in AI/AN communities, schools, work sites, and health centers, clinics, and hospitals [11]. IHS uses an Electronic Health Record (EHR) derived from the VHA VISTA EHR code base and has developed a comprehensive suite of software applications to help meet meaningful use and quality reporting requirements [12].

The National Institutes of Health (**NIH**) [13] is the single largest funder of biomedical research, and the **National Library of Medicine** (**NLM**), the world's largest medical library, produces electronic information that is searched by millions of people (e.g. MEDLINE, PubMed) and also has the lead federal responsibility for developing clinical terminology standards for HIT. NLM also has been a leading source of support for the field of informatics through fellowships at NLM and sponsored university-based training programs [14]. One of many free NLM information resources is MedlinePlus Connect, which allows health organizations and HIT providers to link electronic record (EHR) systems and patient portals to MedlinePlus, which has hundreds of health topic pages aimed at consumers [15].

The **Substance Abuse and Mental Health Services Administration** (**SAMHSA**) supports programs for the promotion of mental health and the treatment and prevention of substance use disorders and mental illness, also known as behavioral health conditions. To help ensure that behavioral health and physical health services share information while ensuring patient confidentiality, SAMHSA and HRSA collaborate to use HIT to support care coordination among networks of providers, patients, and payers.

The **Office of the National Coordinator for HIT** (**ONC**). Located administratively in the Office of the Secretary of HHS, ONC is charged with coordinating nationwide efforts to implement and use HIT to exchange electronic health information [16]. ONC was created in 2004 by a Presidential Executive Order and was codified (mandated legislatively) in the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009. ONC is responsible for coordinating HIT activities within the executive branch, making sure that the federal HIT programs are meeting the objectives of the strategic plan to create a nationwide HIT infrastructure, and reporting on progress being made in public and private sectors.

The **Office for Civil Rights** (**OCR**). Located administratively in the Office of the Secretary of HHS, OCR enforces HIPAA and civil rights laws to "protect fundamental

rights of nondiscrimination and privacy." OCR is the principal drafter and compliance enforcer of the HIPAA rules meant to protect individually identifiable health information, including the Privacy, Security and Breach Notification rules.

Other Key Federal Agencies for HIT

Outside of HHS, the **Veterans Health Administration** (**VHA**), part of the **U.S. Department of Veterans Affairs** (**VA**), is not only a major provider of health services for veterans and the largest integrated healthcare system in the US, but also an early adopter of EHRs and consumer web portals to facilitate patient access to clinical records. VistA, the Veterans Health Information Systems Technology Architecture, provides an integrated inpatient and outpatient EHR for patients at the VA and allows nationwide access through all VA facilities [17].

The **National Institute for Standards and Technology** (**NIST**) was created by Congress in 1901 to develop a measurement infrastructure, beginning with standards in the physical sciences. Now located within the Department of Commerce, NIST has evolved to include global communication networks and other technologies and includes a health and standards testing program that collaborates with ONC to help improve health care delivery through HIT [18].

The **President's Council of Advisors on Science and Technology** (**PCAST**), administered by the Office of Science and Technology Policy in the White House, is an advisory panel appointed by the President that expands the range of science and technology advice available through the executive branch. Members are selected from academic and research institutions, industry, and non-governmental organizations and have expertise in many areas of science and technology innovation. A 2010 PCAST report on HIT called for an acceleration of efforts to build a digital infrastructure for healthcare [19] and PCAST reports in 2014 called for the use of a systems engineering approach to address healthcare cost and quality challenges [20] and analyzed the technical aspects of big data and privacy [21].

The **Federal Trade Commission** (**FTC**) was created by Congress in 1914 to protect consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace and promoting competition by ensuring free and open markets. In February 2010, FTC began enforcing its Health Breach Notification Rule for web-based businesses that are not covered by HIPAA.

Role of the Private Sector in Policy Development

Independent advisory bodies have always played a vital role in health policy development. Since 1949, the **National Committee on Vital and Health Statistics** (**NCVHS**) has served as a statutory advisory body to the Secretary of HHS on health information policy, making policy recommendations on a variety of topics affecting

health information infrastructure and informatics, including data access and quality, standards, privacy and confidentiality, and population health [22].

In 1970, the National Academy of Sciences founded the **Institute of Medicine** (**IOM**) to provide independent advice to Congress and the executive branch on issues related to health and science policy. Over the years, IOM committees have been convened to issue reports on health care coverage and access, health services research priorities, health care quality, patient safety, the role of HIT in health system transformation, public and population health, and many other subjects. IOM studies are sometimes Congressionally mandated or requested, or may also be requested and funded by federal agencies or private organizations [23]. Their influence on health policy development in both public and private sectors has been very substantial.

The **Patient-Centered Outcomes Research Institute** (**PCORI**) is a nonprofit, nongovernmental organization created by the Affordable Care Act to fund comparative effectiveness research (CER) and disseminate findings widely to policy-makers, practitioners, and the general public. PCORI seeks to improve clinical outcomes by filling evidence gaps about what works in clinical practice and by engaging consumers in developing research questions that will answer their questions about treatment options. The emphasis on patient-centered research outcomes (PCOR) is a departure from previous priorities driven by the biomedical research community and is helping to build an information infrastructure for working with electronic health record (EHR) data that can be readily shared with patients and consumers.

Health care represents the largest sector for federal lobbying, accounting for $549 million in calendar year 2013 [24] and there are approximately 8 registered lobbyists for each member of Congress [25]. But individual members of national organizations such as AMIA, HIMSS, the American Hospital Association (AHA), the American Medical Association (AMA), the American College of Physicians (ACP), and many others also can be influential in the policy development process by meeting with Congressional members and staff to provide technical background, sharing real-world experiences about how legislation and regulations are being implemented, and being available to advise on legislative language, speeches, hearings, constituent meetings, and other activities.

The Policy Environment for Clinical Informatics

For practicing informaticians, it is vitally important to be familiar with influential and policy-relevant pieces of legislation. In this section, we will discuss the Health Insurance Portability and Accountability Act (HIPAA), HITECH (Health Information Technology for Economic and Clinical Health Act), the Patient Protection and Affordable Care Act (ACA), and the Food and Drug Administration Safety and Innovation Act (FDASIA). We include a timeline of key legislative and regulatory events associated with these laws to put them in context (Table 3.1).

Table 3.1 Timeline of key legislative and regulatory events

August 1996	Health Insurance Portability and Accountability Act (HIPAA) requires development of standards for electronic exchange of health information under administrative simplification provisions
December 2000	HIPAA Privacy Rule sets national standards to protect individually identifiable personal health information used by health plans, health care clearinghouses, and health care providers (covered entities)
August 2002	HIPAA Privacy Rule is modified and finalized, with a compliance date of April 2003 for most entities
February 2003	HIPAA Security Rule establishes national standards to protect the confidentiality, integrity, and security of electronic personal health information
April 2004	Presidential Executive Order creates Office of the National Coordinator for HIT (ONC) in the Office of the HHS Secretary and calls for widespread use of HIT within 10 years
February 2009	Congress passes the Health Information Technology for Economic and Clinical Health (HITECH) as part of the American Reinvestment and Recovery Act of 2009 (ARRA), outlining an incentive program for adopting electronic health records known as meaningful use and creating a HIT Policy Committee and an HIT Standards Committee to advise ONC
March 2011	ONC releases a 5-year strategic plan for HIT to increase adoption of EHRs, promote health information exchange, and promote individual access to health information
July 2012	Congress passes the Food and Drug Administration Safety and Innovation Act (FDASIA), stimulating medical device innovation while expanding the agency's authority to regulate medical devices
January 2013	HHS releases an "omnibus" Rule that makes changes to HIPAA Privacy, Security and Enforcement Rules as required by the HITECH statute.

From HIPAA to HITECH: What Every Informatician Should Know About Privacy Regulations Governing Health Information

In 1996 Congress passed the Health Insurance Portability and Accountability Act (HIPAA), a remnant of the Clinton health reform effort that was intended to protect ongoing health insurance coverage for workers who change or lose jobs. Title II of HIPAA, known as Administrative Simplification, required the establishment of national standards for electronic health care transactions and development of national identifiers for providers, health insurance plans, and employers. Broadly, the idea was to facilitate the transition of the U.S. health care system from antiquated paper records and communications systems to an efficient electronic information environment by establishing standards for the use and exchange of health care information.

But even as it committed to advancing electronic health information technologies, Congress was concerned about the privacy and security of health records and so the HIPAA law called for passage of national health information privacy legislation within 36 months, with the proviso that the Secretary of Health and Human Services (HHS) would promulgate health privacy standards if Congress failed to

act. And thus in the period from 1999 through 2002 the HIPAA Privacy Rule was developed by HHS. Since that time, HIPAA has been updated once, in the HITECH Act of 2009.

What Should Every Informatician Know About HIPAA Today – and What Developments Might We Expect in the Future?

The Basics of the Privacy Rule: HIPAA 1 – From 2002 to 2009

The Privacy Rule Provides rights to individuals (patients) and mechanisms for the exercise of those rights, while imposing obligations on covered entities to protect the privacy of individually identifiable health information and to facilitate the individual's rights.

Who Is Covered by the Rule?

Covered Entities: Provisions of the rule apply to covered entities: health plans, health care clearinghouses, and "health care providers who transmit health information in electronic form in connection with any transaction referred to in Section 1173(a)(1)." (Transactions include: health claims or encounter information – enrollment and disenrollment – eligibility – payment and remittance advice – premium payments – 1st report of injury – claim status – referral certification and authorization)

What Is Covered?

Health Information: any information created or received by a health care provider that "relates to the past, present or future physical or mental health or condition of an individual", the provision of care, or payment for care.

Individually Identifiable Health Information: a subset of health information, including demographic information, that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information: means individually identifiable health information that is transmitted or maintained electronically, or transmitted or maintained in any other form or medium.

When May a Covered Entity Use or Disclose Protected Health Information (PHI)?

Without a specific consent for "treatment, payment and health care operations" (but subject to "minimum necessary" limitation and "notice" must be provided.)

With certain exceptions, *all other uses/disclosures require an authorization* signed by the individual. (Exceptions to authorization include: when required by law; for public health; to avert serious threats to health or safety; for health oversight; for law enforcement; and for research, subject to various conditions.)

What About Business Associates?

Business Associates "perform or assist in the performance of" a function or activity involving the use or disclosure of individually identifiable health information *on behalf of* a covered entity, under a written contract that cannot permit the business associate to make any uses/disclosures that the covered entity could not make. BAs "work for" CEs on activities related to "treatment, payment and health care operations." They are not directly subject to the jurisdiction of HHS, but are contractually 'regulated through' the covered entity.

Points to Remember

Within the HIPAA Privacy Rule, always think about:

- *Who the Rule covers* – providers, health plans, claims clearinghouses;
- *What the Rule covers* – protected health information (PHI);
- *Who is doing what, for whom, under what condition* – covered entities, business associates on behalf of covered entities, others (under certain exceptions: e.g., public health authorities, researchers under limited circumstances.)

Under the Privacy Rule, consider in every instance under what authority PHI is used or disclosed:

- *Without consent* – for "treatment, payment, health care operations" of the covered entity, subject to minimum necessary limitation and Notice must be provided to the individual;
- *To a business associate performing activities on behalf of a covered entity, by contract*, which cannot permit any uses or disclosures that the covered entity would not be permitted;
- *With an individual authorization,* (e.g., for the release or transfer of records, for the use or disclosure of PHI for research, etc.)*;*
- *Under a waiver granted by an IRB or Privacy Board;*
- *To a person subject to the jurisdiction of the FDA,* (e.g., for the reporting of adverse events to a pharmaceutical company) – but not for commercial purposes;
- *And for certain public health, health oversight and law enforcement purposes.*

These six pathways constitute the entirety of methods by which PHI can be used or disclosed between and among covered entities and business associates, and the ways in which a covered entity or business associate can disclose PHI to an entity

that is not subject to HIPAA per se, such as a pharmaceutical company collecting clinical trial data as permitted by an individual's signed authorization.

What Happens If a Covered Entity Fails to Comply with HIPAA Requirements?

The covered entity could be subject to civil penalties of $100 per violation for failure to comply with standards, and up to $50,000 fine for wrongful disclosure of individually identifiable health information. The covered entity will be unable to use or disclose individually identifiable health information lawfully.

HIPAA in the HITECH Era: 2009 to the Present

In 2009 President Obama signed into law the American Recovery and Reinvestment Act (ARRA) a $787 billion package of "shovel ready" projects intended to stimulate an economy in deep recession. Included in ARRA was the HITECH Act, which provided for between $25 and $36 billion in incentive payments for the adoption of electronic health record (EHR) system that included functionalities sufficient to demonstrate "meaningful use." HITECH also included a series of provisions that were intended to strengthen the privacy and security requirements of HIPAA, and to broaden the reach of the rules.

Who Is Covered Under HITECH?

- Covered Entities (CEs)
- Business Associates (BAs) – not just by contract now, but directly subject to the jurisdiction of HHS in regard to the requirements (and penalties) of the HIPAA Security Rule and relevant provisions of the Privacy Rule. This expanded jurisdiction over business associates specifically included entities that transmit or process data on behalf of CEs, like RHIOs, E-Prescribing Gateways and cloud providers.
- Personal Health Record (PHR) vendors, in relation to new breach reporting obligations.

The Largest New Requirement is Breach Reporting – So What's a Breach?

- A breach is "unauthorized acquisition, access, use, or disclosure" of PHI which compromises security or privacy, except –
- when the person could not have reasonably retained the PHI
- is to an employee acting in good faith and under the scope of his/her employment
- is an inadvertent disclosure made by an authorized person and occurs within the facility

And the PHI is not further acquired, accessed, used, disclosed, etc.

What Happens in the Event of a Breach?

In the event that a CE discovers a breach, it shall "notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired or disclosed as a result of such breach:"

- Without unreasonable delay and in no case later than 60 calendar days;
- In writing, by US mail or electronically (and, in certain cases, via broadcast media, web posting, etc.);
- Notify the Secretary of HHS, either immediately (if more than 500 persons involved) or annually;
- (And similar requirements apply to PHR vendors, who will notify individuals and the Federal Trade Commission).

And What Must the Notification to an Individual Include?

- What happened, including the date of the breach and the date of its discovery;
- The type of PHI involved;
- Steps individuals should take to protect their privacy and/or identity;
- What the CE is doing to investigate, mitigate and protect against future breaches;
- Contact procedures for questions and additional information.

What Is the Cost of Breach Reporting to the Covered Entity, Business Associate or PHR Vendor?

The total costs of a breach incident – including preparing notices to individuals, providing identity theft monitoring service, legal costs, etc. – have been estimated at up to $200 per individual whose PHI was breached. This does not include the loss of consumer trust and institutional reputation incurred by the covered entity, business associate or PHR vendor, nor fines of up to $1.5 million per year that can be levied by HHS.

What Are Some of the Other New Obligations and Requirements HITECH Put in Place?

- CEs must, on request of the individual, provide an accounting of non-oral disclosures made for purposes of treatment, payment or health care operations for a period of 3 years [this rule has not been finalized, and is not enforced by HHS at this time];

- CEs must, on request, restrict disclosure of PHI to a health plan for purposes of payment or health care operations, if the individual self-pays for a service;
- In making uses or disclosures for payment or health care operations, CEs must use a 'limited data set', to the extent practicable;
- If a CE or BA receives direct or indirect remuneration for communications with an individual this is Marketing and requires an authorization, except for communications relating to a drug or biologic currently being prescribed.

Changes Made by HITECH Regarding Enforcement and Penalties

- Business Associates are directly subject to Security and applicable Privacy provisions;
- Criminal penalties can be enforced against individuals, not just CEs and their employees;
- Civil monetary penalties (CMPs) must be pursued by HHS in cases in which a covered entity or business associate shows "willful neglect" of the rules;
- CMPs are increased from $100 per violation with an annual maximum of $25,000 to up to $50,000 per violation and an annual maximum of $1.5 million.

Under HIPAA and HITECH

- PHI can be used and disclosed only as permitted.
- A limited data set that excludes 16 direct identifiers and is disclosed with a data use agreement for research, public health or health care operations is still considered PHI for the purposes of breach reporting.
- The only methods for rendering unsecured PHI "unusable, unreadable or indecipherable" and therefore not subject to breach reporting requirements are *encryption* and *destruction*.
- "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information" – *and therefore is not subject to the requirements of the HIPAA Privacy or Security Rules.* The two acceptable methodologies of de-identification are the Safe Harbor in which 18 identifiers are removed or the Statistician's Certification in which the risk of re-identification is determined to be "very small."

Meaningful Use (HITECH) and the Affordable Care Act (ACA)

Before 2004, the U.S. did not have HIT coordination at the national level. That changed with the appointment of David Brailer by President George W. Bush and the establishment of the Office of the National Coordinator by Presidential Executive Order.

Later, in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed to encourage hospitals and outpatient providers to both adopt electronic health records, and use them in meaningful ways. National coordination was linked with grant programs and payment incentives, under the assumption that this would result in enhanced trust would enable providers who had been "on the fence" about EHR adoption to move forward.

A key to this was the new concept of "**meaningful use**." The idea was to try to ensure that providers would not simply adopt electronic health records, but that they also would use them in ways that would improve the safety and quality of healthcare, and reduce its costs. This was linked with the "escalator concept," the idea being that providers would get on the escalator and continue up it, to higher levels of adoption and better care delivery. Meaningful use has three stages. To qualify for Stage 1, providers simply needed to adopt EHRs that were certified. For Stage 2, providers had to begin to implement advanced care processes linked with clinical decision support. The hope with Stage 3 is that providers will be able to go all the way to demonstrating improved outcomes.

Although they were enacted over a year apart, today the HITECH Act is closely linked with the Affordable Care Act, which is intended to begin payment reform and includes the notion that providers will be accountable for the costs of the care they deliver. As part of HITECH, two HIT committees were formed—the HIT Policy and Standards committees. The concept of meaningful use was developed by the Health Information Technology Policy Committee, which then sent its recommendations to ONC. ONC refined them and worked with CMS to convert these recommendations into regulations that would result in payment for providers who qualified. The Standards Committee has been asked to identify standards for all the main types of clinical data, and this has largely been accomplished, which will make it much easier for vendors to move forward. Examples include LOINC (Logical Observation Identifiers Names and Codes) for laboratory results and SNOMED (Systematized Nomenclature of Medicine-Clinical Terms) for problems. The work of both the HIT Policy and Standards Committees has been completely in the open.

Stage 1 of Meaningful Use has been quite successful, in that around 80% of hospitals and eligible providers in the outpatient setting qualified. Attestation rates, however, have been much lower to date for Stage 2, and it is unclear how much these will rise over time [26, 27]. The final criteria for Stage 3 were released early in 2015. Vendors and providers have generally felt that the criteria to be met have been too difficult, while payers and patient groups have pushed for more stringent criteria. To qualify, providers have to meet all the criteria, which has involved doing a number of things that they would not have done as quickly as they did them because of the incentives involved.

Many have been concerned that the need to meet the criteria has diverted attention from their own quality and efficiency improvement agendas. While the program appears to have gotten a high proportion of providers to adopt, it is probably too early to assess the impact of the meaningful use criteria on the quality, safety and efficiency of healthcare, though these have been the main target of the policy.

Federal Drug Administration Safety and Innovation Act (FDASIA)

Signed into law in 2012, the Federal Drug Administration Safety and Innovation Act (FDASIA) gives the FDA authority to continue to collect user fees from the biomedical industry, as well as to regulate medical software. The Secretary of Health and Human Services asked the Health Information Technology (HIT) Policy Committee to convene a stakeholder group to help provide input into the development of a framework for regulating software. This was done through ONC, FDA, and the Federal Communication Commission. The workgroup was asked to put forward a risk-based regulatory framework, including how healthcare IT systems could be stratified in terms of risk, and recommendations about how the regulatory requirements currently in place should be adapted. The tri-agencies then took these suggestions and released a full report in the spring of 2014 [28].

Key findings of the report were that electronic health records were felt to be relatively low-risk, so that full FDA regulation would not be helpful, and could stifle innovation. Nonetheless, it was clear that HIT does create new risks. One of the main recommendations of the report was that it would be helpful to create a new HIT Safety Center, and a federal contract has been let to provide input around what the mandate of and goals for such a center might be.

Emerging Trends

The regulatory framework for assuring the privacy and security of an individual's health information will continue to evolve. The circle of HIPAA coverage is expanding from covered entities during the first era to business associates and PHR vendors post-HITECH. Protected health information (PHI) is beginning to become less contextually determined; e.g., "PHR identifiable health information" does not need to be created, managed, or held by a CE or BA, but can be held by the person or by another party.

While in the early days of HIPAA there were promises that "there will never be HIPAA police" and that HHS would always look to educate covered entities and business associates about how to follow the rules, the post-HITECH era has seen a marked shift to compliance enforcement, supported by the imposition of fines and penalties for non-compliance. In another development, the Federal Trade Commission (FTC) is increasingly asserting oversight of the privacy and security of health information as a consumer protection issue, which sometimes means that those covered by HIPAA will also be subject to enforcement actions by the FTC.

We foresee many public discussions about big data, interoperability, mobile devices and user-generated data. HIPAA does not apply to health data collected, accessed, used and/or disclosed by non-covered entities, such as websites and consumer-facing devices and apps. At the same time, it is not clear how the FDA

and/or other regulators should regulate HIT hardware and software [29]. Clinical informaticians may be asked to form opinions and offer public comment on whether a new regulatory framework should extend HIPAA-like protections (and obligations on app developers and mobile companies) to such "nonhealth" data.

For example, future informaticians will need to decide whether HIPAA's de-identification methodologies (Safe Harbor and "statistician certification") are adequate in an era of big data. They will need to evaluate the potential risks of re-identification of data, and decide what protections would prevent harm to individuals while maintaining the workflow of clinical research and quality reporting.

Once the HITECH adoption incentives are gone, we don't yet know what array of incentives, mandates, standards, etc. will be needed to improve the interoperability of health data systems across sites of care, payment systems, methods of data collection, etc. There is a tremendous gap between the generators of clinical research data and clinical care data, and also between the original generators of data and those who reuse the data for research and reporting. Currently, there are few opportunities for these spheres to interact and inform each other. Similarly, there are too many examples of healthcare systems developing their own standards when interoperability would be far better served by their using existing standards and specifications. However, as long as healthcare systems see themselves primarily as competitors and as owners of proprietary data, the incentives for data-sharing will continue to be limited.

We encourage clinical informaticians to engage in the coming policy debate on these issues through AMIA and other professional associations, as well as through governance discussions in your own institutions. The debate will be far more productive when practicing informaticians bring real-world evidence to the discussion.

Summary

The adoption and use of HIT in the U.S. has been influenced by a complex set of factors in both public and private sectors. These include geographic variations in technology infrastructure investments; variations in provider experiences and attitudes toward information technology; the complexity of communicating the regulatory environment governing information-sharing under HIPAA; market forces, particularly competition among providers and lack of alignment of financial incentives for providers to invest in Health IT; variations in legal interpretations of HIPAA across institutions; general lack of familiarity among clinical practitioners with the policy process and the regulatory environment in which they practice; and siloes, and even some competition, among the federal entities whose authorities span Health IT.

The recent implementation of meaningful use has had a profound impact on the adoption of HIT in the U.S., and it has also had major effects on what features electronic health records contain. The vendors have been so busy with responding to the requirements of meaningful use that they have been less responsive to the requests of their users. Whether or not this policy will have the desired long-term impact on health

care quality and costs is uncertain, but it has had a huge impact on clinical informatics. Similarly, the extent to which information technology is regulated in the future by the government – and the culture and approach of the different federal regulatory agencies (e.g., CMS, FDA, FTC) is likely to have a major impact on how HIT develops.

At the highest conceptual level, and at the operational level within individual healthcare delivery systems, the HIT enterprise requires ongoing and continuous collaboration and cooperation between public and private sectors. We hope that this chapter has helped to illuminate the reasons why all clinical informaticians will benefit from a working knowledge of the policy process and regulatory environment, including the key federal and private-sector agencies and organizations that engage with each other to drive HIT implementation and use.

Questions for Discussion

1. The Medicare and Medicaid EHR Incentive program provides financial incentives for the meaningful use of certified EHR technology to improve patient care. Payers and patient groups have generally pushed for more stringent meaningful use criteria, while providers and vendors have generally felt that the criteria were too difficult. Why did stakeholders disagree about the speed of implementing and adopting EHRs?
2. The Office of the National Coordinator is charged with coordinating HIT within the executive branch and reporting on progress in the public and private sectors. How do you think the role of ONC will change in the new post-HITECH ecosystem, after the financial incentives for adoption of EHRs are gone?
3. What is the role of professional organizations, particularly the American Medical Informatics Association (AMIA), in policy development and implementation?
4. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. Is the Privacy Rule adequate to protect the privacy of personal health information?
5. The FDA has the authority to regulate medical software and will focus on medical device Health IT functionality, but not on platforms or product names. Is this a reasonable regulatory approach?

References

1. Frieden TR. Government's role in protecting health and safety. N Engl J Med. 2013;368:1857–9. doi:10.1056/NEJMp1303819 [cited 2014 Dec 6]. Available from http://www.nejm.org/doi/full/10.1056/NEJMp1303819.
2. Turnock BJ. Public health – what it is and how it works. 3rd ed. Boston: Jones and Bartlett Publishers; 2004.

3. The Center for Consumer Information and Insurance Oversight (CCIIO), Centers for Medicare and Medicaid Services (CMS), Department of Health and Human Services (HHS). Ensuring compliance with the health insurance market reforms. [Internet]. 2014 [cited 2015 Jan 1]. Available from http://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Market-Reforms/compliance.html.
4. Health and Human Services (HHS) FY 2015 budget in brief. [Internet]. 2014 [cited 2015 Jan 1]. Available from http://www.hhs.gov/budget/fy2015-hhs-budget-in-brief/hhs-fy2015budget-in-brief-overview.html.
5. AHRQ. HHS awards $139 million to drive adoption of health information technology. Rockville: Agency for Healthcare Research and Quality [Updated October 13, 2004–August 3, 2009]. Available from: http://www.ahrq.gov/news/press/pr2004/hhshitpr.htm.
6. Agency for Healthcare Research and Quality (AHRQ), HHS. [Internet] 2014 [cited 2015 Jan 1]. Available from http://healthit.ahrq.gov/health-it-tools-and-resources.
7. Public Health Informatics Conference. About the conference. [Internet] [cited 2015 Mar 18]. Available from http://phiconference.org/about-the-conference/.
8. Food and Drug Administration Safety and Innovation Act (FDASIA). [Internet] 2015 [cited 2015 Jan 9]. Available from http://www.fda.gov/RegulatoryInformation/Legislation/FederalFoodDrugandCosmeticActFDCAct/SignificantAmendmentstotheFDCAct/FDASIA/.
9. Health Resources and Services Administration (HRSA). HIT implementation toolbox: 9 steps to implement EHRs. [Internet] 2015 [cited 2015 Jan 1]. Available from http://www.hrsa.gov/healthit/toolbox/healthitimplementation/index.html.
10. Indian Health Service. Health information technology. [Internet] 2015 [cited 2015 Jan 1]. Available from http://www.ihs.gov/forproviders/healthit/.
11. IHS. Best and promising practices. [Internet] 2015 [cited 2015 Jan 1]. Available from http://www.ihs.gov/forproviders/bestpractices/.
12. IHS. Health information technology. [Internet] 2015 [cited 2015 Jan 1]. Available from http://www.ihs.gov/oit/index.cfm?module=dsp_oit_hit.
13. National Institutes of Health (NIH). Institutes, centers, and offices. [Internet] 2015 [cited 2015 Jan 15]. Available from http://www.nih.gov/icd/.
14. National Library of Medicine. NLM's university-based biomedical informatics research training programs. [Internet] 2014 [cited 2015 Jan 1]. Available from http://www.nlm.nih.gov/ep/GrantTrainInstitute.html.
15. National Library of Medicine (NLM). MedlinePlus Connect. [Internet] 2014 [cited 2015 Jan 1]. Available from http://www.nlm.nih.gov/medlineplus/connect/overview.html.
16. Office of the National Coordinator, HHS. About ONC. [Internet] 2014 [cited 2015 Jan 1]. Available from http://www.healthit.gov/newsroom/about-onc.
17. U.S. Department of Veterans Affairs. VistA. [Internet] 2014 [cited 2015 Jan 1]. Available from http://www.ehealth.va.gov/VistA.asp.
18. National Institute for Science and Technology (NIST), Department of Commerce. Health information technology. [Internet] 2015 [cited 2015 Feb 9]. Available from http://www.nist.gov/healthcare/.
19. President's Council of Advisors in Science and Technology (PCAST). Realizing the full potential of health information technology to improve healthcare for Americans. [Internet] 2010 [cited 2015 Jan 1]. Available from http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.
20. PCAST. Better health care and lower costs: accelerating improvement through systems engineering. [Internet] 2014 [cited 2015 Jan 9]. http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_systems_engineering_in_healthcare_-_may_2014.pdf.
21. PCAST. Big data and privacy: a technological perspective. [Internet] 2014 [cited 2015 Jan 9]. Available from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.
22. National Committee on Vital and Health Statistics. [Internet] 2014 [cited 2015 Jan 1]. Available from http://www.ncvhs.hhs.gov/about/about-the-committee/.

23. Institute of Medicine. About the IOM. [Internet] 2013 [cited 2014 Dec 28] Available from http://www.iom.edu/About-IOM.aspx.
24. Cooper K. Top dollars go to health lobbying. Political Moneyline, Congressional Quarterly [Internet] 2014 [cited 2014 Dec 28]. Available from http://blogs.rollcall.com/moneyline/top-dollars-go-to-health-care-lobbying/.
25. Eaton J, Pell MB. Lobbyists swarm capitol to influence health reform. Center for Public Integrity. [Internet] 2010 [cited 2014 Dec 28]. Available from http://www.publicintegrity.org/2010/02/24/2725/lobbyists-swarm-capitol-influence-health-reform.
26. Patel V, Jamoom E, Hsiao CJ, Furukawa MF, Buntin M. Variation in electronic health record adoption and readiness for meaningful use: 2008–2011. J Gen Intern Med. 2013;28(7):957–64.
27. Desroches CM, Worzala C, Bates S. Some hospitals are falling behind in meeting 'meaningful use' criteria and could be vulnerable to penalties in 2015. Health Affairs (Project Hope). 2013;32(8):1355–60.
28. FDASIA HIT report: proposed strategy and recommendations for a risk-based framework. [Internet] 2014 [cited 2014 Dec 29]. Available from http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf.
29. Brown SH, Miller RA. Legal and regulatory issues related to the use of clinical software in health care delivery. In: Greenes RA, editor. Clinical decision support: the road to broad adoption. 2nd ed. Academic. Boston, MA. http://www.sciencedirect.com/science/article/pii/B9780123984760000269.