The Office of the National Coordinator for Health Information Technology

Privacy & Security Update
Office of the Chief Privacy Officer
Office of the National Coordinator for Health IT, HHS

FACA Joint Meeting
April 19, 2016

Lucia C. Savage, JD
Chief Privacy Officer

HIPAA Basics & State-Focused Activities

PART I – Privacy

- Individuals Right to Access
  - » Including directing transmission of their PHI to a third party, even an app
- HIPAA Supports Interoperability-permitted uses
- State Privacy Project Update

PART II – Security

- Cybersecurity (CISA) Task Force
- Information Sharing and Analysis Organizations (ISAO)
- Role of ONC in HHS Security Efforts

The Problem

1 IN 3 INDIVIDUALS

who have seen a health care provider in the last year experienced at least one of the following gaps in information exchange.

Had to bring an X-ray, MRI, or other type of test result with them to the appointment.

Had to wait for test results longer than they thought reasonable.

Had to redo a test or procedure because the earlier test results were not available.

Had to provide their medical history again because their chart could not be found.

Had to tell a health care provider about their medical history because they had not gotten their records from another health care provider.

Source: http://www.nejm.org/doi/pdf/10.1056/NEJMsa063979

Interoperability Pledge

- The Pledge:
  - **Consumer Access:** To help consumers easily and securely access their electronic health information, direct it to any desired location, learn how their information can be shared and used, and be assured that this information will be effectively and safely used to benefit their health and that of their community.
  - **No Blocking/Transparency**: To help providers share individuals' health information for care with other providers and their patients whenever permitted by law, and not block electronic health information (defined as knowingly and unreasonably interfering with information sharing).
  - **Standards**: Implement federally recognized, national interoperability standards, policies, guidance, and practices for electronic health information, and adopt best practices including those related to privacy and security.

OCR Guidance on Patient Access

HHS.gov Health Information Privacy — U.S. Department of Health & Human Services

I'm looking for...

HHS A-Z Index

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

HHS Home > HIPAA > For Professionals > Privacy > Guidance > Individuals' Right under HIPAA to Access their Health Information

- HIPAA for Professionals
- Privacy
  - Summary of the Privacy Rule
  - Guidance
  - Combined Text of All Rules
- Security
- Breach Notification
- Compliance & Enforcement
- Special Topics
- Patient Safety
- Covered Entities & Business Associates
- Training & Resources

Text Resize A A A | Print | Share

Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

Newly Released FAQs on Access Guidance – Click Here!

Introduction

Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. With the increasing use of and continued advances in health information technology, individuals have ever expanding and innovative opportunities to access their health information electronically, more quickly and easily, in real time and on demand. Putting individuals "in the driver's seat" with respect to their health also is a key component of health reform and the movement to a more patient-centered health care system.

The regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protect the privacy and security of individuals' identifiable health information and establish an array of individual rights with respect to health information, have always recognized the importance of providing individuals with the ability to access and obtain a copy of their health information. With limited exceptions, the HIPAA Privacy Rule (the Privacy Rule) provides individuals with a legal, enforceable right to see and receive copies upon request of the information in their medical and other health records maintained by their health care providers and health plans.

[OCR Access FAQs]

OCR Access Guidance, Interoperability and Delivery System Reform

Health IT Buzz
The Latest on Health Information Technology from ONC

EHR/EMR | Health Innovation | From the ONC Desk | ONC Programs

Health IT Buzz > Electronic Health & Medical Records > Interoperability > When and Where You Need It Most: Your Rights to Access and Transmit Your Health Information

When and Where You Need It Most: Your Rights to Access and Transmit Your Health Information

January 11, 2016, 11:08 am / Karen B. DeSalvo, M.D., M.P.H., M.Sc., and Lucia Savage, J.D. / Chief Privacy Officer

Tweet Share Share 23 Email this page

In order to effectively manage their health, individuals need to be able to access and use their health information when, where, and how they want, including sending it to the people and tools helping them become or stay healthy – neighbors, friends, relatives, health care providers who are treating or consulting with the individual, or even third-party software tools used for self-management. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the privacy of individuals' protected health information (PHI) and when and how that information can be shared. HIPAA also governs security protections for certain health information and establishes an array of individual rights with respect to that information. For example, HIPAA has long required that individuals be given copies of their health information referred to as the "right to access" or be able to direct that third parties of their choosing receive copies. The specific regulation is 45 CFR 164.524, and can be found in the HIPAA Privacy Rule.

Last week, the U.S. Department of Health and Human Services Office for Civil Rights, the entity responsible for interpreting and enforcing HIPAA, published an important set of Frequently Asked Questions (FAQs) clarifying how an individual's right to access their individual health information operates, including key points related to

NEW! HIPAA Access Guidance

Available online: **HHS OCR ACCESS GUIDANCE**: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Fact Sheet/FAQs

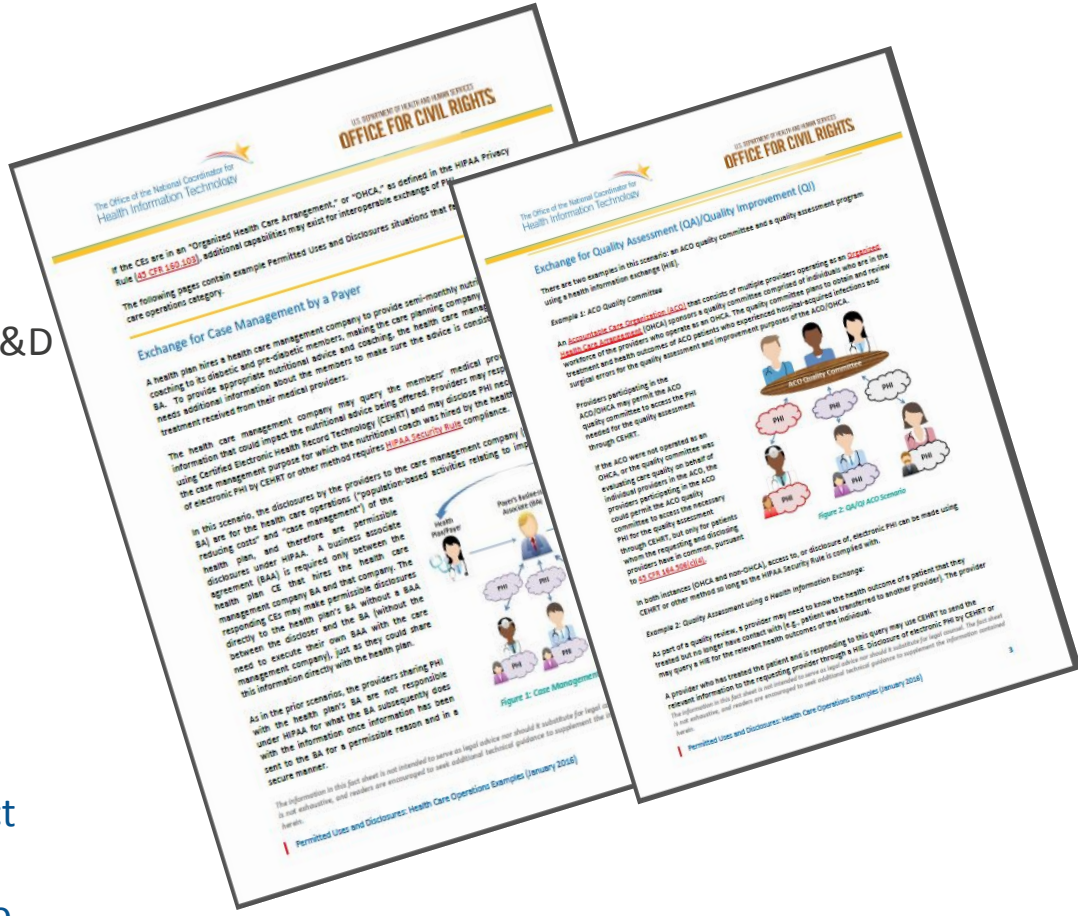
- Scope
- Form and Format and Manner of Access
- Timeliness
- Other (Clinical Labs)
- Fees
- Direct that a copy be transmitted to a third party, including an app.

HIPAA Patient Access Drill Down:

- HHS Office for Civil Rights enforces this individual right
  - Follow OCR on Twitter: @hhsocr
  - http://www.hhs.gov/hipaa
  - Developer-oriented Wiki-style portal: http://hipaaqsportal.hhs.gov/
- OCR issued new guidance in early 2016. Key concepts for apps and APIs in ONC's 2015 Edition rule
  - Timing of providing requested records
  - Automation
  - Electronic formats, if readily available
- This right has some limits:
  - Provider can reject media (such as a thumb drive) that reasonably threaten the security of the provider systems
  - Psychiatric notes and prison medical records can be withheld.
  - There are other limits that the individual can appeal.

Exchange Data as Permitted By Law (164.506): Pledge #2

- OCPO launched a 4-part blog series entitled “The Real HIPAA Supports Interoperability” on February 4
  - » Blog 1: The Real HIPAA Supports Interoperability
  - » Blog 2: Background on HIPAA’s PU&D
  - » Blog 3: Examples of Care Coordination, Care Planning, Case Management
  - » Blog 4: Examples of Quality Assurance and Population-Based Activities
- OCPO/OCR co-branded educational fact sheets that provide practical, plain language, examples with illustrations to supplement the blog series.

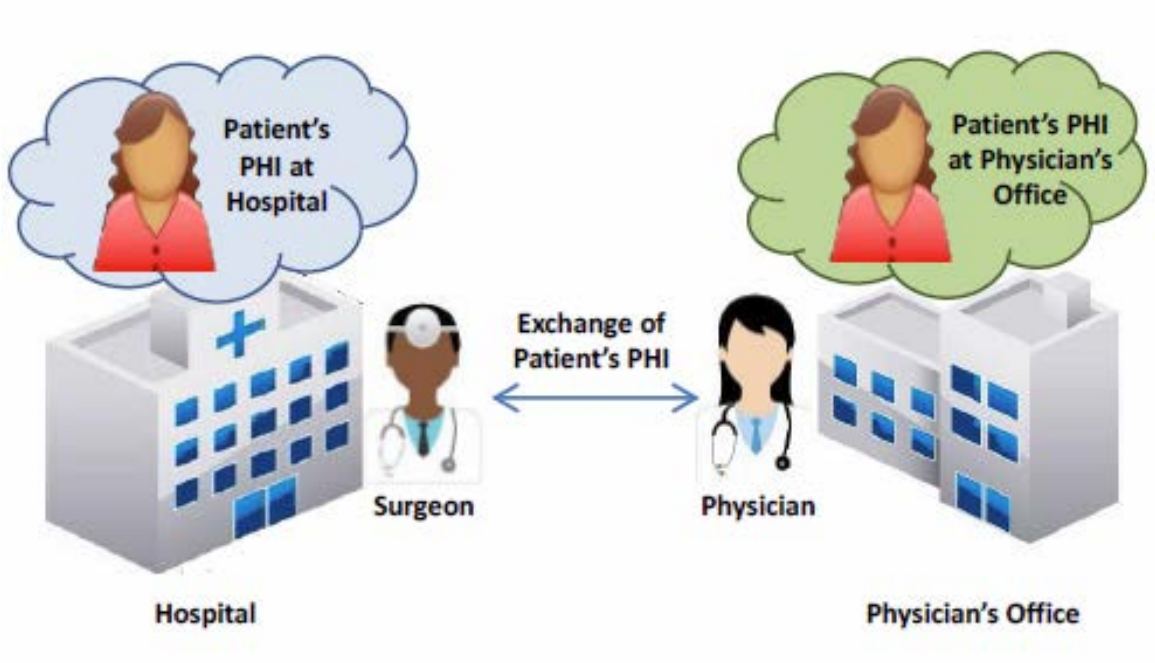


https://www.healthit.gov/newsroom/fact-sheets
Permitted Uses and Disclosures: Exchange for Health Care Operation [PDF - 1.3 MB] *
Permitted Uses and Disclosures: Exchange for Treatment [PDF - 1.1 MB] *

What are HIPAA Permitted Uses and Disclosures (PU&D)?

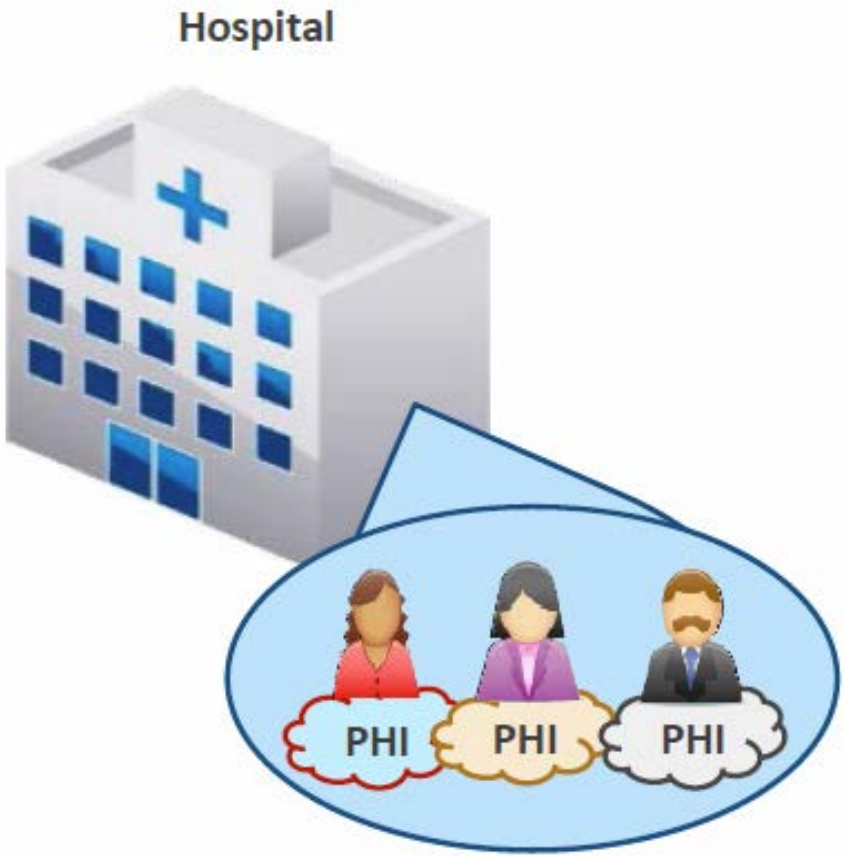
- Permitted Uses and Disclosures (PU&D) are situations in which a covered entity is permitted, but not required, to use and disclose PHI without first having to obtain a written authorization from the patient.

Basic Illustration of Permitted Uses

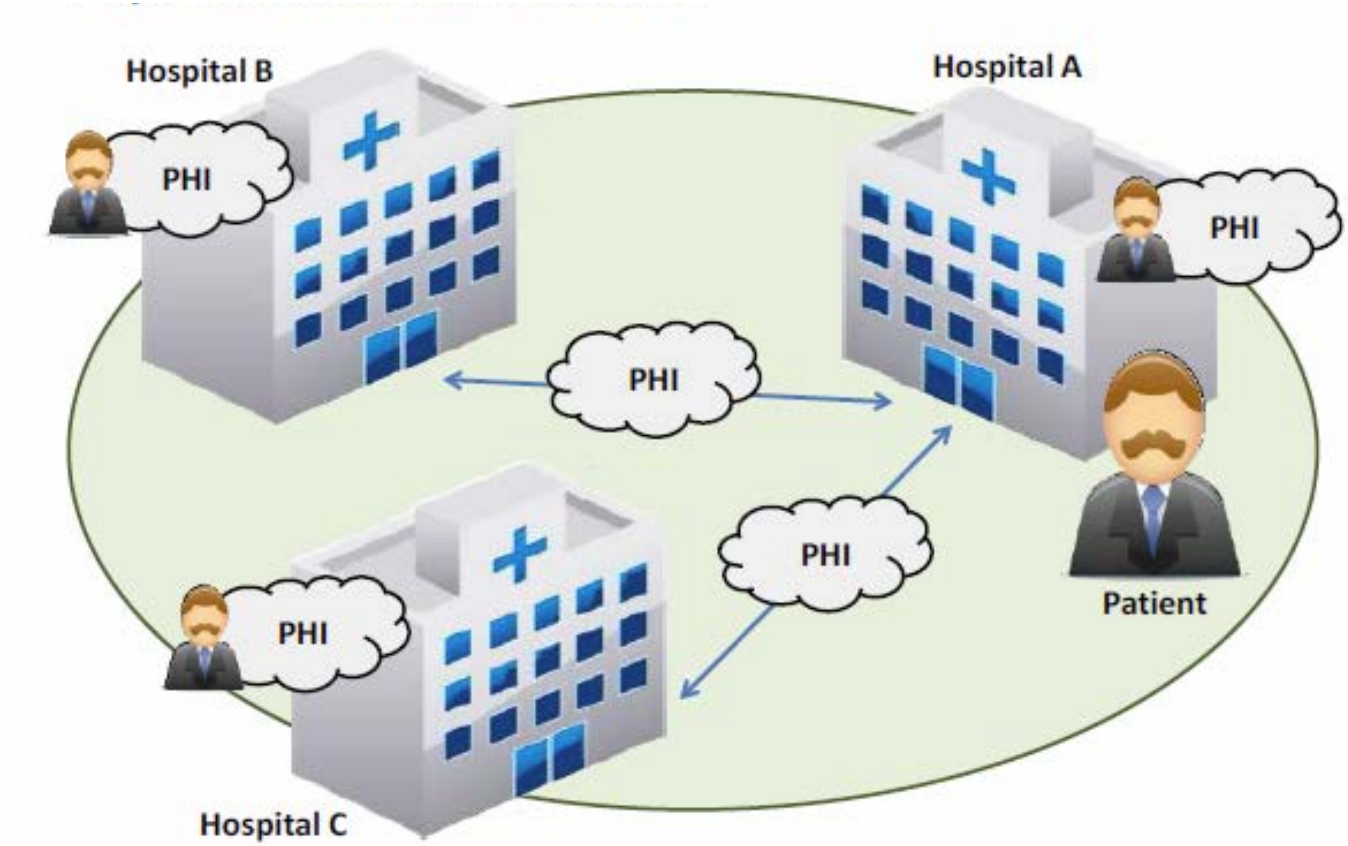


What Types of Activities are Considered Permitted Uses and Disclosure ?

- Conducting quality assessment and improvement activities
- Conducting case management and care coordination (including care planning)
- Conducting population-based activities relating to improving health or reducing health care cost
- Developing protocols
- Evaluating performance of health care providers and/or health plans



Population-Based Activities



How 2015 CEHRT Automates Permitted Uses and Patient Access

Under HIPAA

- Health information can be **shared for permitted uses (TPO)**
- Patients have the **right to an electronic copy** of their medical records, if the records are stored electronically, and **right to send a copy (transmit) elsewhere**

MU Stage 3 Requirements

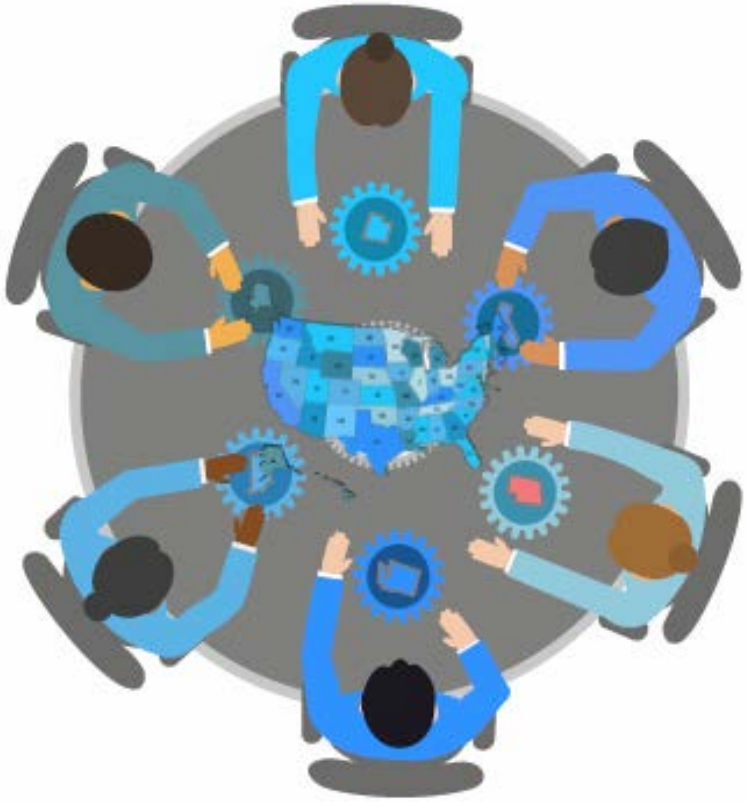
Patient must be given electronic access to portal within 24 hours in order to

- **view online, download and transmit** their health information
- **AND access to an API** that can be used by 3rd party apps

Related 2015 Edition CEHRT Requirements

- **API functionality** including
  - lookup and retrieve whole or partial patient record
- **API security** measures
- A **"transmit" option that includes unencrypted email**

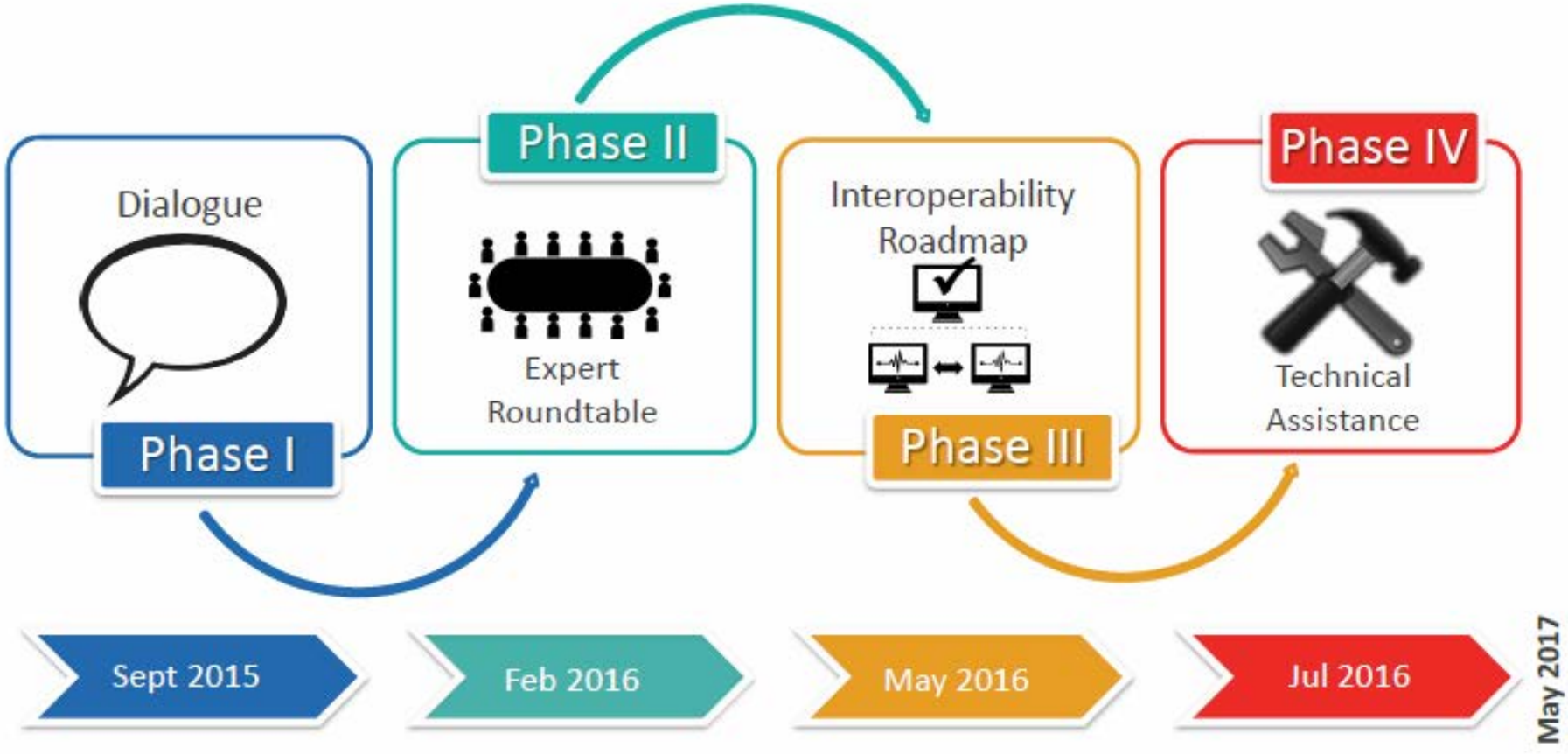
State-Privacy Project Update (Grant Award: Sept. 2015 – May 2017)



- Convene 5-8 States
- Utilize focused approach
- Explore Model Criteria

ONC Funding Opportunity Announcement (FOA)/Award:
http://www.grants.gov/web/grants/view-opportunity.html?oppId%3D277387

Timeline and Objectives Sept 2015 to May 2017



OCR Patient Access Guidance and Related Blog Posts

- OCR Patient Access Guidance
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- OCR Patient Access Blog Post
  - http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html#
- ONC Patient Access Blog Post
  - http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/your-rights-to-access-and-transmit-your-health-information/

The Office of the National Coordinator for Health Information Technology

Privacy & Security Update
Office of the Chief Privacy Officer
Office of the National Coordinator for Health IT, HHS

PART II – OCPO SECURITY

OCPO SECURITY

- Security in the Shared Roadmap
- CISA Taskforce
  - Overview
  - Members
  - Inaugural Meeting
- Information Sharing and Analysis Organizations (ISAO)
  - Overview
  - ISAO Activities
  - Project Update
- Role of ONC in HHS Security Efforts

Cybersecurity in the Roadmap Commitments and Milestones

- ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cyber security for critical public health infrastructure.
- Support, promote, and enhance information sharing capabilities within the healthcare and public health sector for bi-directional information sharing about cyber threats and vulnerabilities between the private health care industry and the federal government
- ☑ONC will work with NIST and OCR to finalize and publish the NIST Critical Infrastructure Cybersecurity Framework and HIPAA Security Rule Crosswalk
- ONC will work with stakeholders and ASPR to develop best practices for actions that small & medium size health care organizations can take when they become aware of cyber threats. ONC will consult with OCR to make sure the practices are compliant with the HIPAA Rules.

Healthcare Industry Cybersecurity Task Force Overview

- CISA Section 405:
  - The Cybersecurity Information Sharing Act of 2015 section 405(c) tasked HHS with the creation of a Healthcare Industry Cybersecurity Task Force, in collaboration with the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS)
  - Under the Act, Per CISA, the Task Force will consist of "…health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate…"

Healthcare Industry Cybersecurity Task Force Overview

- Task Force Charge:
  - Analyze how industries other than the healthcare industry have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;
  - Analyze challenges and barriers private entities in the healthcare industry face securing themselves against cyber attacks; and
  - Review challenges that HIPAA covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record.

In addition, the Task Force is charged to develop and deliver

- Information for the HHS Secretary to disseminate to healthcare industry stakeholders of all sizes for purposes of improving their preparedness for and response to cybersecurity threats affecting the healthcare industry and
- A plan for implementing Title I of the Act [Cybersecurity Information Sharing], so that Federal Government and healthcare industry stakeholders may in real time share actionable cyber threat indicators and defensive measures.

Healthcare Industry Cybersecurity Task Force Members

- After a public application period announced at HIMSS;
- Task Force members were selected based on recommendations from a panel of subject matter experts from HHS, DHS, and NIST. The following criteria were used in selecting Task Force members:
  - Service in a position of influence in an organization that is representative of a component of the broad health care and public health sector
  - Experience in dealing with technical, administrative, management, and/or legal aspects of health information security
  - Knowledge of major health information security policies, best practices, organizations, and trends
  - Ability to participate actively in Task Force meetings and contribute to Task Force products
- Complete info at Health Care Stakeholders Task Force

Healthcare Industry Cybersecurity Task Force Members

Theresa Meadows, MS, RN, CHCIO, FHIMSS, FACHE (Co-Chair) **Senior Vice President and Chief Information Officer, Cook Children's Health Care System**	**Emery Csulak, CISSP (Co-Chair)** **Chief Information Security Officer and Senior Privacy Official, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services**	**Fred Trotter** **Data Journalist, CareSet Systems**
Kevin Stine **Chief, Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology**	Joshua Corman Co-Founder, I Am The Cavalry	Ram Ramadoss, MBA, CISA, CISM, CISSP, CRISC, CIPP Vice President, CRP Privacy and Information Security and EHR Compliance Oversight, Catholic Health Initiatives
Laura Laybourn **Director, Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications, U.S. Department of Homeland Security**	Terry Rice Vice President, IT Risk Management, and Chief Information Security Officer, Merck & Co	Jacki Monson, JD Chief Privacy and Information Security Officer, Sutter Health
Alissa Johnson, PhD **Chief Information Security Officer, Stryker Corp.**	Michael McNeil Global Product Security and Services Officer, Philips Healthcare	Mark Jarrett, MD, MBA, MS Senior Vice President and Chief Quality Officer, Northwell Health and Professor of Medicine, Hofstra Northwell School of Medicine
Anura Fernando **Principal Engineer, Medical and Software Systems Interoperability, UL, LLC**	David Finn, CISA, CISM, CRISC Health Information Technology Officer, Symantec Corp.	Roy Mellinger, CISSP-ISSAP, ISSMP, CIM Vice President, IT Security, and Chief Information Security Officer, Anthem, Inc.
Dan McWhorter **Vice President and Chief Intelligence Strategist, FireEye, Inc.**	Christine Sublett, MA, CISSP, CIPT, CRISC, CGEIT Chief Information Security Officer and Head of Compliance, Augmedix, Inc.	George DeCesare, JD Senior Vice President and Chief Technology Risk Officer, Kaiser Permanente Health Plan
Vito Sardanopoli, CISM, CISSP, CISA **Director of Cyber Security Services and Governance, Quest Diagnostics**	David Ting Co-Founder and Chief Technology Officer, Imprivata, Inc.	Lauren Thompson, PhD Director, Department of Defense/Department of Veterans Affairs Interagency Program Office, Defense Health Management Systems

Health Care Industry Cybersecurity Task Force Inaugural Meeting

- CISA Task Force first in-person meeting is scheduled for April 21, 2016
  - The meeting is open to the public and it is the first of four in-person meetings the task force will hold during the next year before reporting their findings to Congress and the public
  - LOCATION: US Access Board 8th Floor Conference Room; 1331 F Street, NW, Suite 800, Washington, DC
  - Inaugural Meeting
- Future Meetings

IN PERSON

every 2-3 months on third Thursday of month

- April 21, 2016 [1st in person meeting]
- July 21, 2016
- September 15, 2016
- December 15, 2016

TELECONFRENCE

During months without in-person meetings

- May 19, 2016
- June 16, 2016
- August 18, 2016
- October 20, 2016
- November 17, 2016

Cyber Threat Information Sharing: Information Sharing and Analysis Organizations (ISAO)

- An ISAO is a group created to gather, analyze, and disseminate critical infrastructure information
- ISAOs offer a flexible approach to self-organized information sharing activities
- Key benefits:
  - » Share and Receive Actionable Cyber Threat Information to Protect Networks
  - » Increased and More Timely Awareness of Cyber Risks allows organizations to Implement Effective Mitigations and Reduce the Frequency and Impact of Cyber Incidents.

HHS ISAO Proposal - What we are trying to solve

A single entity currently does not exist that bridges the information sharing gap between HHS and the private sector

Current ad hoc information sharing is often dependent on voluntary cooperation from private sector entities

Improving information sharing in the evolving information sharing landscape as a result of EO 13691

ISAO ASPR Planning Grant

- The Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response (ASPR) awarded a grant to Harris County (TX) Health to gauge an understanding of the needs for cybersecurity information for sectors in Healthcare and Public Healthcare ("the Sector").
  - HHS is the "sector specific agency" for cyber-preparedness in the health and public health sector.
- The grant is HHS' first step in selecting a strategy that will enable organizations to collaborate in the information process within the private sector and between the private sector and government.
- This grant compliments HHS' effort in facilitating the President's Executive Order (EO) 13691 - Promoting Private Sector Cybersecurity Information Sharing,

HHS ISAO Proposal - Issues we are trying to solve

- HPH Sector is experiencing competition among information sharing organizations, which is not present in other sectors
  - » Has led to inefficiency and delays in sharing information
  - » HHS has not been able to ensure that information is shared with the HPH sector as a whole, beyond each organization's membership base
- Less economic incentive for companies within the HPH Sector to focus on cybersecurity compared to other sectors
- The HPH Sector is at a lower maturity than others with regard to cybersecurity
- HHS is encouraging the expanded use of electronic systems for managing health information, and therefore has a significant interest in, and the urgency to ensure that, these systems are secure.

Other ONC Efforts in Security and Cybersecurity

- Advise NC on security and cybersecurity issues, including ISAOs, Security Hygiene, Ransomware, etc.
- Work with Critical Infrastructure Partnership Advisory Council (CIPAC), Healthcare and Public Health Government Coordinating Council (HPH GCC) on cyber related activities.
- Coordinate with Department of Homeland Security, e.g.
  - Working with OCIO leading HHS's approach to implementing CISA / Automated Information Sharing (AIS) requirements and Cyber Threat Indicator Sharing aligned with DHS procedures
- Serve on the Joint GCC/SCC Cybersecurity Working group/Forum
  - Ensure alignment and coordination with Interoperability Roadmap Commitments, Calls-to-Action, and Milestones to HPH Sector activities (e.g. Sector-Specific Plan items)
  - Involvement with how to leverage the public-private partnership to address Cybersecurity and NSC/WH tasks

Role of ONC in HHS Security Efforts, cont'd.

- ASPR Planning Grant on ISAO
  - ONC is collaborating with ASPR in this initiative; providing technical assistance, education and outreach support.
- PIRT (Privacy Incident Response Team)
  - ONC get advanced notice of any privacy incidents, and provide guidance to the affected agency/operating divisions to aid in response.
  - Reviewed draft breach notification letters and provide feedback.
- HHS Information Sharing Concepts of Operations (CONOPS)– led by OCIO
  - The purpose of this concept of operations (CONOPS) is to establish a coordinated approach between the various HHS organizations and offices that will need to collaborate closely in responding to cyber incidents and events.
  - This plan provides a framework that facilitates and promotes information sharing between HHS and the HPH Sector by providing common understanding and expectations on how HHS coordinates internally and shares information with external HPH Sector stakeholders.