The Future Role of Government in Health Information Technology and Digital Health

FEBRUARY 2018

BIPARTISAN POLICY CENTER

healthITnow

STAFF

Janet Marchibroda
Director, Health Innovation Initiative
Bipartisan Policy Center

Joel White
Executive Director
Health IT Now

G. William Hoagland
Senior Vice President
Bipartisan Policy Center

Catherine Pugh
Senior Director
Health IT Now

Mark Segal
Consultant
Bipartisan Policy Center

Tim Swope
Senior Policy Analyst
Bipartisan Policy Center

BIPARTISAN POLICY CENTER'S HEALTH INNOVATION INITIATIVE

With guidance from former Senate Majority Leader William H. Frist, MD and former Representative Bart Gordon, BPC's Health Innovation Initiative focuses on advancing innovative strategies to improve health and health care; accelerating the discovery, development, and delivery of safe and effective cures and treatments for patients; and effectively using data and technology to improve the lives of Americans.

HEALTH IT NOW

Health IT Now (HITN) is a broad-based coalition of patient groups, provider organizations, employers, and payers that supports incentives to deploy health information technology to improve care, patient outcomes, and to lower costs.

ACKNOWLEDGEMENTS

The Bipartisan Policy Center and Health IT Now would like to acknowledge and thank members of the Work Group on the Future Role of Government in Health Information Technology and Digital Health – listed in Appendix A – who contributed their time and expertise to the development of the principles and recommendations included in this report.

DISCLAIMER

The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center's founders or its board of directors.

Introduction

Health information technology (IT) and digital health are transforming the way that health care is delivered, managed, and improved—while empowering individuals to more effectively manage their health and navigate an increasingly complex health care system.

Since enactment of the bipartisan Health Information Technology Economic and Clinical Health (HITECH) Act on February 17, 2009, adoption of health IT, including electronic health records (EHRs), within the U.S. health care system has grown significantly and become the norm.

As of December 31, 2017, nearly $38 billion has been spent under the Centers for Medicare and Medicaid Services (CMS) EHR Incentive Programs, established as a result of HITECH, in support of physician and hospital adoption and "meaningful use" of EHRs.[1] HITECH contributed to significant increases in health IT adoption. The percentage of physicians who have adopted any EHR increased from 48 percent in 2009 to 87 percent in 2015.[2] During the same period, the percentage of hospitals that have adopted an EHR rose from 12 percent to 84 percent.[3]

The Meaningful Use program incentives have ended for clinicians participating in Medicare, but the rules associated with EHR use have been integrated into the Medicare Quality Payment Program (QPP). There is also significant interest in applying similar revisions to the continuing Meaningful Use programs for physicians participating in Medicaid and for hospitals participating in Medicare and/or Medicaid.

The federal government does not typically dictate the "features and functions" of private sector products or technology. However, a very directive federal policy approach for health IT emerged from the significant federal investment in adoption and use of health IT required by HITECH, and congressional and administration intent to assure that EHR technology could support the provider Meaningful Use requirements.

In response to HITECH, the Department of Health and Human Services (HHS), through the Office of the National Coordinator for Health IT (ONC), developed and implemented a very robust EHR certification program (now referred to as the ONC Health IT Certification Program), containing many detailed requirements, designed primarily to assure that such technology could support provider qualification for federal incentives under the CMS EHR Incentive Programs.[4]

While robust specifications were helpful in the early stages of HITECH implementation, over time, the level of prescriptiveness contained within the CMS EHR Incentive Programs, the Merit-based Incentive Payment System (MIPS) within QPP, and the ONC Health IT Certification Program, have contributed to dissatisfaction and increased burdens among technology users and developers.

For example, research suggests that:

- Practicing physicians spend about half of their workdays on EHRs and desk work, including 37 percent of their time in the examination room with patients, and one to two hours each night, which are devoted mostly to tasks conducted using an EHR.[5]

- Emergency physicians spend about 44 percent of their time on data entry, versus 28 percent on direct patient care.[6]

- Submitting quality data can also be time-consuming and burdensome, taking on average, 11 hours and costing $723.50 per eligible clinician.[7]

As a result, EHR and payment-related requirements can lead to lower productivity, higher costs, and physician burnout.

- A study conducted by AmericanEHR and the American Medical Association shows that:

  - 43 percent of physicians have yet to overcome the productivity challenges related to their EHR systems;

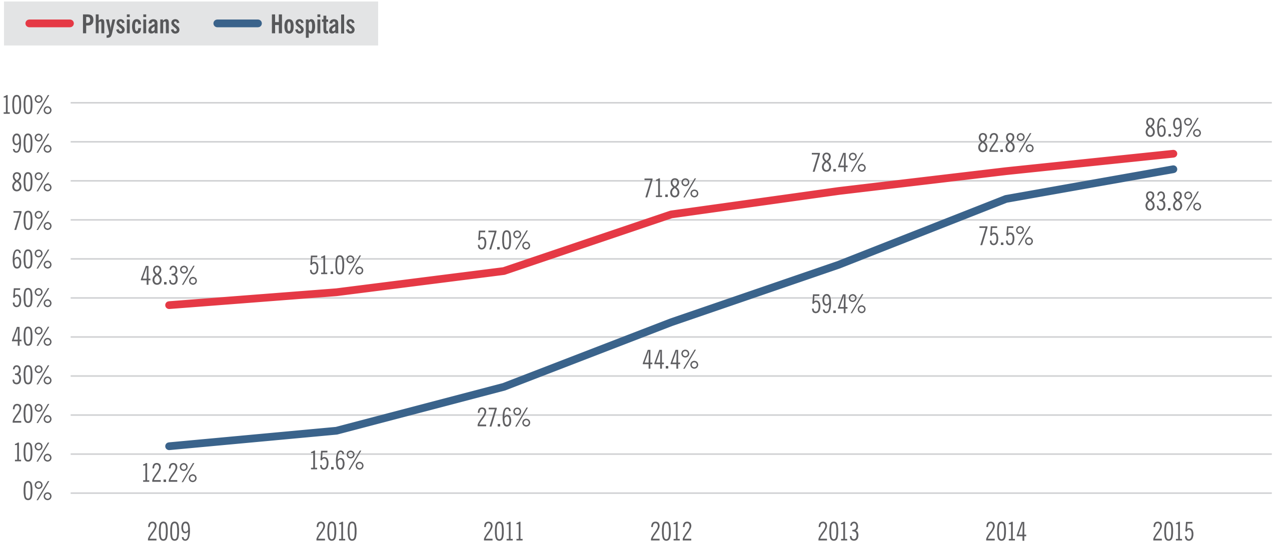
  - 42 percent thought that their EHR system's ability to improve efficiency was difficult or very difficult; and

  - 54 percent found that their EHR system increased their total operating costs.[8]

- Also, more than half of physicians—54 percent—experience symptoms of burnout, representing a 22 percent increase over the last three years.[9]

When well-designed, implemented, and used, EHRs—as well as other technologies used in treatment and clinical documentation—support better patient care and improved clinical outcomes through enhanced communication.[10] However, embedding very specific requirements for both providers and developers regarding what must be done, how it must be done, and how it must be measured—through a "one-size fits all" regulatory approach—can result in unintended consequences, including diversion of resources away from other activities that result in better outcomes and reduced costs. These consequences include failure to achieve the results that drove the requirements in the first place. The private sector is advancing efforts to address these challenges, including the pediatric EHR initiative supported by the American Academy of Pediatrics and EHR recognition programs supported by the Healthcare Information Management Systems Society (HIMSS).

Figure 1: Adoption of EHR Systems Among U.S. Hospitals and Physicians



Source: Office of the National Coordinator for Health Information Technology. "Office-based Physician Electronic Health Record Adoption." Health IT Quick-Stat, no.50. December 2016. Available at: https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php.
JaWanna Henry, Yuriy Pylypchuk, Talisha Searcy, and Vaishali Patel. "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015." ONC Data Brief, no.35. Office of the National Coordinator for Health Information Technology: Washington DC. May 2016.
Available at: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php.

There is growing recognition within the federal government of the unanticipated consequences of existing regulatory requirements on those who deliver care. In fact, a number of work streams are now underway within HHS to reduce burdens and advance regulatory reforms, reflecting the administration's goals of reducing red tape and compliance costs. Both ONC and CMS are convening efforts to identify and remove unnecessary regulatory burdens. ONC has already publicized its intention to enable developers to attest to meeting certain criteria without requiring external certification testing and to increasingly rely on private sector test methods and tools.[11,12,13,14]

HHS' focus on burden reduction and regulatory reform is well timed and has been well received among stakeholders. Reassessment and recalibration of the role of the federal government in overseeing health IT and digital health—including EHRs—should be a key component of HHS regulatory reform efforts.

Now that HITECH has achieved its primary goal of widespread adoption of EHRs by health care providers and increased digitization of health care, regulators should shift their focus to the more traditional role of assuring core "consumer" protections, while leaving to the market the evolution of products to meet the changing and customized needs of providers and their patients.

In the years since passage of HITECH, digital health has rapidly expanded as innovations in health IT have extended well beyond EHRs. These include transformative efforts in telehealth, artificial intelligence, and consumer and provider apps. Moreover, the data generated from digitization is driving further change. For example, data collected through health IT is being used to assess, manage and predict health outcomes of populations. Algorithms are harnessing data from multiple devices and technologies to inform clinical and patient decision-making.

Fundamentally, a regulatory model primarily organized around EHRs and incentives for their use no longer makes sense. Today's highly prescriptive, inflexible, EHR-centric regulatory approach stifles, rather than stimulates, innovation. Public policy needs to evolve and adapt to clinical and scientific breakthroughs, as well as to advancements in digital and analytical technologies and capabilities. Policy must continue to encourage discovery and innovation across the continuum of care, including public health.

Congress has already started the process. The bipartisan 21st Century Cures Act—enacted on December 13, 2016—clarifies regulatory authority associated with health IT and digital health by amending the Food, Drug and Cosmetic Act to exclude certain health software functions from the definition of "medical devices" that would be regulated by the Food and Drug Administration (FDA). Those excluded include functions used for administration, healthy lifestyle, patient records, low-risk clinical decision support, and basic information transfer. The 21st Century Cures Act also requires the HHS Secretary–in consultation with providers, health IT developers, and other stakeholders–to establish a goal and develop a strategy and recommendations for reducing regulatory or administrative burdens.

In response, the FDA is implementing its new Digital Health Innovation Plan, which transitions its evaluation approach for certain medical devices from one that is largely product-based to one that is developer-based.[15] As part of this approach, FDA enables private third-party certification of developer quality and other processes. And, as noted above, HHS has taken several steps to reduce burdens and advance regulatory reforms.

To inform and support the administration and Congress as they work to improve the development and use of health technology through regulatory reforms, Health IT Now and the Bipartisan Policy Center have convened a Work Group on the Future Role of Government in Health IT and Digital Health. This work group consists of more than 50 experts and stakeholders—from organizations representing clinicians, consumers and patients, hospitals and health systems, and technology companies—to assess the current regulatory landscape, identify the most pressing needs of technology users, and develop consensus recommendations on the future role of government in both a post-Meaningful Use era and a rapidly evolving delivery system and technology environment.

Over the course of a series of meetings in late 2017 and early 2018, the Work Group outlined key principles for, and attributes of, a new oversight framework for health IT and digital health; examined the current role of government; and formulated consensus recommendations for the ideal future role of the federal government in health IT and digital health. A summary of this work, along with our detailed recommendations is provided below.

Principles For An Oversight Framework

The goal of any oversight framework for health IT and digital health, as with the goal of health policy more generally, should be to improve health and health care, including making care more effective and efficient. In order to maximize innovation and responsiveness, the government's regulatory role within this framework should focus on core consumer protections and relate to the full range of digital health technologies, including, but not limited to, EHRs.

A core and shared belief is that the development and advancement of features and functions beyond core consumer protections should be left to the private sector. The federal government should also continue to play a role in non-regulatory functions, such as funding research to identify successful practices and adopting consensus standards within its own health IT to signal government support.

The work group identified the following key principles to guide the future oversight framework for health IT and digital health.

1

The oversight framework should encourage innovation.

This means that it should:

- Be flexible and able to evolve as the technology evolves;
- Be technologically neutral (i.e., not favor one technology approach over another);
- Avoid being overly prescriptive;
- Encourage good development processes, rather than requiring specific features and functions;
- Support minimally necessary standards and baseline protections; and
- Avoid creating unreasonable barriers to entry for developers (small and large).

2

The oversight framework should be risk-based.

This means that oversight policies—including those carried out by the federal government—should be based on the risk of harm to patients.

3

The oversight framework should be stable and predictable.

This means that any changes to the framework must be understandable by affected parties; implemented with sufficient notice and lead time; and not create or add to uncertainties among providers, developers, and individuals.

4

The oversight framework should be accountable to the public and enforceable.

This means that its contents should be developed with considerable stakeholder input and its performance measured and made transparent. Those aspects of the framework that fall under the responsibility of the federal government and impose specific obligations on particular parties should be enforced.

5

The oversight framework should reflect the principles of a learning health system.

This means that the framework should undergo continuous improvement and innovation, with best practices seamlessly embedded as new knowledge is captured through experience.[16]

Desired Technology Outcomes

The oversight framework should promote technology that supports high quality, safe, patient-centered care and the quadruple aim of improving population health, increasing patient satisfaction, reducing per-capita health care spending, and enhancing clinician and staff satisfaction.

The oversight framework should address the following six technology outcomes:

1

Interoperability

Technology should facilitate interoperability and information sharing, which play a critical role—along with other technology outcomes—in advancing higher quality, more cost-effective, patient-centered care.

2

Usability

Technology should reflect evidence-based, user-centered design principles; human factors science; and best practices. It should not create unnecessary burden on end users. It should also be culturally competent, enabling access by users with diverse languages and abilities.

3

Safety

Technology should not create patient harm. Instead, it should help reduce patient harm by supporting the delivery of safer care.

4 Security

Technology should assure that information is available and accessible only to authorized individuals and processes and also provide assurance that information is not altered or destroyed in an unauthorized manner.

5 Patient Access to Information

Technology should enable and not create barriers to patients' access to their own health information.

6 Support for an Evolving Health Care System

Technology should be adaptable and flexible enough to meet the changing needs of users and an evolving health care system.

A more detailed analysis of each of these technology outcomes, including both current and recommended future roles for government, is provided below.

Recommendations for the Future Role Of Government

The following summarizes the Work Group's recommendations for an oversight framework for health IT and digital health, grounded in the principles and technology outcomes described above.

AN OVERVIEW

In summary, the federal government's future role in health IT and digital health across all six technology outcomes should focus on the four following functions.

1

Provide assurance that core consumer protections are met.

The federal government should carry out its traditional role of assuring core consumer protections. Any other regulatory activities should be transitioned to private sector accreditation, certification, recognition, and/or standards bodies or—if appropriate—eliminated.

2

Recognize standards and promote their adoption.

The federal government should recognize private sector consensus standards, adopt such standards within federal programs, utilize market-sensitive policy levers—such as incentives, rather than technology mandates or penalties—to promote their adoption and use, and support adoption through educational efforts.

3

Convene experts and stakeholders.

The federal government should continue to serve in the role of convener, by bringing together stakeholders and experts to identify health IT and digital health-related issues that need to be addressed and strategies to address those challenges.

4

Fund research and development activities.

The federal government should invest in research and development activities designed to assess the current state of the field, define key challenges, and identify best practices and other solutions.

Transitioning to this future state will require the following:

1. HHS' continued implementation of 21st Century Cures Act provisions which clarify the boundary between FDA-regulated and non-regulated health technology, including FDA's implementation of regulations related to digital health, which support consumer protections related to higher risk software that have the potential of causing patient harm.[17,18,19]

2. Continued enforcement of existing laws and regulations that create level playing fields and fair markets, including those overseen by the Federal Trade Commission, the HHS Office of Civil Rights (OCR), the HHS Office of the Inspector General (OIG), the Federal Communications Commission (FCC), and other agencies that focus on specific issue areas related to fair commercial practices, security and privacy, and interoperability/information blocking.

3. Changes and reduction in scope of the ONC Health IT Certification Program, which would involve narrowing its focus to core consumer protections, and transitioning other requirements to private sector efforts.

4. The Agency of Healthcare Research and Quality's (AHRQ's) rapid implementation of 21st Century Cures Act provisions to support software developer reporting to patient safety organizations (PSOs) and participation in patient safety activities.[20]

5. Reduction of prescriptive technology and burdensome reporting requirements contained in CMS quality improvement, payment, and delivery system reform programs.

Detailed analyses of the current role of government and recommendations for its future role—associated with each of the six technology outcomes—are provided below.

INTEROPERABILITY

There are various definitions of interoperability, with a common theme of data liquidity resulting from: (1) secure exchange and use of electronic health information without special effort of the user; (2) complete access, exchange, and use of all electronically accessible health information for authorized use; and (3) no information blocking.[21] Although much of the federal effort regarding interoperability has focused on EHRs, there is clear federal and private sector recognition that interoperability must span the range of health IT and the care continuum.[22]

Although the federal government has taken many steps to increase interoperability, to date there has been only limited progress. Key consensus themes regarding needed actions include the following:

- Reliance on private-sector leadership and standards;

- Robust testing;
- Attention to both provider-provider and provider-patient interoperability;
- Coordination across federal programs;
- Measurement of interoperability levels and progress;
- The need for strong business cases to drive further interoperability progress; and
- Effective federal enforcement of laws and regulations regarding both patients' right of access to their data and prevention of information blocking.

Current Role of Federal Government Related to Interoperability

ONC has primary responsibility for health IT interoperability initiatives, along with CMS. In addition, the HHS OIG plays a role in enforcement of compliance with information blocking prohibitions, and Congress has required that the General Accountability Office (GAO) issue a report on accurate patient matching, an important factor in achieving effective interoperability. Federal agency responsibilities are summarized below.

Interoperability requirements are currently contained in the ONC 2015 Edition Certification Criteria (e.g., Direct Project-related, Common Clinical Data Set, IHE profiles) under the ONC Health IT Certification Program.[23] In addition, ONC maintains an online Interoperability Standards Advisory (ISA) that is intended to "coordinate the identification, assessment, and public awareness of interoperability standards and implementation specifications that can be used by the healthcare industry to address specific interoperability needs..."[24] CMS also includes interoperability and information blocking requirements within the Medicare and Medicaid EHR Incentive Programs, as well as MIPS.[25,26]

The Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) contained provisions related to interoperability, including a requirement that HHS achieve a national objective of widespread exchange of health information through interoperable certified EHR technology by December 2018.[27] The Act also specifies that if such widespread exchange is not achieved by December 2018, HHS must submit a report highlighting barriers to this goal and outlining federal plans to achieve the objective by December 2019.[28] Both ONC and the National Quality Forum (NQF) have developed interoperability measurement frameworks that can help track progress against this objective.[29,30]

The 21st Century Cures Act also contains several provisions related to interoperability, including requiring ONC to perform the following:[31]

- By December 2017, require that health IT developers or entities, as a condition of certification: (1) publish API and allow health information from such technology to be accessed, exchanged and used without special effort and (2) have successfully tested the real-world use of the technology for interoperability;
- By December 2017, convene stakeholders to develop reporting criteria, including measures related to interoperability, for which data collection and reporting actions will be taken by an independent body;
- Work with OCR to issue a rulemaking on "reasonable and necessary" exceptions to the information blocking prohibition;
- Implement a process for public submission of claims regarding lack of interoperability or information blocking; and
- Develop a Trusted Exchange Framework and Common Agreement (TEFCA) and rules for its use. ONC released the draft TEFCA in January 2018 for public comment.

The 21st Century Cures Act also requires the HHS OIG to carry out enforcement activities related to information blocking and tasks GAO with conducting a study to review policies and activities of ONC and other stakeholders to ensure appropriate patient matching and survey ongoing efforts to assess effectiveness.[32]

Recommendations for Future Government Role Related to Interoperability

1. To enhance interoperability progress, the federal government should design payment and delivery models, including value-based fee-for-service and alternative payment models, in ways that create a strong business case and clear signals for stakeholders to engage in interoperability and information exchange.

2. The federal government should recognize private sector consensus standards for interoperability, addressing such areas as data content, data transport, vocabulary/coding, and APIs, after careful review for maturity, suitability, implementability, market readiness and acceptance, and usability.

3. The federal government should adopt recognized private sector consensus standards in its own software (self-developed, commissioned, or commercial off-the-shelf software) related to care delivery (e.g., at the Department of Defense and the Department of Veterans Affairs).

4. The federal government should participate in and support private sector standards development, encouraging patient and consumer engagement and perspectives in such efforts.

5. The federal government should seek to harmonize interoperability definitions, policies, and requirements across federal agencies and programs.

6. The federal government should encourage enhanced private sector interoperability testing and improved testing tools.

7. The federal government should use its existing authority, including that provided under MACRA and the 21st Century Cures Act, to ensure that information flows freely, without information blocking. As part of this work, applicable federal agencies, including the OIG, CMS, and ONC should enforce 21st Century Cures information blocking provisions, addressing both provider and patient access to information, with enforcement, prosecutions and penalties that are fact-based and proportionate and with HHS providing clear rules of the road for providers, exchanges and networks, and developers.

8. Consistent with 21st Century Cures Act requirements, the federal government should measure the extent of and progress on interoperability across the care continuum, using valid and reliable private sector-developed consensus measures that involve minimal burdens for providers and developers.

9. The federal government should recognize and incentivize the adoption of standards designed to improve matching of patient data across systems, which is a critical element of effective interoperability.

10. Implementation of ONC interoperability-related authority should encourage data portability to enable greater competition and substitutability of health IT by end-users. This will enable users to exercise informed choice around product capabilities and usability. As part of this focus on data portability, the federal government should encourage private sector adoption of minimum data portability standards.

USABILITY

The term “usability” refers to “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.”[33]

The federal government has engaged in various efforts to evaluate and enhance the usability of health IT, with mixed results. There is a consensus across the federal government and the private sector that the usability of health IT should be enhanced, that government programs – in some cases – have had a negative impact on usability and provider burden, and that the federal government’s role in this area in the future should be more focused, emphasizing reduction of provider burden and greater reliance on private sector efforts to enhance health IT usability. During a recent hearing of the Senate Health, Education, Labor, and Pensions Committee, ONC leadership stated that usability was one of its two main priorities – along with interoperability.[34]

Current Role of Federal Government Related to Usability

ONC and the National Institute of Standards and Technology (NIST) are the two federal agencies that focus on usability of both health IT and digital health.

Limited requirements related to usability are contained in the 2015 Edition Certification Criteria of the ONC Health IT Certification Program, specifically with regard to identifying and submitting information about user-centered design processes, and assuring that a minimum number of individuals participate in summative usability testing.[35]

The 21st Century Cures Act contained provisions related to usability, requiring that by December 2017, ONC must:[36]

- Require that health IT developers or entities, as a condition of certification, do not prohibit or restrict communication by users or other parties regarding usability or users' experiences when using the health IT; and

- Convene stakeholders to develop EHR reporting criteria through a public, transparent process to focus on measuring EHR performance and to include measures on security, usability, user-centered design, interoperability, and conformance to certification testing. It should be noted that during the October 31, 2017 Senate HELP Committee hearing, ONC leadership indicated that it did not have appropriated funding for this activity.[37]

NIST has developed several best-practices and tools to support usability. The agency is establishing a framework in collaboration with AHRQ and ONC that defines and assesses health IT usability. The goal is to create a detailed specification of an objective, repeatable procedure for measuring and evaluating the usability of health IT systems.[38]

Recommendations for Future Government Role Related to Usability

1. CMS and ONC should continue to reexamine current health IT regulatory requirements (especially those related to Medicare and Medicaid) and reduce or eliminate those provisions that increase provider burdens or hinder usability. The agencies also should continue to work to moderate the pace of policy change to enable providers, health IT developers, and other stakeholders the time to absorb and implement changes.

2. Assessments of usability of software products should occur within the private sector, informed by best practices in user centered design, evidence, and research. Such assessments should involve users, usability experts, standards development organizations, developers, and others, and inform efforts to create more equal bargaining power between developers of technology and their purchasers.

3. ONC should limit its role in usability to both convening and supporting the development and dissemination of standards and best practices, including those that enhance health IT usability and reduce provider burden.

4. NIST should continue to recognize and support the development and dissemination of usability design standards, principles and best practices.

SAFETY

Health IT-specific patient safety goals cover three fundamental domains: health IT that is safe; safe use of health IT; and finally, actually using health IT to improve patient safety.[39]

Consistent with 21st Century Cures provisions, the primary federal government responsibility for regulating higher risk health IT and digital health lies with the FDA, which retains authority to regulate a specified subset of high-risk health IT functions. In addition, other federal agencies have limited and targeted responsibility as well, such as AHRQ and ONC. Coordinated efforts to address the safety of non-FDA-regulated health IT should lie with the private sector, with a focus on coordination, standards, process certification, and transparency.

Current Role of Federal Government Related to Safety

ONC, FDA, and AHRQ are the primary agencies with current responsibilities related to safety for health IT and digital health.

ONC's current safety-related activities are fairly limited:

- Limited and focused safety-related requirements are contained in 2015 Edition Certification Criteria for Safety-Enhanced Design under the ONC Health IT Certification Program, including a requirement that health IT developers identify the quality management system used to develop, test, implement, and maintain capabilities of certified health IT.[40]

- ONC has also issued the SAFER Guides and other health IT safety resources and funded development work for a health IT safety collaborative.[41]

- Finally, ONC has established a direct certification oversight role to address safety and other issues.[42]

FDA has a long-established medical device notification and approval process. The agency issues regulation and guidance, including notices of enforcement discretion, related to health IT that it considers a medical device.

The 21st Century Cures Act identifies certain types of health IT that are not subject to regulation by FDA because they are not defined as a medical device. The act also includes provisions that could shift non-regulated product functions into the regulated category based on the risk of these functions (the so-called "claw back" authority). The FDA issued initial guidance on December 8, 2017, describing its intended approach.[43] Within regulated health IT, the FDA is developing new approaches, such as the Digital Health Software Precertification Program, focusing on certification of process vs. product as part of its Digital Health Innovation Action Plan.[44,45] In a blog post announcing this FDA action plan, FDA Commissioner Scott Gottlieb emphasized that "FDA will help innovators navigate a new, modern regulatory process so that promising, safe and effective developments in digital health can advance more quickly and responsibly, and Americans can reap the full benefits from these innovations."[46]

AHRQ, along with OCR, implements the Patient Safety and Quality Improvement Act and its use of PSOs as a patient safety tool.[47] The 21st Century Cures Act requires AHRQ to extend to developers the same protections available to providers who work with PSOs.[48]

Recommendations for Future Government Role Related to Safety

1. The FDA should continue its risk-based regulation of high-risk software as reflected in guidance issued December 7, 2017, which – as authorized by the 21st Century Cures Act – can re-regulate non-regulated functions if risk is assessed to be high.

2. The FDA should expeditiously implement and evaluate its new approach to focus on health IT development processes rather than products.

3. Evaluation or certification of software outside of FDA jurisdiction (which continues to apply to health IT classified as a medical device), should largely transition to independent evaluation or certification bodies in the private sector.

4. ONC, AHRQ, and other federal agencies should support and participate in private sector priority-setting and coordination efforts (e.g., a health IT safety center), as well as private sector development of both process and risk management standards, tools, and best practices.

5. AHRQ should expeditiously implement the provisions of the 21st Century Cures Act to facilitate developer participation in and safety event reporting through PSOs. PSO participation would enable methods and approaches for appropriate investigation of safety events or risks in a protected space.

SECURITY

From the standpoint of patients, consumers and providers, both privacy and health IT security are of great importance, and the HIPAA law authorizes regulations and guidelines that address both concepts. The framework, however, focuses specifically on security, which is most relevant to technology oversight and is a critical enabler of privacy.

Consistent with HIPAA, health IT security has three elements:[49]

- Confidentiality – Electronic protected health information (ePHI) is accessible only by authorized people and processes;
- Integrity – ePHI is not altered or destroyed in an unauthorized manner; and
- Availability – ePHI can be accessed as needed by an authorized person.

The federal government has played an important and active role in advancing health IT security in many ways, through legal, technical, product certification, and provider-level requirements.

Recent cybersecurity threats have underscored the importance of health IT security to safe and effective use of interoperable health IT. Both the federal government and the private sector have important roles to play in this task.

Current Role of Federal Government Related to Security

ONC, CMS, FDA, OCR, and NIST are the federal agencies that currently carry out security-related activities in health care. In addition, the HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) oversees HHS cybersecurity activities in coordination with the HHS Office of the Chief Information Officer. For example, ASPR houses the HCCIC, which is responsible for information sharing and alerting the industry on cybersecurity vulnerabilities. The federal government also has a broader cybersecurity focus, inclusive of health care, most notably through the Department of Homeland Security.[50]

Privacy and security requirements are contained in ONC's 2015 Edition Certification Criteria, including those focused on authentication, access control and authorization, auditable events and tamper-resistance, audit reports, amendments to PHI, automatic access time-out, emergency access, end-user device encryption, integrity, trusted connection, auditing actions on health information, and accounting of disclosures.[51]

ONC also has developed and made available various security resources and in January 2018, appointed a new Chief Privacy Officer.

CMS, through both the Quality Payment Program and its Medicare and Medicaid EHR Incentive Programs, require provider attestation to having completed a HIPAA security risk assessment. [52,53]

Further, FDA has identified health IT-relevant security standards.[54]

Additionally, OCR's HIPAA Security Requirements create obligations for Covered Entities and Business Associates.[55]

Finally, NIST has identified a variety of general and health IT-relevant security standards. [56]

Recommendations for Future Government Role Related to Security

1. The federal government should continue to identify and advance health IT security standards and best practices, leveraging the work of the private sector.
2. The federal government should facilitate information sharing about security threats and security readiness broadly within the health care sector (between and among public and private sector organizations), through collaboration with HHS, the FBI, the Department of Homeland Security, and private sector organizations like the National Health Information Sharing and Analysis Center (NH-ISAC).[57]
3. HHS should provide technical assistance to provider and developer organizations to ensure that they can utilize available government and private sector resources.
4. OCR should reduce and remove – where possible – ambiguities in how the HIPAA Security rule should be applied and also simplify how it is explained, so that consumers are better informed of their rights and data holders have more confidence in what they should be doing, with enforcement taking into account the data holder's use of best practices.

5. Assessments of the security of software products should occur within the private sector in the context of the overall responsibilities set out by HIPAA and other security-related laws and regulations but going beyond these laws and regulations as needed to reflect consensus standards and best practices.

6. As a best practice, health IT developers and vendors should—consistent with developer and customer obligations under the HIPAA Security and Privacy Rules and applicable contractual terms and customary commercial and contractual practices—engage in transparent discourse with clients and prospects about relevant security-related product and service information, such as patching policies, relied-upon software, and completion of private sector third party security audits, where appropriate, and when revealing such information will not increase security risks or run contrary to applicable laws or regulations.

PATIENT ACCESS TO THEIR HEALTH INFORMATION

Patients and their families or care givers should have access to relevant, usable clinical information directly, via apps and similar technology. Such information facilitates patient decision-making and self-care and can also be made available to providers and other patient-designated information recipients. Patient access to such information is a priority interoperability use case that is unique in that it is also grounded in a fundamental HIPAA-designated patient right of access to their health information. Emerging technologies (e.g., APIs and apps) and recent legislation and regulations (e.g., MACRA and the 21st Century Cures Act) are likely to significantly increase the scope and value of patients' access to their electronic health information.

ONC, OCR, and CMS are the primary agencies with responsibilities related to patients' access to their own health information.

ONC's 2015 Edition Certification Criteria include requirements for capabilities associated with viewing, downloading, and transmitting data to a third party, as well as APIs.[58] CMS also includes requirements associated with view, download, and transmit, as well as API access within the Medicare and Medicaid EHR Incentive Programs and MIPS.[59,60] Under OCR, HIPAA right of access regulations address and define patient and consumer rights to electronic data.[61]

Recommendations for Future Government Role Related to Patient Access to Information

1. The federal government should facilitate patients' access to their health data as a priority goal.

2. Consistent with 21st Century Cures Act provisions, ONC should expand the standardized data elements available to patients and their designated individuals and entities, approaching the availability of the "all data" requirement in a step-wise, steady, and practical fashion, with a priority focus on data that is of value to and usable by patients (e.g., relevant and no more extensive than necessary), to facilitate shared decision-making.[62]

3. OCR and CMS should focus on education about and enforcement of patients' rights of access in the context of evolving technology solutions, such as APIs and 21st Century Cures Act provisions.

4. OCR should track, measure, and report on patient complaints relating to their right of access to their health data, including the status of such complaints and their resolution by OCR.

5. The GAO study on patient data access, required by the 21st Century Cures Act, should be prioritized over the near-term, with a focus on identifying barriers and opportunities across the data distribution chain.

SUPPORT FOR AN EVOLVING HEALTH CARE SYSTEM

Health IT and digital health can facilitate access to the data needed by value-based and other delivery and payment models, and also can provide tools that providers, payers, and innovative programs like accountable care organizations (ACOs) need to meet their goals. To this end, health IT and digital health can enable federal and state payment, incentive, and care delivery programs to meet the needs of program sponsors and participants.

To date, use of health IT has been a central aspect of federal, state, and private sector value-based delivery and payment models, but in some instances, in a very prescriptive manner.

Going forward, the role of government should be to encourage robust business cases for stakeholders to use health IT and engage in information exchange rather than impose prescriptive technology-related requirements. Such detailed technology requirements, in addition to hindering flexibility and innovation, can be a barrier for participation in value-based models for smaller provider and payer organizations, especially in models that penalize providers for relatively small technology-based compliance gaps.

Current Role of Federal Government Related to Health IT Supporting an Evolving Health Care System

CMS requires the use of certified EHR technology (CEHRT) for most government value-based and incentive programs (e.g., QPP/MIPS/APM, Meaningful Use, MSSP, other ACO programs, CPC+, etc.).[63,64]

Congress and HHS have established or implied a clear relationship between certification and the ability for health IT to support Meaningful Use, MIPS, and to an extent, other QPP alternative payment model (APM) programs, including CPC+. The ONC Health IT Certification program is designed to reflect such a role. At the same time, CMS has decided not to specify what health IT to use for most QPP programs or to pursue program-specific certification, an option that had been raised in prior rulemaking discussions. There is no concrete requirement that HIT be tied to successful results in government programs, and certification has not translated clearly to provider success in improving patient outcomes and reducing the cost of care.

Recommendations for Future Government Role Related to Health IT Supporting an Evolving Health Care System

1. The federal government should design payment and delivery models, drawing on applicable private sector lessons learned and best practices, in ways that create a strong business case and clear signals for stakeholders to use health IT and digital health, rather than prescriptive technology possession or use requirements that can hinder flexibility, innovation, and participation in value-based models by smaller provider and payer organizations.

2. Future EHR Incentive and QPP program changes should not require providers to undertake technology-dependent activities that do not align with applicable vendor capabilities

3. The federal government should ensure that those to whom it delegates authority or responsibility are aligned with this non-prescriptive approach.

4. The federal government should use appropriate policy analysis and research methods to evaluate the role of health IT in its innovative payment and delivery models consistent with a commitment to a learning health system.

Conclusion

Many challenges remain in health IT and digital health development, implementation, and use, and there is a strong desire from both stakeholders and policymakers to address these challenges. One area of emerging consensus is that the regulatory framework should be an enabler of the private sector, rather than stand in the way of the market. Health IT Now and the Bipartisan Policy Center convened the Work Group of the Future Role of Government in Health IT and Digital Health to explore these core challenges and unearth the barriers to a more efficient and effective government role. Outdated regulatory frameworks and requirements will limit the ability of health IT and digital health to facilitate advances in innovation. The current system is out of date and falls further behind with each passing day.

Congress and the administration have an excellent opportunity to build a better system that fosters a free market, with competition and incentives that produce innovative tools that ultimately help providers and patients deliver and receive high-quality, efficient, and effective care.

Nearly 10 years after the passage of the HITECH Act, the time is now to update the course of federal health IT policy. We encourage Congress, the administration, and the private sector, to take up this challenge and meet this opportunity.

APPENDIX A: WORK GROUP MEMBERS

BPC and Health IT Now would like to thank and acknowledge the following Work Group members who contributed their time and expertise to the development of this report.

Peter Basch, MD
MedStar Health

Peggy Binzer
Alliance for Quality Improvement and Patient Safety

Meryl Bloomrosen
Premier, Inc.

Claire Brandewie
McKesson

Jasey Cardenas
United Spinal Association

Greg Carey
athenahealth

Amy Colberg
Brain Injury Association of America

John Michael DeCarlo
IBM

Josh Emperado
Agfa HealthCare

David Fairbrothers
Dorsata

Federation of American Hospitals

Eli Fleet
HIMSS

David Fuhrmann
Epic

Joe Ganley
McKesson

Elisabeth George
Philips

Tina Grande
Healthcare Leadership Council

John Halamka, MD
Beth Israel Deaconess
Harvard Medical School

Barbara Hobbs
MEDITECH

Cherie Holmes Henry
NextGen Healthcare

Lindsay Jager
Cerner

Jim Jirjis, MD, MBA, FACP
HCA Healthcare

Leslie Krigstein
CHIME

Tom Leary
HIMSS

Janet Marchibroda
Bipartisan Policy Center

Joshua Marker
Evidation Health

Meg Marshall
Cerner

Brooke Nepo
Healthcare Leadership Council

Jessica Peterson, MD, MPH
American Academy of Opthamology

Elridge Proctor
Lung Cancer Alliance

Catherine Pugh
Health IT Now

Lucia Savage
Omada Health

Mari Savickis
CHIME

Hoda Sayed-Friel
MEDITECH

Chris Schleicher
athenahealth

Mark Segal
for Bipartisan Policy Center

Jeff Smith
American Medical Informatics Association (AMIA)

Ronni Solomon
ECRI Institute

Andrew Sperling
National Alliance on Mental Illness

Sarah Swank
Dignity Health

Tim Swope
Bipartisan Policy Center

James Turner
Health IT Now

Yelena Vaynberg
IBM

Steven Waldren, MD
American Academy of Family Physicians

Joel White
Health IT Now

Adam Whitlatch
Epic

John Wylam
National MS Society

Stephanie Zaremba
athenahealth

Several other individuals representing clinicians, health systems, and patient organizations participated in the Work Group's efforts but are not listed here.

Endnotes

[1] Centers for Medicare and Medicaid Services. “December 2017 EHR Incentive Program.” December 2017.
Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/December2017_SummaryReport.pdf.

[2] Office of the National Coordinator for Health Information Technology. “Office-based Physician Electronic Health Record Adoption.” *Health IT Quick-Stat, no.50*. December 2016. Available at: https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php.

[3] JaWanna Henry, Yuriy Pylypchuk, Talisha Searcy, and Vaishali Patel. “Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015.” *ONC Data Brief, no.35*. Office of the National Coordinator for Health Information Technology: Washington DC. May 2016.
Available at: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php.

[4] Federal Register. “2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange.” *Health and Human Services Department*. September 11, 2014. Available at: https://www.federalregister.gov/documents/2014/09/11/2014-21633/2014-edition-release-2-electronic-health-record-ehr-certification-criteria-and-the-onc-hit.

[5] Brian Arndt, John Beasley, Michelle Watkinson, Jonathan Temte, Wen-Jan Tuan, Christine Sinsky, and Valerie Gilchrist,. “Tethered to the EHR: Primary Care Physician Workload Assessment Using EHR Event Log Data and Time-Motion Observations.” *Annals of Family Medicine*. September/October 2017.
Available at: http://www.annfammed.org/content/15/5/419.full.

[6] Robert Hill, Lynn MarieSears, and Scott Melanson. “4000 Clicks: a productivity analysis of electronic medical records in a community hospital ED.” *The American Journal of Emergency Medicine*. November 2013. Available at: https://www.sciencedirect.com/science/article/pii/S0735675713004051.

[7] Lawrence Casalino, David Gans, Rachel Weber, et. al. “US Physician Practices Spend More Than $15.4 Billion Annually To Report Quality Measures.” *Health Affairs*. 35 (3). March 2016. Available at: https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2015.1258.

[8] AmericanEHR and the American Medical Association. “Physicians Use of EHR Systems 2014.” 2014.
Available at: http://www.americanehr.com/research/reports/Physicians-Use-of-EHR-Systems-2014.aspx.

[9] Tait Shanafelt Omar Hasan, Lotte Dyrbye, et al. “Changes in Burnout and Satisfaction with Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014.” Mayo Clinical Proceedings 90 (12): 1600-1613. 2015.
Available at: http://www.mayoclinicproceedings.org/article/S0025-6196(15)00716-8/fulltext.

[10] Thomson Kuhn, Peter Basch, Michael Barr, Thomas Yackel. “Clinical Documentation in the 21st Century: Executive Summary of a Policy Position Paper From the American College of Physicians.” *Annals of Internal Medicine*. February 17, 2015.
Available at: http://annals.org/aim/fullarticle/2089368/clinical-documentation-21st-century-executive-summary-policy-position-paper-from.

[11] The Office of the National Coordinator for Health Information Technology. “Self-Declaration Approach Program Guidance #17-04.” November 22, 2017.
Available at: https://www.healthit.gov/sites/default/files/policy/selfdeclarationapproachprogramguidance17-04.pdf.

[12] Steven Posnack. “A 5-year Goal to Transition the ONC Health IT Certification Program’s Testing Portfolio.” *Health IT Buzz*. August 3, 2017.
Available at: https://www.healthit.gov/buzz-blog/healthit-certification/5-year-goal-transition-onc-health-certification-programs-testing-portfolio/.

[13] Elise Sweeney Anthony and Steven Posnack. “Certification Program Updates to Support Efficiency & Reduce Burden.” *Health IT Buzz*. September 21, 2017.
Available at: https://www.healthit.gov/buzz-blog/healthit-certification/certification-program-updates-support-efficiency-reduce-burden/.

[14] Steven Posnack. “The ONC Health IT Certification Program Approves the HIMSS-Immunization Integration Program (IIP) Testing Method.” October 17, 2017.
Available at:
https://www.healthit.gov/buzz-blog/interoperability/onc-health-certification-program-approves-himssimmunization-integration-program-iip-testing-method/.

[15] Food and Drug Administration. “Digital Health Innovation Action Plan.” 2017.
Available at: https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf.

[16] National Academy of Medicine. “Best Care at Lower Cost: The Path to Continuously Learning Health Care in America.” 2012. Available at:
http://www.nationalacademies.org/hmd/Reports/2012/Best-Care-at-Lower-Cost-The-Path-to-Continuously-Learning-Health-Care-in-America.aspx.

[17] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[18] Food and Drug Administration. “Digital Health Software Precertification (Pre-Cert) Program.” 2017.
Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/default.htm.

[19] Food and Drug Administration. “Digital Health Innovation Action Plan.” 2017.
Available at: https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf.

[20] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[21] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf. The Cures Act defines interoperability as follows: INTEROPERABILITY.—The term ‘interoperability’, with respect to health information technology, means such health information technology that—‘‘(A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; ‘‘(B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and ‘‘(C) does not constitute information blocking as defined in section 3022(a).’’

[22] Office of the National Coordinator for Health IT. “Draft Trusted Exchange Framework.” January 5, 2018.
Available at: https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.

[23] Federal Register. “2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base.

[24] The Office of the National Coordinator for Health Information Technology. “2018 Interoperability Standards Advisory.” December 2017.
Available at: https://www.healthit.gov/isa/sites/default/files/2018%20ISA%20Reference%20Edition.pdf.

[25] Centers for Medicare and Medicaid Services. “Quality Payment Program.” Available at: https://qpp.cms.gov/.

[26] Centers for Medicare and Medicaid Services. “Electronic Health Records (EHR) Incentive Programs.”
Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.

[27] Public Law 114-10 (2015). The Medicare Access and CHIP Reauthorization Act of 2015.
Available at: https://www.congress.gov/bill/114th-congress/house-bill/2/text.

[28] Public Law 114-10 (2015). The Medicare Access and CHIP Reauthorization Act of 2015.
Available at: https://www.congress.gov/bill/114th-congress/house-bill/2/text.

[29] The Office of the National Coordinator for Health Information Technology. “Proposed Interoperability Standards Measurement Framework.” April 2017.
Available at: https://www.healthit.gov/sites/default/files/ONCProposedIOStandardsMeasFrameworkREV.pdf.

[30] National Quality Forum. “Interoperability 2016-2017 Final Report.” September 2017.
Available at: http://www.qualityforum.org/Publications/2017/09/Interoperability_2016-2017_Final_Report.aspx.

[31] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[32] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[33] National Institute of Standards and Technology. “Health IT Usability.” 2017. Available at: https://www.nist.gov/programs-projects/health-it-usability.

[34] Senate Health, Education, Labor and Pensions Committee. “Full Committee Hearing: Implementation of the 21st Century Cures Act: Achieving the Promise of Health Information Technology.” October 31, 2017.
Available at: https://www.help.senate.gov/hearings/implementation-of-the-21st-century-cures-act-achieving-the-promise-of-health-information-technology.

[35] Federal Register. “2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base.

[36] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[37] Senate Health, Education, Labor and Pensions Committee. “Full Committee Hearing: Implementation of the 21st Century Cures Act: Achieving the Promise of Health Information Technology.” October 31, 2017.
Available at: https://www.help.senate.gov/hearings/implementation-of-the-21st-century-cures-act-achieving-the-promise-of-health-information-technology.

[38] National Institute of Standards and Technology. “Health IT Usability.” 2017. Available at: https://www.nist.gov/programs-projects/health-it-usability.

[39] Hardeep Singh, Dean Sittig. “Measuring and improving patient safety through health information technology: The Health IT Safety Framework.” *BMJ Quality & Safety*. 25(4): 226-232. 2015. Available at: http://qualitysafety.bmj.com/content/qhc/25/4/226.full.pdf.

[40] Federal Register. “2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base.

[41] Office of the National Coordinator for Health Information Technology. “SAFER Guides.” 2017. Available at: https://www.healthit.gov/safer/safer-guides.

[42] Federal Register. “ONC Health IT Certification Program: Enhanced Oversight and Accountability.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2016/10/19/2016-24908/onc-health-it-certification-program-enhanced-oversight-and-accountability.

[43] Food and Drug Administration. “Guidances with Digital Health Content.” 2018. Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm.

[44] Food and Drug Administration. “Digital Health Software Precertification (Pre-Cert) Program.” 2017. Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/default.htm.

[45] Food and Drug Administration. “Digital Health Innovation Action Plan.” 2017. Available at: https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf.

[46] Scott Gottlieb. “Fostering Medical Innovation: A Plan for Digital Health Devices.” June 15, 2017. Available at: https://blogs.fda.gov/fdavoice/index.php/2017/06/fostering-medical-innovation-a-plan-for-digital-health-devices/.

[47] Agency for Healthcare Research and Quality. “Patient Safety and Quality Improvement Act of 2005.” Available at: https://pso.ahrq.gov/legislation/act.

[48] Public Law 114-255 (2016). 21st Century Cures Act. Available at: https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[49] Department of Health and Human Services. “Security 101 for Covered Entities.” 2007. Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es.

[50] See for example the Health Care Industry Cybersecurity Task Force Report. June 2017. Available at: https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx.

[51] Federal Register. “2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base.

[52] Centers for Medicare and Medicaid Services. “Quality Payment Program.” Available at: https://qpp.cms.gov/.

[53] Centers for Medicare and Medicaid Services. “Electronic Health Records (EHR) Incentive Programs.” Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.

[54] Food and Drug Administration. “Cybersecurity.” 2017. Available at: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

[55] Department of Health and Human Services. “Security 101 for Covered Entities.” 2007. Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es.

[56] National Institute of Standards and Technology. “Security - Health Information Technology.” 2017. Available at: https://www.nist.gov/programs-projects/security-health-information-technology.

[57] National Health Information Sharing and Analysis Center (NH-ISAC). Available at: https://nhisac.org/.

[58] Federal Register. “2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications.” *Health and Human Services Department*. October 16, 2015. Available at: https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base.

[59] Centers for Medicare and Medicaid Services. “Quality Payment Program.” Available at: https://qpp.cms.gov/.

[60] Centers for Medicare and Medicaid Services. “Electronic Health Records (EHR) Incentive Programs.” Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.

[61] Department of Health and Human Services. “Your Rights Under HIPAA.” 2017. Available at: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

[62] The Office of the National Coordinator for Health Information Technology. “Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process.” January 5, 2018. Available at: https://www.healthit.gov/sites/default/files/draft-uscdi.pdf.

[63] Centers for Medicare and Medicaid Services. "Quality Payment Program." Available at: https://qpp.cms.gov/.

[64] Centers for Medicare and Medicaid Services. "Electronic Health Records (EHR) Incentive Programs." Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.

Notes

BIPARTISAN POLICY CENTER

The Bipartisan Policy Center is a non-profit organization that combines the best ideas from both parties to promote health, security, and opportunity for all Americans. BPC drives principled and politically viable policy solutions through the power of rigorous analysis, painstaking negotiation, and aggressive advocacy.

bipartisanpolicy.org | 202-204-2400
1225 Eye Street NW, Suite 1000
Washington, D.C. 20005

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan

healthITnow

Health IT Now is a broad-based coalition focused on improving the U.S. healthcare system through data and health information technology. As the premier health IT advocacy organization in Washington, DC, Health IT Now is on the front lines of the fight to increase access to technology-enabled care, promote interoperability across the healthcare continuum, reduce federal regulatory burden, and engineer a data-driven response to the opioid crisis.

healthitnow.org | 202-643-8645
440 First Street NW, Suite 430
Washington, D.C. 20001

healthITnow

440 First Street NW, Suite 430
Washington, D.C. 20001
202-643-8645 | healthitnow.org

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, D.C. 20005
202-204-2400 | bipartisanpolicy.org