The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

Health IT Advisory Committee

January 18, 2018

The Office of the National Coordinator for Health Information Technology

Overview of 21st Century Cures Act and Office of Policy Updates

Elise Sweeney Anthony, Director of Policy
Office of the National Coordinator for Health IT

January 18, 2018

Understanding Certified Health IT Interactive PDFs

- ONC has created an interactive PDF for better understanding certified health IT and how it supports clinicians in providing care
- User-friendly tool to learn about certification requirements in plain terms
- The interactive PDF covers the eight certification criteria categories:
  - Clinical Processes
  - Care Coordination
  - Clinical Quality Measurement
  - Privacy and Security
  - Patient Engagement
  - Public Health
  - Health IT Design & Performance
  - Electronic Exchange

Understanding Certified Health IT Interactive PDFs

- ONC also created supplemental interactive PDFs highlighting certification criteria that support the **access** and **exchange** of health information across the care continuum and by patients:

Supporting Care Across the Continuum

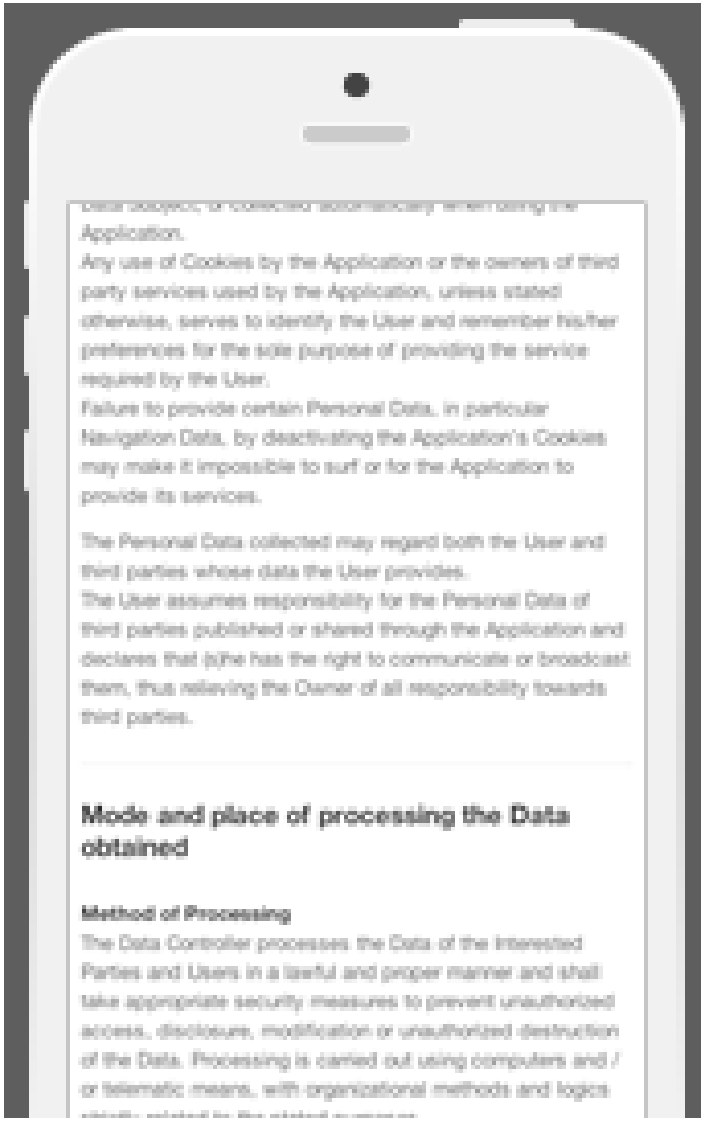
Expanding Patient Electronic Health Information Access and Exchange

ONC's Model Privacy Notice Background

- Model Privacy Notice (MPN): a voluntary, openly available resource designed to help developers provide transparent notice to consumers about what happens to their data.
- The MPN's approach is to provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users.
- The 2011 version of the MPN was developed in collaboration with the Federal Trade Commission and focused on Personal Health Records (PHRs), which were the emerging technology at the time.
- The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.

Reasons for Updating the MPN

- There is now a broad range of consumer health technologies beyond PHRs.
- More and more individuals are obtaining access to their electronic health information and using consumer health technology to manage this information.
- Users are concerned about privacy and security of their data.
- Existing privacy policies are long, complex, and confusing.
- Very few users read the privacy policy and those that do read it may not fully understand the content in the policy.



Process for Updating the MPN

- ONC put out a request for information on March 1, 2016 and sought comment on what information practices health technology developers should disclose to consumers and what language should be used to describe those practices.
- Feedback resulted in the 2016 version of the MPN that served as the basis for the Privacy Policy Snapshot Challenge. The Challenge called upon developers, designers, health data privacy experts, and creative, out-of-the-box thinkers to use the 2016 MPN to create an online tool that can generate a user-friendly "snapshot" of a product's privacy practices.
- The Challenge led to the updated 2018 MPN which incorporates user feedback from the Challenge participants. It can be used with the 3 MPN generators selected through the Challenge.

ONC's 2018 MPN

2018 Model Privacy Notice

The Model Privacy Notice (MPN) is a voluntary, openly available resource designed to help health technology developers provide clear notice to consumers about what happens to their digital health data when the consumer uses the developer's product. The MPN's approach is to provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.

The Office of the National Coordinator for Health Information Technology (ONC) updated the 2011 and 2016 versions of the MPN to address the larger variety of products collecting health data emerging on the market. The 2018 version of the MPN template incorporates user feedback from participants of ONC's 2017 Privacy Policy Snapshot Challenge (the Challenge). The Challenge called for developers to create an online MPN generator(s) using the 2016 MPN template. The winning MPN generators assist health technology developers with creating customizable privacy notices that are easy to understand and informative. The generators supplement the consumer-friendly notices with means for providing access to a developer's full privacy policy, and if applicable, HIPAA Notice of Privacy Practices and documentation for adjusting certain user preferences.

Preamble for Health Technology Developers	
What is the Model Privacy Notice (MPN)?	The MPN is a voluntary, openly available resource to help health technology developers who collect digital health data clearly convey information about their privacy policies to their users. Similar to a nutritional label, the MPN provides a snapshot of a company's existing privacy and security policies to encourage transparency and help consumers make informed choices when selecting products. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.
Who is the MPN for?	The MPN is for health technology developers whose technology or app uses and/or shares users' health data[1].
What laws might apply to you?	Health technology developers should consult the Federal Trade Commission (FTC)'s Mobile Health Apps Interactive Tool (which was developed in conjunction with the following Department of Health and Human Services offices and agency: ONC, Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)) to determine if they need to comply with the FTC Act, the FTC's Health Breach Notification Rule, HHS's Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules, or FDA rules implementing the Federal Food, Drug & Cosmetic Act, as applicable. This tool is not meant to be legal advice about all compliance obligations, but identifies relevant laws and regulations from these three federal agencies.
Does use of this MPN satisfy HIPAA requirements to provide a notice of privacy practices?	No. The MPN does not ensure compliance with HIPAA or any other law. However, the MPN may be used, as applicable, in conjunction with a HIPAA notice of privacy practices (please see MPN). To find more information on HIPAA directed towards health technology developers, visit the HIPAA Q's Portal for Health App Developers.

2018 Model Privacy Notice

Note: Developers of consumer health technology or apps ("health technology developers") that collect digital health data about individuals would use this template to disclose to consumers the developer's privacy and security policies. "**We**" refers to the health technology developer or technology product and "**you/your**" refers to the user/consumer of the health technology.

HIPAA	
This health technology developer is a HIPAA covered entity	☐ Yes ☐ No
[If yes] If the health technology developer is a HIPAA covered entity, select one of the statements on the right that applies to be inserted in the privacy notice.	☐ Please note that the health data we collect as part of this [insert name of technology product] are **NOT** covered by HIPAA and our company's HIPAA Notice of Privacy Practices does **NOT** apply ☐ Some of the health data we collect as part of this [insert name of technology product] also **are** protected by HIPAA. ○ Read our HIPAA Notice of Privacy Practices (embed link or popup] for more information.

Use: How we use your data internally

Primary Service: Our app or technology is used primarily to _____ (allow developers to insert particular use)

We collect and use your **identifiable data[2] to**:

- ☐ Provide the primary service[3] of the app or technology
- ☐ Develop marketing materials for our products
- ☐ Conduct scientific research
- ☐ Support company operations (e.g., quality control or fraud detection)
- ☐ Develop and improve new and current products and services (e.g., analytics[4])
- ☐ Other: _____
- ☐ We DO NOT collect and use your identifiable data

Share: How we share your data externally with other companies or entities

We share your **identifiable data[2] to**:

- ☐ Provide the primary service[3] of the app or technology
- ☐ Develop marketing materials for our products
- ☐ Conduct scientific research
- ☐ Support company operations (e.g., quality control or fraud detection)
- ☐ Develop and improve new and current products and services (e.g., analytics[4])
- ☐ Other:_____
- ☐ We DO NOT share your identifiable data[2]

ONC's 2018 MPN

We share your **data AFTER removing identifiers (note that remaining data may not be anonymous) to:**
☐ Provide the primary service[3] of the app or technology ☐ Develop marketing materials for our products ☐ Conduct scientific research ☐ Support company operations (e.g., quality control or fraud detection) ☐ Develop and improve new and current products and services (e.g., analytics[4]) ☐ Other:_____ ☐ We DO NOT share your data after removing identifiers

Sell: Who we sell your data to	
We sell your **identifiable data**[2] to some or all of the following: data brokers[5], marketing firms, advertising firms, or analytics firms.	☐ Yes, automatically ☐ Yes, only with your permission[6] ○ [If yes] Here is how you can check your settings, including permissions set as a default… ☐ No, we DO NOT sell your data
We sell your **data AFTER removing identifiers (note that remaining data may not be anonymous)** to some or all of the following: data brokers[5], marketing firms, advertising firms, or analytics firms.	☐ Yes, automatically ☐ Yes, only with your permission[6] ○ [If yes] Here is how you can check your settings, including permissions set as a default… ☐ No, we DO NOT sell your data after removing identifiers (note that remaining data may not be anonymous)
Store: How we store your data	
We store your data on the device	☐ Yes ☐ No
We store your data outside the device at our company or through a third party	☐ Yes ☐ No
Encryption[7]: How we encrypt your data	
We encrypt your data in the device or app	☐ Yes, automatically ☐ Yes, but only when you take certain steps (click to learn how) ☐ No ☐ N/A
We encrypt your data when stored on our company servers or with an outside cloud computing[8] services provider	☐ Yes, automatically ☐ Yes, but only when you take certain steps (click to learn how) ☐ No ☐ N/A
We encrypt your data while it is transmitted	☐ Yes, automatically ☐ Yes, but only when you take certain steps (click to learn how) ☐ No ☐ N/A

Privacy: How this technology accesses other data	
The technology or app requests access to other device data or applications, such as your phone's camera, photos, or contacts	☐ Yes, only with your permission. It connects to… ☐ Camera ☐ Photos ☐ Contacts ☐ Location services ☐ Microphone ☐ Health monitoring devices ☐ Other: _____ [If yes] Here is how you can check your settings, including permissions set as a default… ☐ No: This technology or app does NOT request access to other device data or applications, such as your phone's camera, photos, or contacts.
The technology or app allows you to share the collected data with your social media accounts, like Facebook	☐ Yes ☐ Yes, only with your permission. [If yes] Here is how you can check your settings… ☐ No: This technology or app does not allow you to share the collected data with your social media accounts, such as Facebook.
User Options: What you can do with the data that we collect	
The technology or app allows you to access, edit, share, or delete the data we have about you	☐ Yes. You can… ☐ Access your data ☐ Edit your data ☐ Share your data ☐ Delete your data [If yes] Here is how to do this… ☐ No
Deactivation[9]: What happens to your data when your account is deactivated	
When your account is deactivated/terminated by you or the company, your data is…	☐ Deleted immediately ☐ Deleted after __ days, weeks, months, years [select applicable interval] ☐ Permanently retained and used ☐ Retained and used until you request deletion
Policy Changes: How we will notify you if our privacy policy changes	
Describe how/if the company will notify consumers of privacy policy changes (e.g. merger or acquisition) and provide link to section in privacy policy.	
Breach[10]: How we will notify you and protect your data in case of an improper disclosure	
(Company name) complies with all applicable laws regarding breaches. Describe how the company will protect consumers' data in the case of a breach and provide link to section in privacy policy.	

Public Health Updates

The Fight Against Communicable Diseases: Leveraging Health IT

- To combat the devastating effects of communicable diseases (e.g., Zika virus, flu), ONC is aiming to create the ability and capacity for public health laboratories (PHLs) to send and receive a standard pregnancy status with electronic lab orders.
  - ONC is partnering with HHS IDEALab, CDC, CMS and the Association of Public Health Laboratories to create a national system for electronic order entry that can interface with the PHLs and electronic health records and use HL7 messaging or a web-based tool to create efficient and standard transmittance of pregnancy status for lab orders.
  - We are using electronic test order and results (ETOR) for this planned exchange. Currently, there is limited capacity for providers and public health labs to exchange this information electronically.
  - In the Fall of 2017, ONC included pregnancy status in the Interoperability and Standards Advisory, which was one of the recommendations of the Task Force.

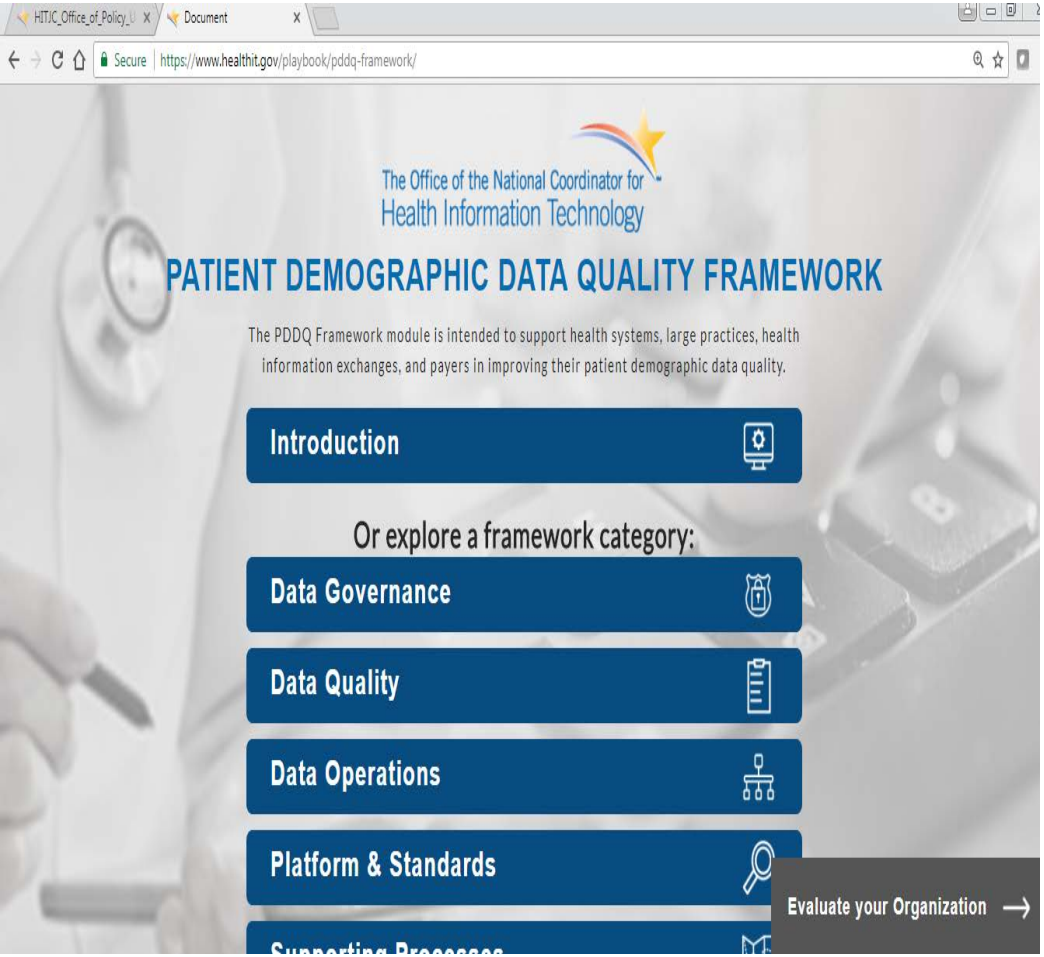
Disaster Preparedness and Response—Patient Unified Lookup System for Emergencies

- PULSE is designed to provide interconnectivity to enable provider organizations (including HIOs) and healthcare professionals to query for and view patient documents during disasters
- Specifically, PULSE:
  - Authenticates Disaster Healthcare Volunteer (DHV/ESAR-VHP) providers to the PULSE Web Portal
  - Allows disaster workers to query and view patient documents (e.g., C-CDAs)
  - Federates queries and patient document requests to all connected HIOs
  - Functions only in certain regions in California

Disaster Preparedness and Response—2017 Hurricanes

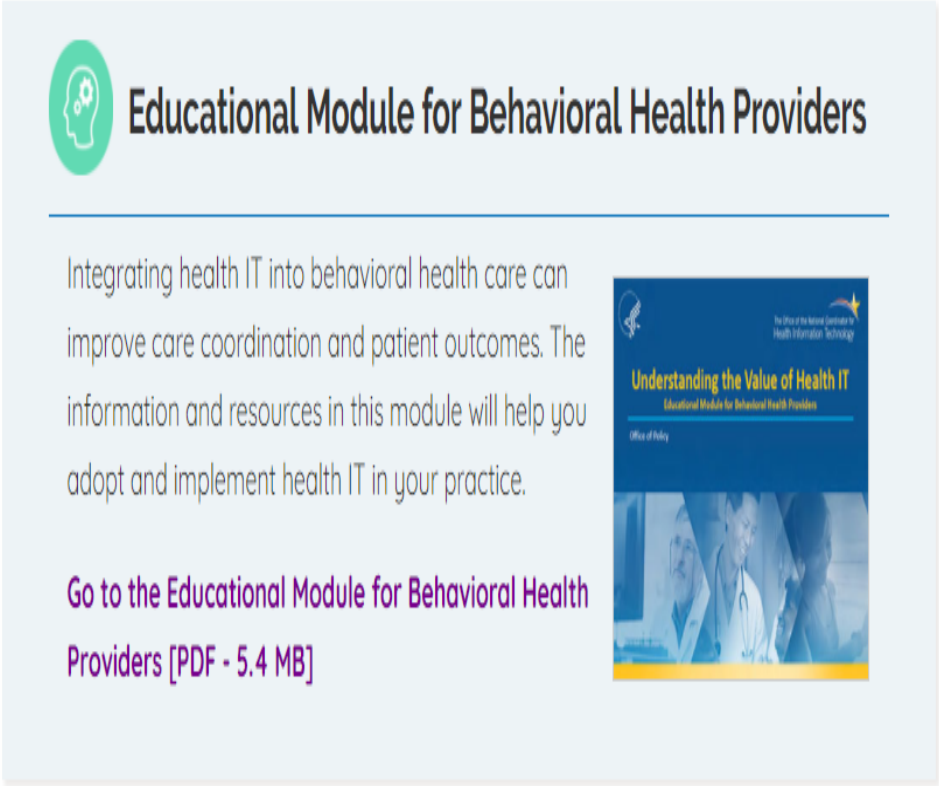
- ONC staff set up a command structure to:
  - Promote and document promising practices of health IT disaster preparedness/response/recovery systems
  - Provide support to state and public health agencies to ensure data from electronic surveillance systems are received in a timely and accurate manner to assist in disaster preparedness and response efforts
  - Continue to provide situational awareness on health IT related issues specific to the hurricane disaster response
  - Provide technical assistance and coordination to states and territories on their Advance Planning Document (APD) to provide funding to facilitate exchange of case reporting

Health IT Playbook – Patient Demographic Data Quality Framework & Ambulatory Guide



- **ONC released the [Patient Demographic Data Quality Framework] and [Ambulatory Guide] to assist health care practices and systems in assessing, measuring, and improving patient demographic data quality.**
  - The Framework may be accessed via the ONC Health IT playbook at: https://www.healthit.gov/playbook/pddq-framework/
  - The Guide may be accessed via the ONC Health IT playbook at: https://www.healthit.gov/playbook/ambulatory-guide/

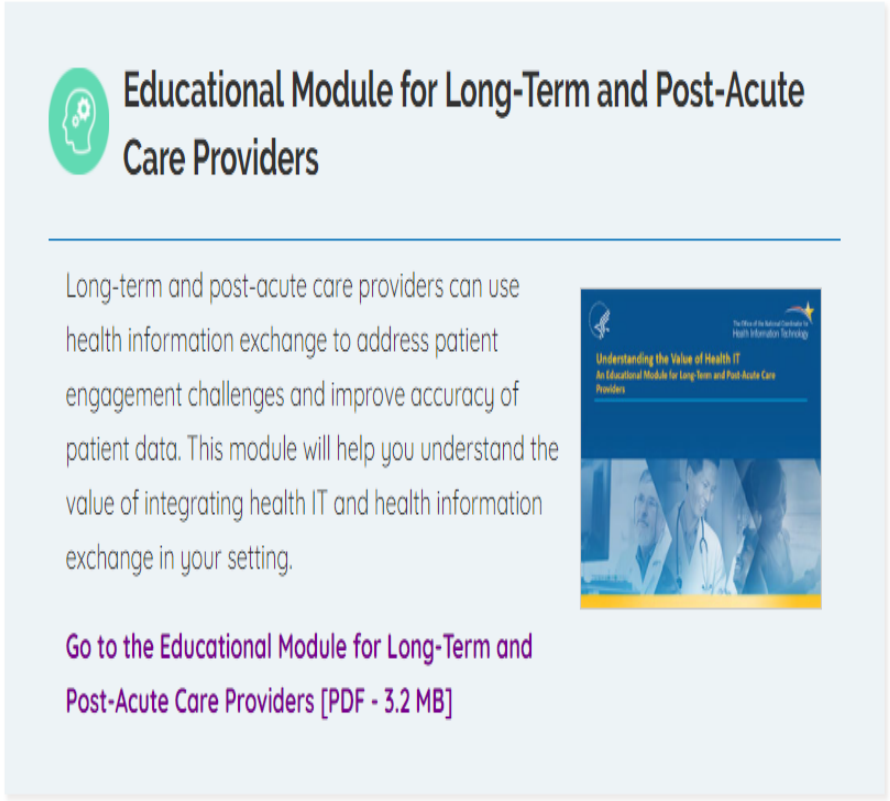
Health IT Playbook – Educational Module for Behavioral Health Providers



- The *Educational Module for Behavioral Health Providers* contains resources and information for behavioral health providers seeking to adopt and implement health IT.

- The module may be accessed via the ONC Health IT playbook at: https://www.healthit.gov/playbook/pdf/educational-module-Behavioral-Health-Providers.pdf

Health IT Playbook – Educational Module for LTPAC Providers



- The *Educational Module for Long- Term and Post Acute Care Providers* contains resources and information for LTPAC providers seeking to adopt and implement health IT.

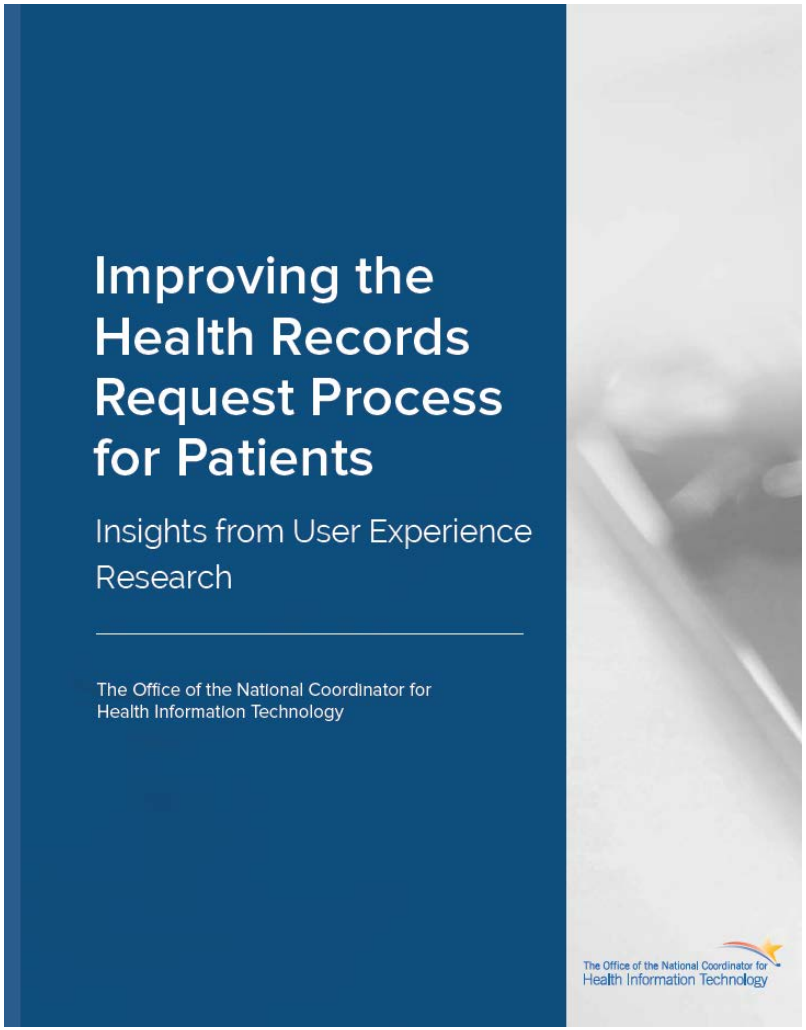
- The module may be accessed via the ONC Health IT playbook at: https://www.healthit.gov/playbook/pdf/educational-module-LTPAC.pdf

Consumer: ONC Report

ONC conducted interviews with **17 consumers** to understand their experiences — and challenges — accessing their patient data.

We also analyzed medical record release information and forms from **50 large health systems and hospitals across the country representing 32 states.**

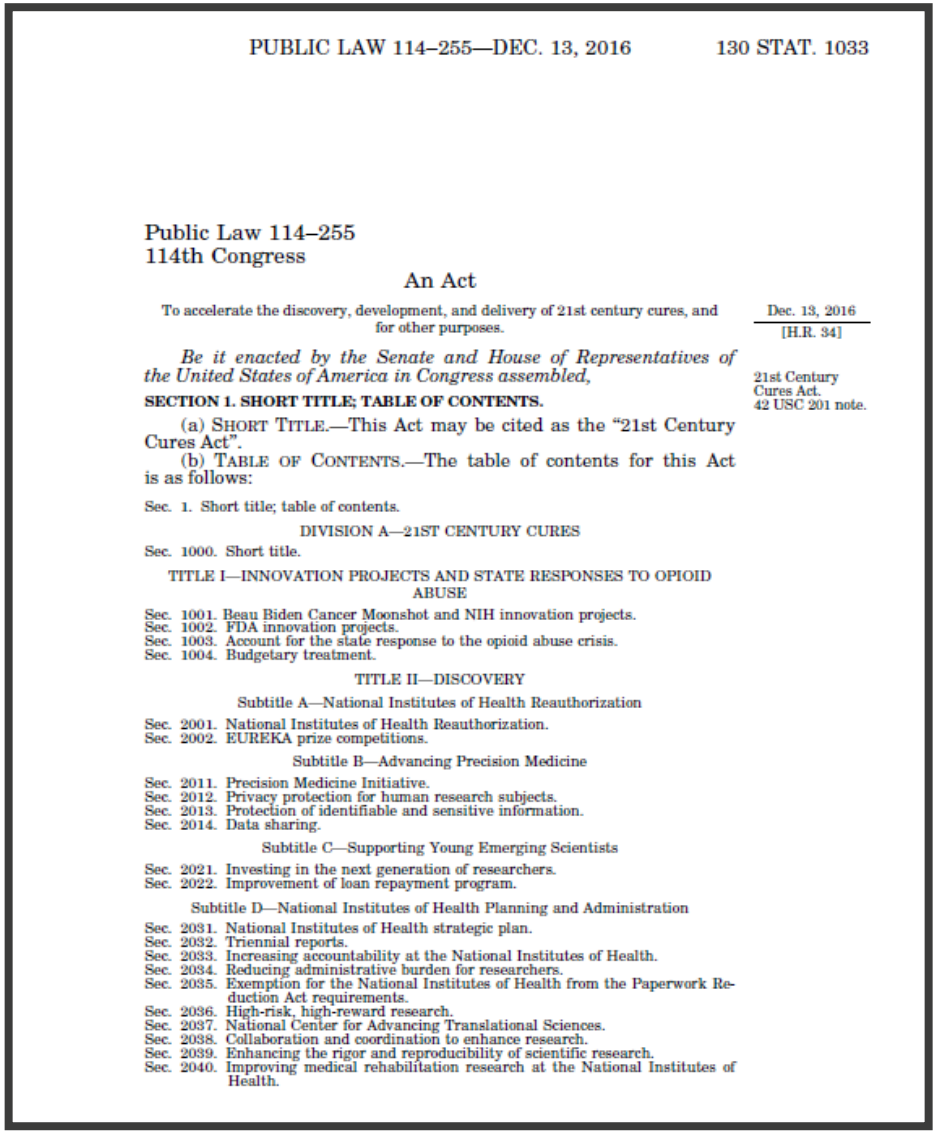
Then, **we talked to insiders** — ONC and partner stakeholders, as well as 4 medical record fulfillment administrators — to unpack the records request process and look for opportunities to make it better for consumers.



21st Century Cures Act – Title IV

Title IV – DELIVERY

- **Sec. 4001.** Assisting doctors and hospitals in improving quality of care for patients.
- **Sec. 4002.** Transparent reporting on usability, security, and functionality.
- **Sec. 4003.** Interoperability.
- **Sec. 4004.** Information blocking.
- **Sec. 4005.** Leveraging electronic health records to improve patient care.
- **Sec. 4006.** Empowering patients and improving patient access to their electronic health information.
- **Sec. 4007.** GAO study on patient matching.
- **Sec. 4008.** GAO study on patient access to health information.



PUBLIC LAW 114–255—DEC. 13, 2016 130 STAT. 1033

Public Law 114–255
114th Congress

An Act

To accelerate the discovery, development, and delivery of 21st century cures, and for other purposes.

Dec. 13, 2016
[H.R. 34]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

21st Century Cures Act.
42 USC 201 note.

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "21st Century Cures Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Section 4001 – Focus on Burden Reduction

- In Section 4001(a) of 21st Century Cures, the Secretary of HHS is required to set goals concerning the reduction of regulatory and administrative burden relating to the use of EHRs.
- The Secretary shall establish a goal with respect to the reduction of burden, create a strategy, and craft recommendations to achieve that goal. The strategy shall prioritize several areas, including but not limited to:
  - CMS programs (for example, alternative payment models and Merit-based Incentive Payment Systems);
  - Public health;
  - Health IT certification;
  - Individuals access to their electronic health information;
  - Aligning and simplifying quality measures; and
  - Privacy and security.

Section 4001 Overview: Pediatric Certification

In addition to burden reduction, section 4001(b)(C)(iii) refers to health IT for pediatrics.

> "…the Secretary, in consultation with relevant stakeholders, shall make recommendations for the voluntary certification of health information technology for use by pediatric health providers to support the health care of children."

Section 4002 Overview: Transparent reporting on usability, security and functionality

- Section 4002 lays out several items concerning the usability of EHRs.
  - Conditions of Certification
    - "[T]he Secretary…shall require, as a condition of certification and maintenance of certification for programs maintained or recognized under this paragraph, consistent with other conditions and requirements under this title, that the health IT developer or entity" not engage in information blocking, does not inhibit the appropriate exchange, access, and use of electronic health information, or does not engage in other prohibited practices.
  - EHR Reporting Program
    - "the Secretary shall award grants, contracts, or agreements to independent entities on a competitive basis to support the convening of stakeholders…collect the information required to be reported in accordance with the criteria established as described subsection (a)(3), and develop and implement a process…and report such information to the Secretary."

Section 4003 Overview: Trusted Exchange Framework and Common Agreement

Section 4003(b) directs the National Coordinator to establish a "trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks[.]"

Section 4003 Overview: Digital Provider Directory

- In 4003(c), the Cures Act requires that the Secretary create a provider digital contact information index, which can be established *de novo* or through a partnership with a private entity.
- The Center for Program Integrity (CPI) in CMS will be responsible for implementing the provision. CPI is working with ONC on implementation of the provision.

Section 4003 Overview: Health Information Technology Advisory Committee

- In 4003(e), the Cures Act established the Health Information Technology Advisory Committee (HITAC).
- Timeline of relevant HITAC establishment milestones:
  - June 30, 2017: Health IT Policy and Standards Committees officially sunset
  - July - August 2017: ONC archived former committees' materials, which are still available at healthit.gov
  - August 2017: Charter for the HITAC approved by Secretary Price
  - January 2018: First meeting of the HITAC

HITAC Priority Target Areas

Priority Target Areas noted in Section 4003 cover the following areas:

- Achieving a health information technology infrastructure that allows for the electronic access, exchange, and use of health information
- The promotion and protection of privacy and security of health information in health IT
- The facilitation of secure access by an individual to such individual's protected health information
- Any other target area that the HITAC identifies as an appropriate target area to be considered

Additional Target Areas

"(C) ADDITIONAL TARGET AREAS.—For purposes of this section, the HIT Advisory Committee may make recommendations under subparagraph (A), in addition to areas described in subparagraph (B), with respect to any of the following areas:

1. Health care coordination and continuity; reducing medical errors; improving population health; reducing chronic disease and advancing research and education
2. Children's needs and other vulnerable populations
3. Collection of patient demographic data, including at a minimum, race, ethnicity, primary language, and gender information
4. Self-service; telemedicine; home health and remote monitoring

Additional Target Areas, cont'd

5. Technological needs of diverse populations
6. Technologies that support data for quality and public reporting programs; public health or drug safety
7. Management of identifiable health information for unauthorized individuals
8. Use of a certified health information technology for each individual in the United States

Section 4004 Overview: Information Blocking

- Section 4004(a) provides a definition of information blocking:
  - In this section, the term 'information blocking' means a practice that—
    - ''(A) except as required by law or specified by the Secretary pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and
    - "(B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or (ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Section 4005 Overview: Leveraging EHRs to improve patient care

- Section 4005(a)-(b) – Certification as it relates to the capability "of transmitting to, and where applicable, receiving and accepting data from, registries in accordance with standards recognized by the Office of the National Coordinator for Health Information Technology, including clinician-led clinical data registries, that are also certified to be technically capable of receiving and accepting from, and where applicable, transmitting data to certified electronic health record technology in accordance with such standards."
- Section 4005(c) – Treatment of health IT developers with respect to patient safety organizations and report
  - "…a health information technology developer shall be treated as a provider…for purposes of reporting and conducting patient safety activities concerning improving clinical care through the use of health information technology that could result in improved patient safety, health care quality, or health care outcomes."

Section 4006 Overview: Empowering patients and improving patient access to their electronic health information

- Section 4006 instructs the Secretary to use "existing authorities to encourage partnerships between health information exchange organizations and networks and health care providers, health plans, and other appropriate entities with the goal of offering patients access to their electronic health information in a single, longitudinal format that is easy to understand, secure, and may be updated automatically."
- Includes several provisions, including provisions related to education of providers, access to health information, and usability.

Sections 4007 and 4008

- Section 4007
  - » GAO study on patient matching.
- Section 4008
  - » GAO study on patient access to health information.

Proposed Rule
Health IT: Interoperability and Certification Enhancements

- Target Publication is **April 2018**
- Update certain provisions of the HITECH Act
- Implement certain provisions of the 21st Century Cures Act, including provisions related to:
  - » conditions of certification and maintenance of certification for a health information technology developer or entity;
  - » the voluntary certification of health IT for use by pediatric health providers;
  - » health information networks voluntary attestation to their adoption of a trusted exchange framework and common agreement in support of network-to-network exchange; and
  - » reasonable and necessary activities that do not constitute information blocking.