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

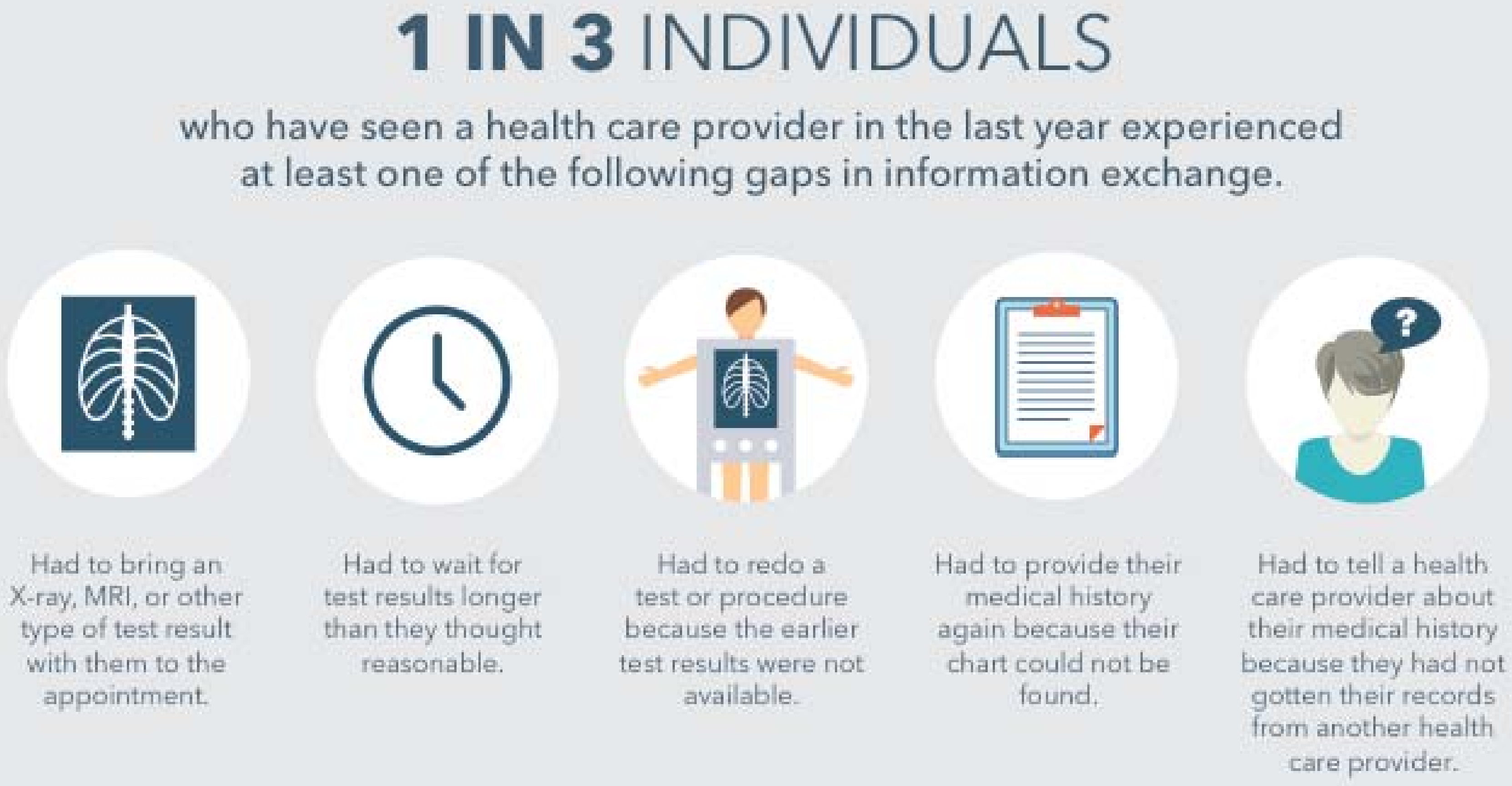
HIPAA Summit
Washington DC, March 22, 2016

Lucia C. Savage, JD
Chief Privacy Officer

Agenda

- Interoperability Pledge
- Individuals Right to Access
  - Including directing transmission of their PHI to a third party, even an app
- HIPAA Supports Interoperability-#permitteduse
- How Patient Access and #permitteduse fits into Certified EHR Technology.
  - Unencrypted email at individuals’ choosing
  - “Open” API
- Security Update:
  - CISA section 405 Health Care Sector Cybersecurity Task Force
- Open for Comment

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.

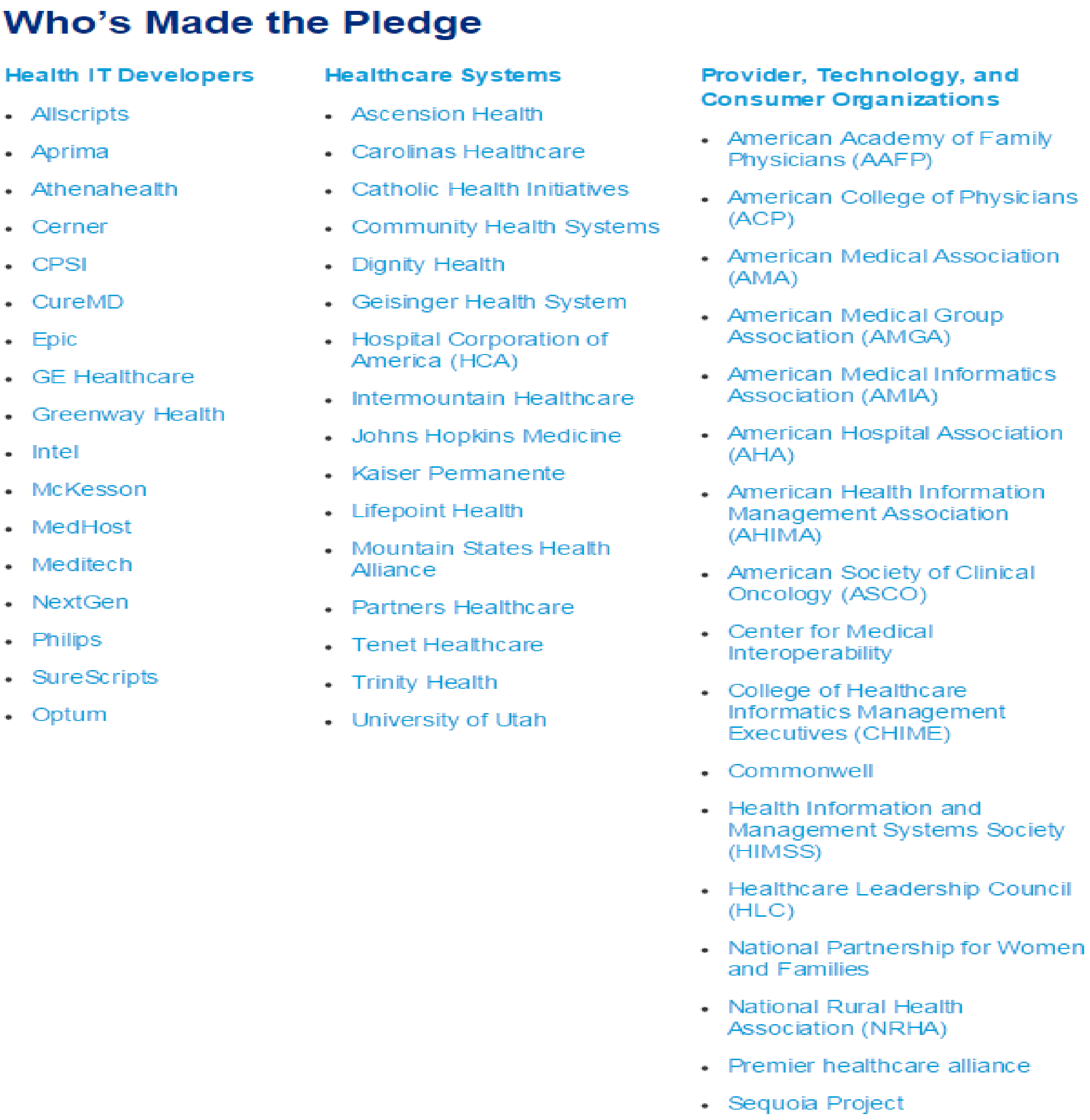
- Had to bring an X-ray, MRI, or other type of test result with them to the appointment.
- Had to wait for test results longer than they thought reasonable.
- Had to redo a test or procedure because the earlier test results were not available.
- Had to provide their medical history again because their 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.

Interoperability Pledge—Who Pledged (as of 2/29)?



Who's Made the Pledge

Health IT Developers

- Allscripts
- Aprima
- Athenahealth
- Cerner
- CPSI
- CureMD
- Epic
- GE Healthcare
- Greenway Health
- Intel
- McKesson
- MedHost
- Meditech
- NextGen
- Philips
- SureScripts
- Optum

Healthcare Systems

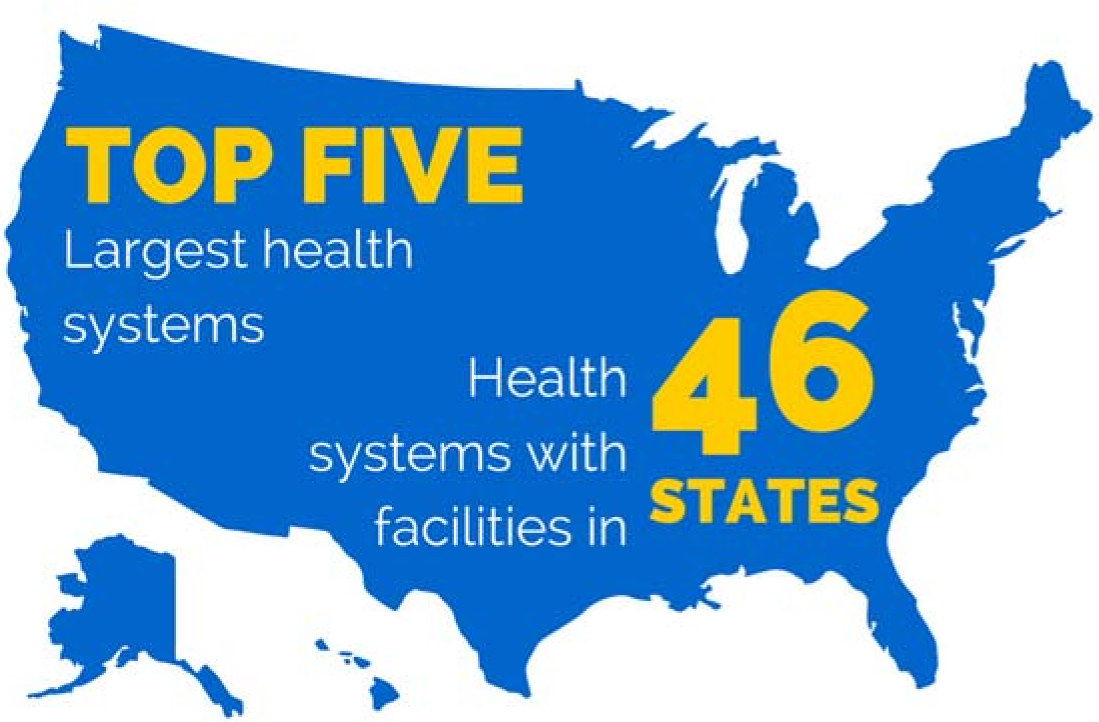
- Ascension Health
- Carolinas Healthcare
- Catholic Health Initiatives
- Community Health Systems
- Dignity Health
- Geisinger Health System
- Hospital Corporation of America (HCA)
- Intermountain Healthcare
- Johns Hopkins Medicine
- Kaiser Permanente
- Lifepoint Health
- Mountain States Health Alliance
- Partners Healthcare
- Tenet Healthcare
- Trinity Health
- University of Utah

Provider, Technology, and Consumer Organizations

- American Academy of Family Physicians (AAFP)
- American College of Physicians (ACP)
- American Medical Association (AMA)
- American Medical Group Association (AMGA)
- American Medical Informatics Association (AMIA)
- American Hospital Association (AHA)
- American Health Information Management Association (AHIMA)
- American Society of Clinical Oncology (ASCO)
- Center for Medical Interoperability
- College of Healthcare Informatics Management Executives (CHIME)
- Commonwell
- Health Information and Management Systems Society (HIMSS)
- Healthcare Leadership Council (HLC)
- National Partnership for Women and Families
- National Rural Health Association (NRHA)
- Premier healthcare alliance
- Sequoia Project

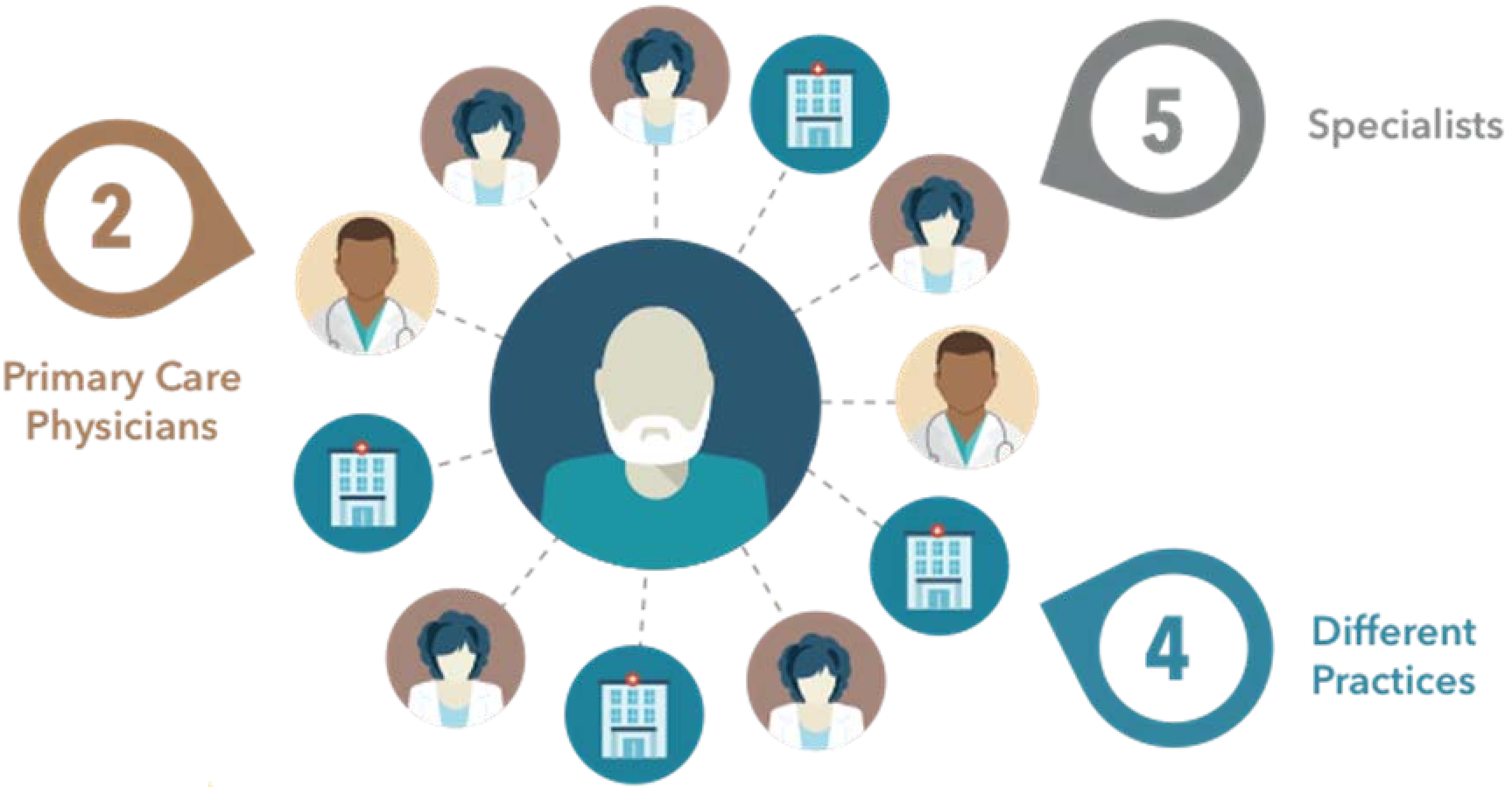
Your Organization Can Pledge Too

- https://www.healthit.gov/commitment



Patient Access (164.524): Pledge #1

In a given year, the average Medicare patient visits...



Source: https://www.healthit.gov/sites/default/files/briefs/oncdatabrief30_accesstrends_.pdf

Value of Online Access

PATIENTS VALUE ONLINE ACCESS TO THEIR HEALTH RECORDS

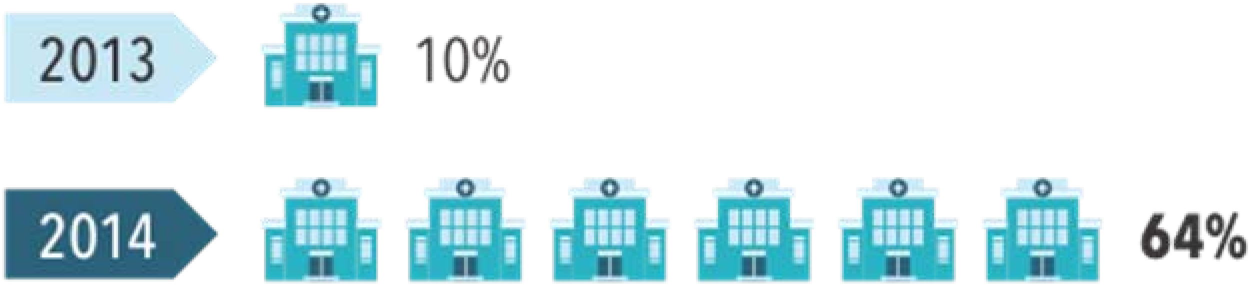
AGE IS NOT A FACTOR

7/10 individuals value online access to their health data.[1]

67% of U.S. adults age 65 and older say that accessing their medical information online is important.[2]

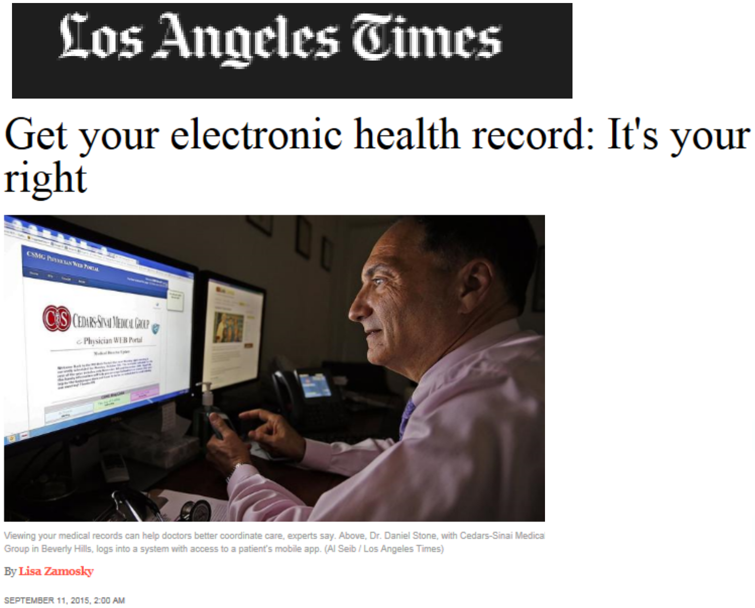
Increasingly More Patients Have Online Access

In 2014, **6 out of 10 hospitals** provided their patients with the capability to **view, download, and transmit** their health information —a significant increase from the previous year.



Source: https://www.healthit.gov/sites/default/files/briefs/oncdatabrief29_patientengagement.pdf

Going Mainstream



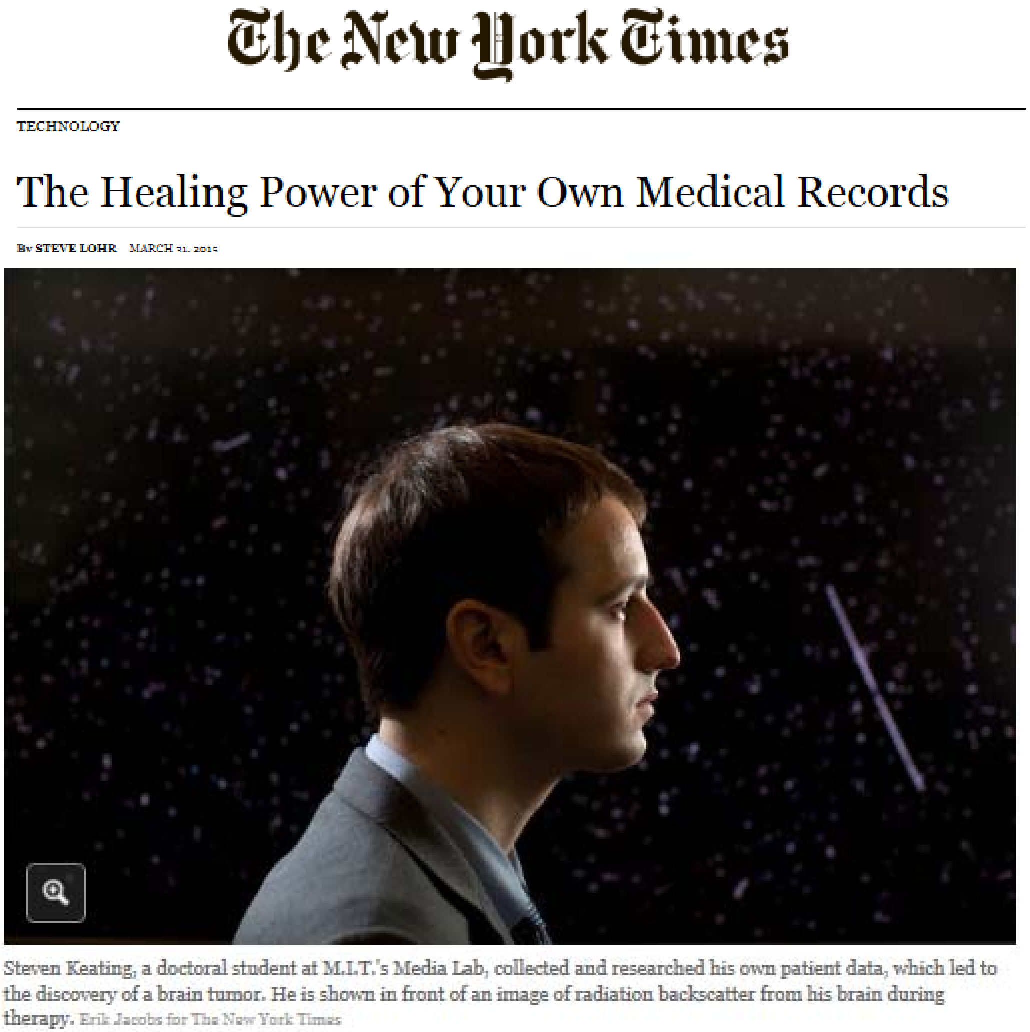
Los Angeles Times

Get your electronic health record: It's your right

Viewing your medical records can help doctors better coordinate care, experts say. Above, Dr. Daniel Stone, with Cedars-Sinai Medical Group in Beverly Hills, logs into a system with access to a patient's mobile app. (Al Seib / Los Angeles Times)

By Lisa Zamosky

SEPTEMBER 11, 2015, 2:00 AM



The New York Times

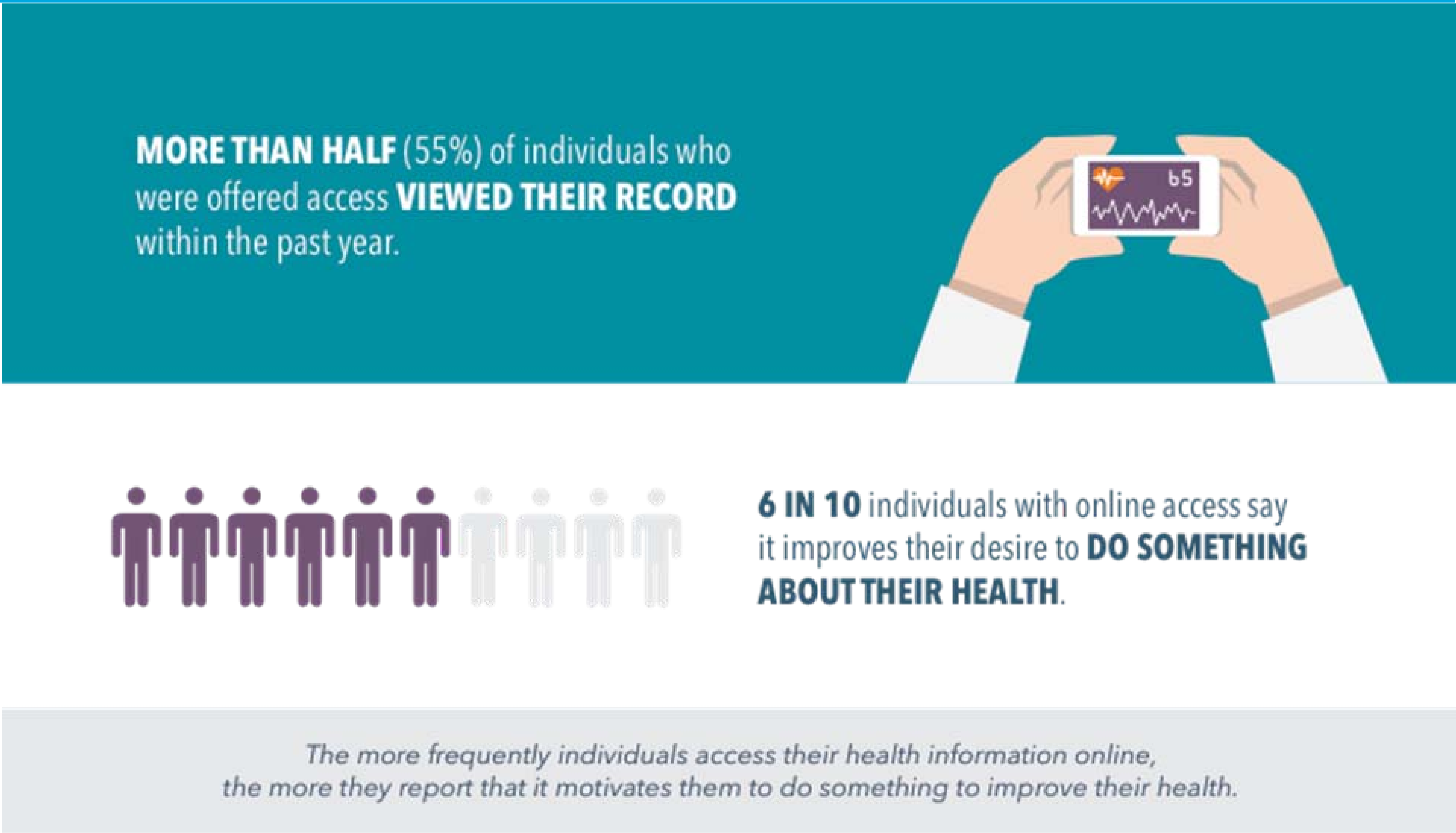
TECHNOLOGY

The Healing Power of Your Own Medical Records

By STEVE LOHR MARCH 31, 2015

Steven Keating, a doctoral student at M.I.T.'s Media Lab, collected and researched his own patient data, which led to the discovery of a brain tumor. He is shown in front of an image of radiation backscatter from his brain during therapy. Erik Jacobs for The New York Times

If you build it will they come?



MORE THAN HALF (55%) of individuals who were offered access **VIEWED THEIR RECORD** within the past year.

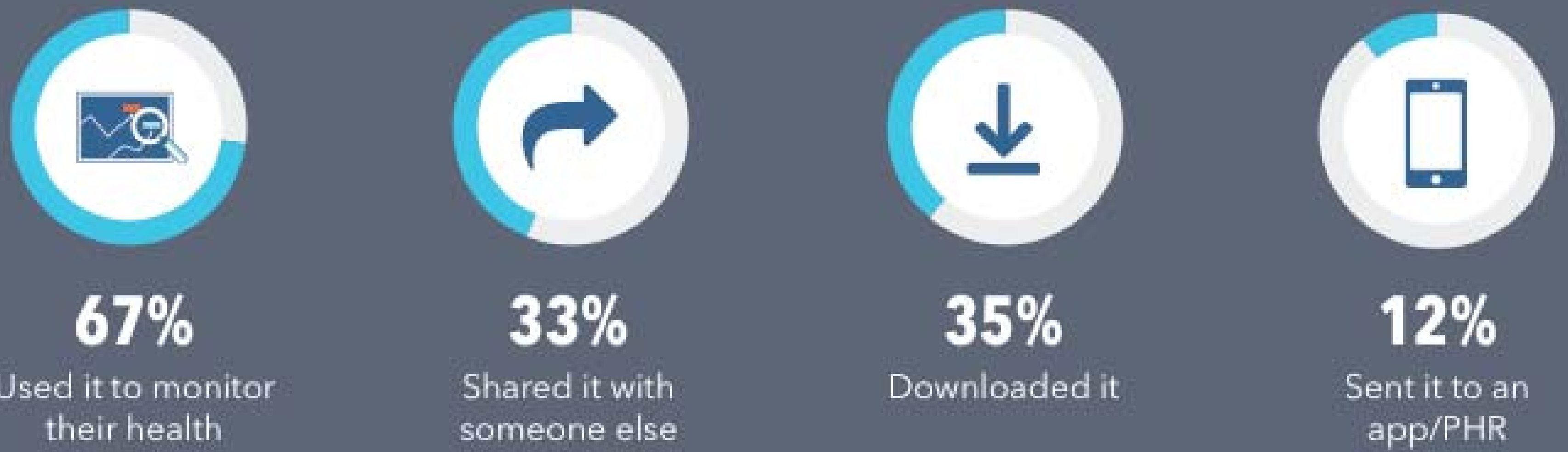
6 IN 10 individuals with online access say it improves their desire to **DO SOMETHING ABOUT THEIR HEALTH**.

The more frequently individuals access their health information online, the more they report that it motivates them to do something to improve their health.

Sources: http://www.nejm.org/doi/pdf/10.1056/NEJMsa063979
http://www.nationalpartnership.org/research-library/health-care/HIT/engaging-patients-and-families.pdf

Individuals are Engaging with their Health Records Online

Individuals are using their online access to address information gaps and manage their health.



67% Used it to monitor their health

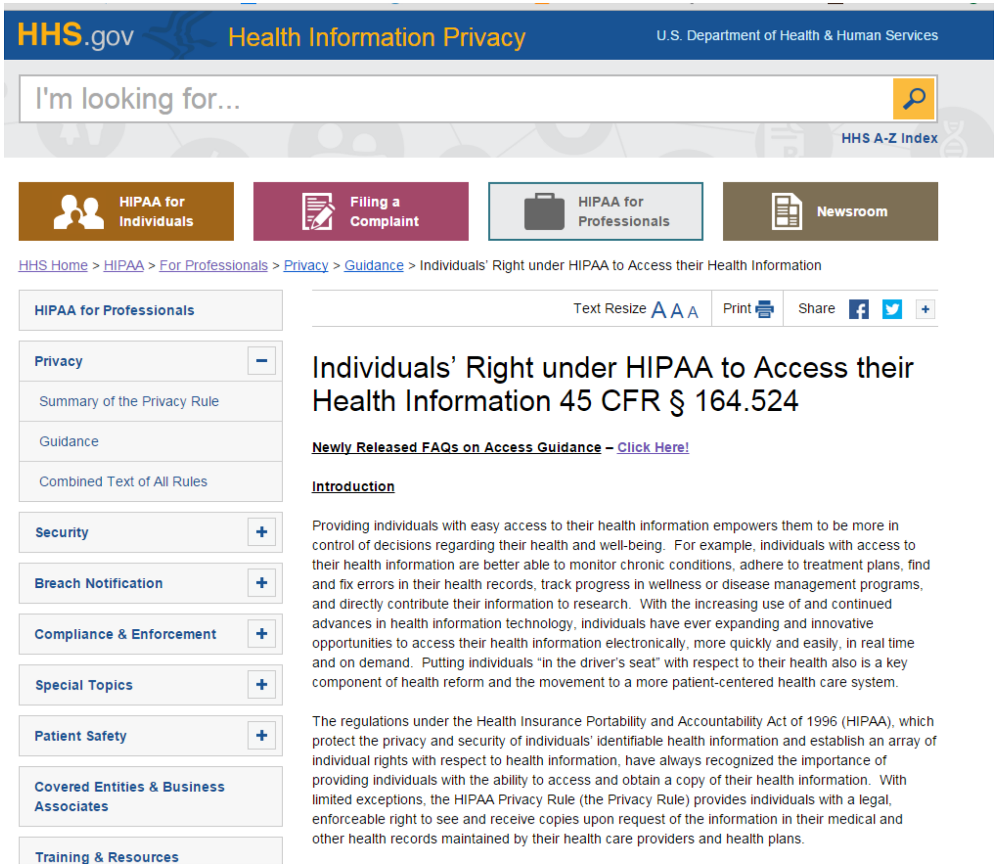
33% Shared it with someone else

35% Downloaded it

12% Sent it to an app/PHR

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

OCR Guidance on Patient Access



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

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

Newly Released FAQs on Access Guidance – Click Here!

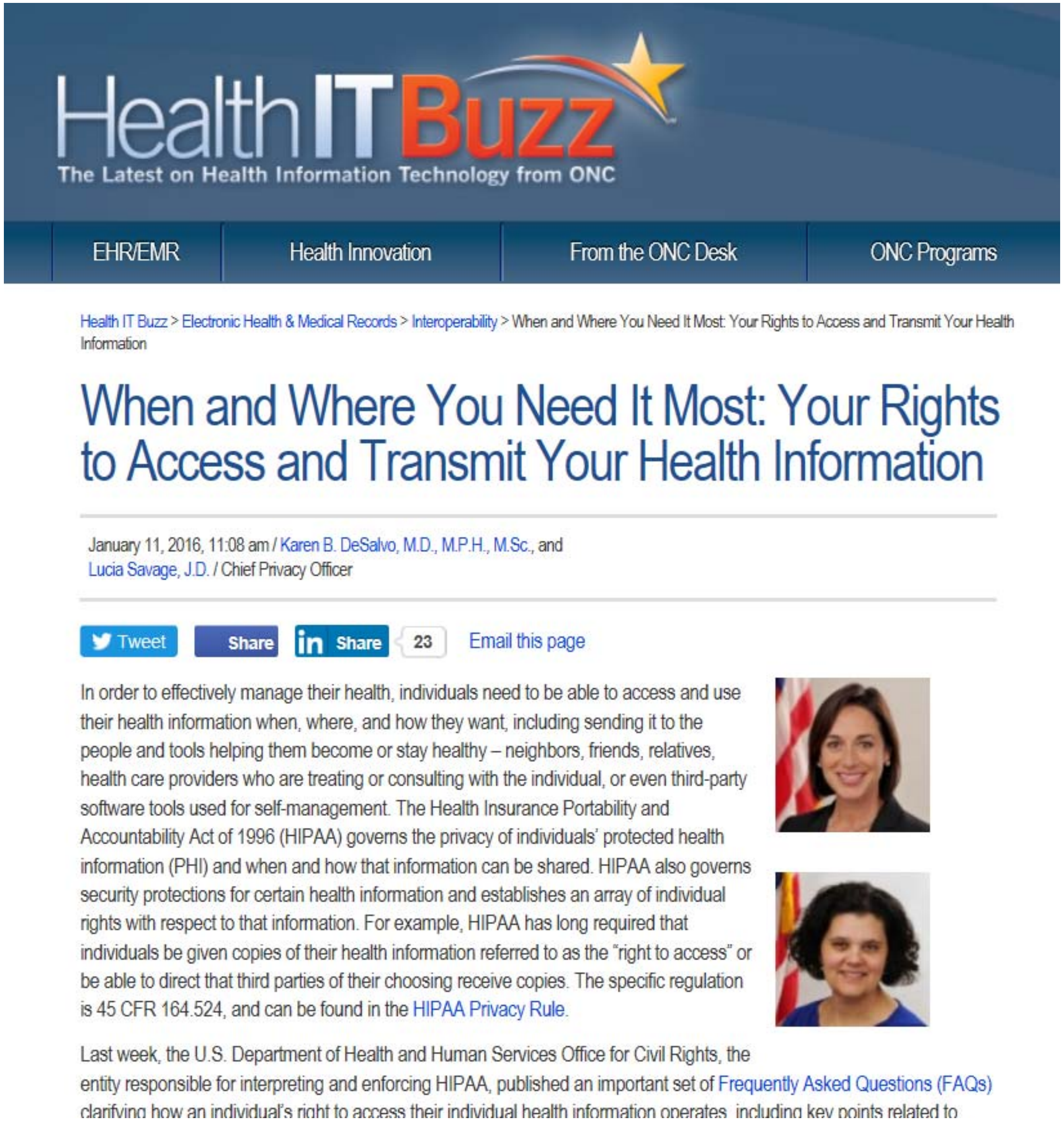
Introduction

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 > 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

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 at HHS OCR ACCESS GUIDANCE

Fact Sheet/FAQs

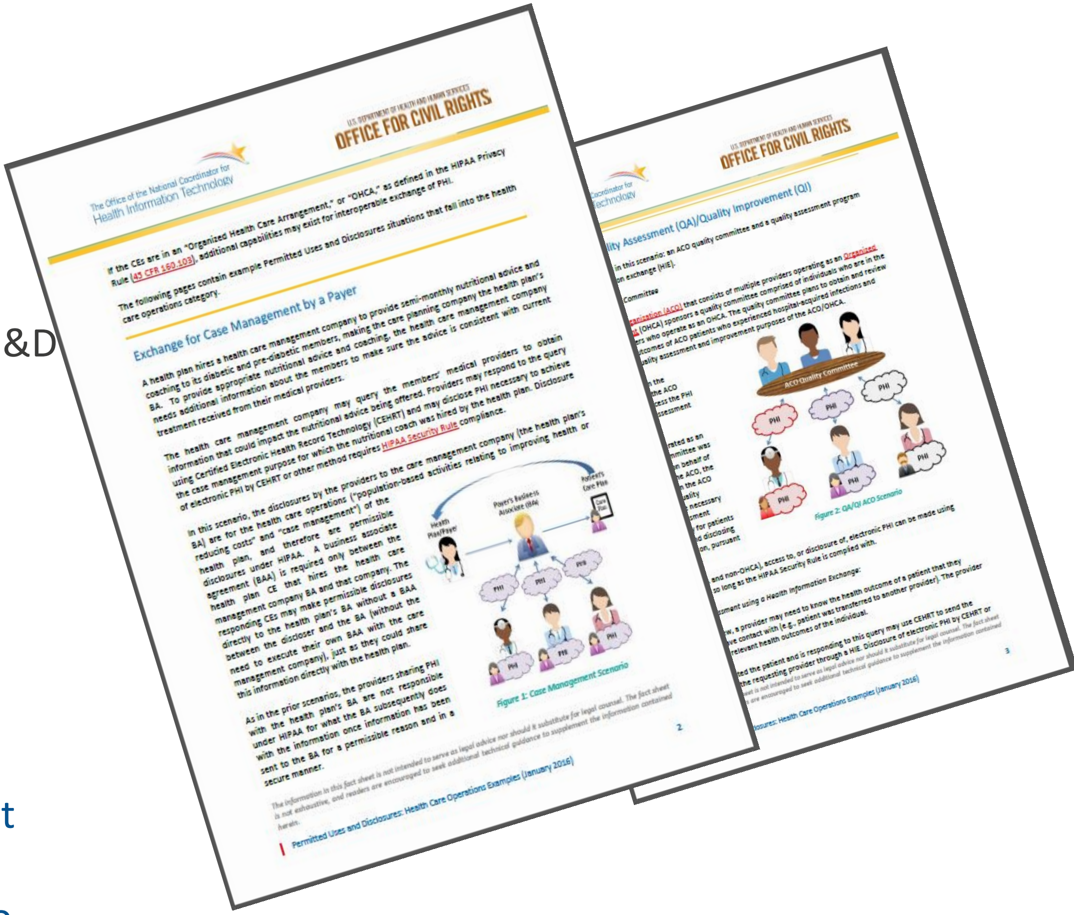
- Scope
- Form and Format and Manner of Access
- Timeliness
- Other (Clinical Labs)
- Fees
- Direct that a copy be transmitted to a third party, including an app.

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 on January 7. Key concepts for apps and APIs
  - Timing
  - Automation
  - Electronic formats
- 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.



The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

If the CEs are in an “Organized Health Care Arrangement,” or “OHCA,” as defined in the HIPAA Privacy Rule (45 CFR 160.103), additional capabilities may exist for interoperable exchange of PHI.

The following pages contain example Permitted Uses and Disclosures situations that fall into the health care operations category.

Exchange for Case Management by a Payer

A health plan hires a health care management company to provide semi-monthly nutritional advice and coaching to its diabetic and pre-diabetic members, making the care planning company the health plan’s BA. To provide appropriate nutritional advice and coaching, the health care management company needs additional information about the members to make sure the advice is consistent with current treatment received from their medical providers.

The health care management company may query the members’ medical providers to obtain information that could impact the nutritional advice being offered. Providers may respond to the query using Certified Electronic Health Record Technology (CEHRT) and may disclose PHI necessary to achieve the case management purpose for which the nutritional coach was hired by the health plan. Disclosure of electronic PHI by CEHRT or other method requires HIPAA Security Rule compliance.

In this scenario, the disclosures by the providers to the care management company (the health plan’s BA) are for the health care operations (“population-based activities relating to improving health or reducing costs” and “case management”) of the health plan, and therefore are permissible disclosures under HIPAA. A business associate agreement (BAA) is required only between the health plan CE that hires the health care management company BA and that company. The responding CEs may make permissible disclosures directly to the health plan’s BA without a BAA between the discloser and the BA (without the need to execute their own BAA with the care management company), just as they could share this information directly with the health plan.

Figure 1: Case Management Scenario

As in the prior scenarios, the providers sharing PHI with the health plan’s BA are not responsible under HIPAA for what the BA subsequently does with the information once information has been sent to the BA for a permissible reason and in a secure manner.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Permitted Uses and Disclosures: Health Care Operations Examples (January 2016)

2

Coordinator for
Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

lity Assessment (QA)/Quality Improvement (QI)

in this scenario: an ACO quality committee and a quality assessment program
on exchange (HIE).

Committee

anization (ACO) that consists of multiple providers operating as an Organized
nt (OHCA) sponsors a quality committee comprised of individuals who are in the
ers who operate as an OHCA. The quality committee plans to obtain and review
utcomes of ACO patients who experienced hospital-acquired infections and
uality assessment and improvement purposes of the ACO/OHCA.

n the
the ACO
cess the PHI
ssessment

rated as an
mmittee was
n behalf of
he ACO, the
n the ACO
uality
necessary
sment
for patients
d disclosing
on, pursuant

Figure 2: QA/QI ACO Scenario

and non-OHCA), access to, or disclosure of, electronic PHI can be made using
so long as the HIPAA Security Rule is complied with.

sment using a Health Information Exchange:

w, a provider may need to know the health outcome of a patient that they
ve contact with (e.g., patient was transferred to another provider). The provider
relevant health outcomes of the individual.

ted the patient and is responding to this query may use CEHRT to send the
the requesting provider through a HIE. Disclosure of electronic PHI by CEHRT or

eet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet
s are encouraged to seek additional technical guidance to supplement the information contained

losures: Health Care Operations Examples (January 2016)

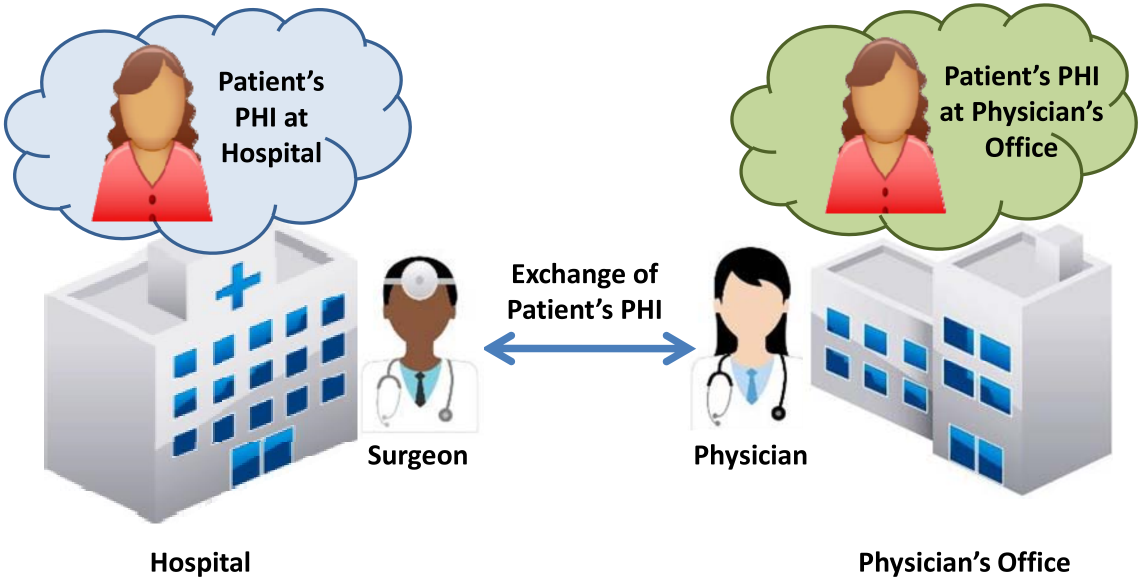
3

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 Permitted Uses and Disclosures (PU&D)?

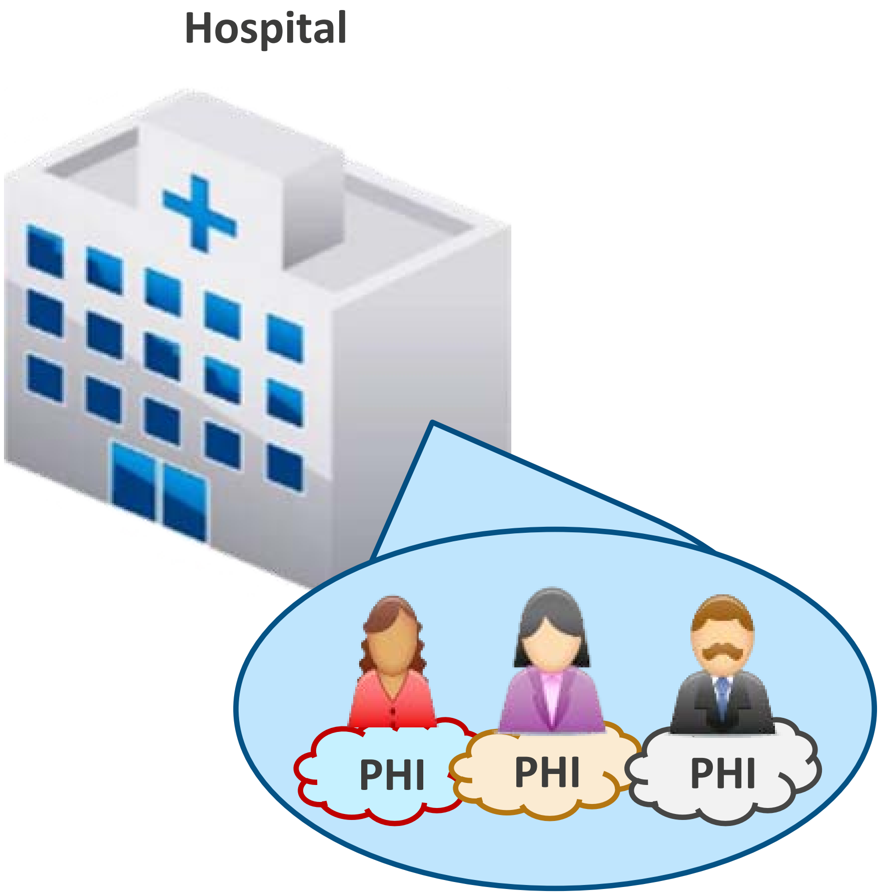
- Permitted Uses and Disclosures (PU&D) are situations in which a covered entity is permitted, but not required, to use and disclose PHI without first having to obtain a written authorization from the patient.

Basic Illustration of Permitted Uses


Patient's PHI at Hospital
Patient's PHI at Physician's Office
Exchange of Patient's PHI
Surgeon
Physician
Hospital
Physician's Office

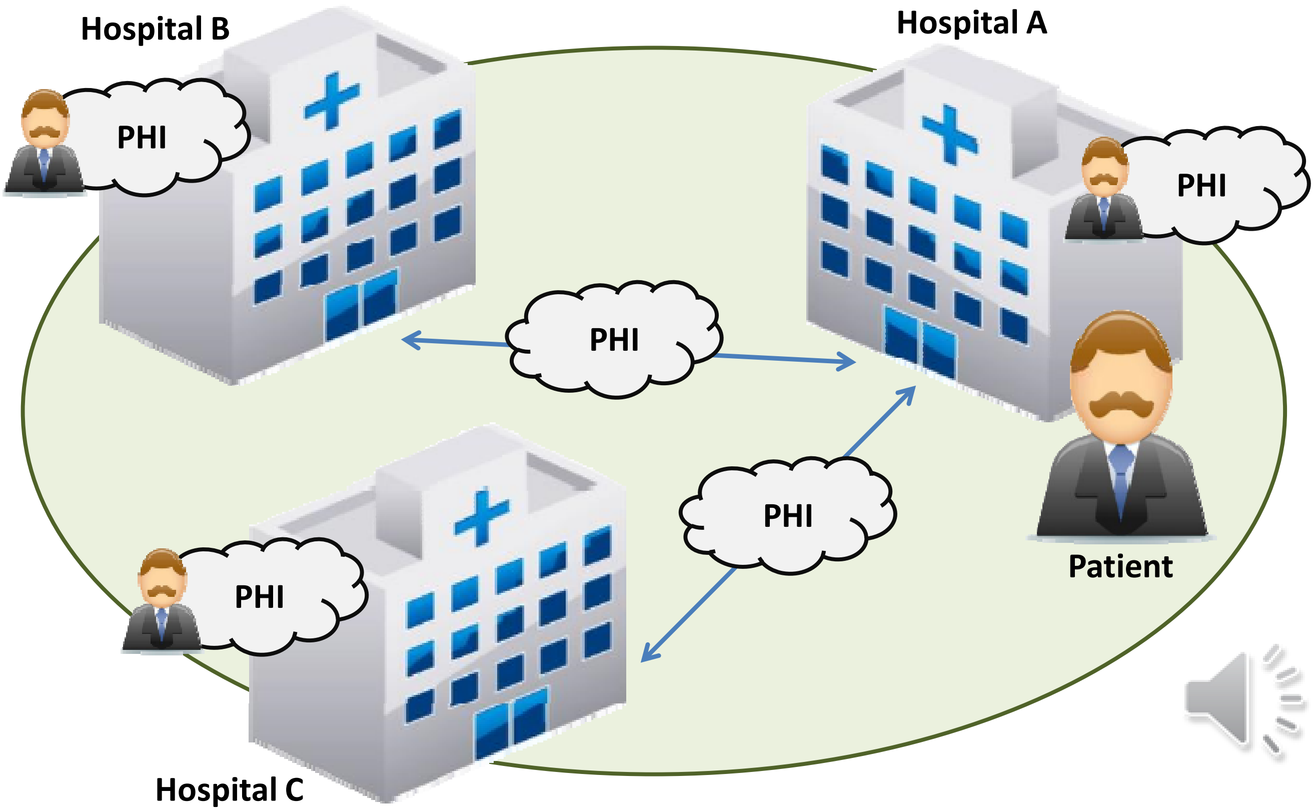
What types of activities are considered Permitted Uses and Disclosure ?

- 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



Scenario 1: Health Care Operation – Quality Improvement for Population Based Activities

Population-Based Activities



HIPAA Permitted Uses Drill Down

- MYTH: HIPAA makes it impossible to exchange health information electronically for patient care
- FACT: HIPAA permitted uses actually *allow* health information to be exchanged in a number of specific circumstances
  - Providers can share PHI for **treatment**, broadly defined to include things like referrals, care management by someone hired by the provider, or transitions of care
  - Providers and payers can share PHI for **operations** such as quality improvement, care coordination and other activities
  - Under HIPAA, this type of sharing does not require a written patient authorization; however, other laws or organizational policies may impose such requirements.
  - Information can be shared electronically, supporting interoperability and making **information available to the right people at the right time for patient care**
- ONC is releasing **fact sheets** and a series of **blog posts** with numerous examples of when electronic health information can be exchanged

Permitted Uses Drill Down: Key Concepts for Exchange between Covered Entities

- "*May*" = discretion
  - Lawyers call it "permitted uses or disclosures"
  - Permitted is a key concept: it is the Covered Entity's choice
  - BAs can undertake the disclosure function on CEs behalf
    - E.g. HIEs
- Minimum necessary applies
- What is permitted:
  - Access, use and disclosure for a covered entity's own treatment, payment or health care operations
  - Access and use by another CE, or disclosure to the other CE, for the recipient CE's treatment, payment or health care operations

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 CEHRT Requirements

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

APIs in the 2015 Edition Certification Rule

- Three API criteria
  - Lookup a patient
  - Retrieve part of a patient record
  - Retrieve an entire patient record
- Required security criteria
  - Authentication, authorization, & access control
  - Auditing
  - Encryption

“Transmit” in the 2015 Edition Certification Rule

- VDT = View, Download, Transmit
- In 2015, new method to satisfy “transmit” criteria (must have capabilities for both):
  - Unencrypted option – Used at patient direction to email to a patient-specified email address
    - Cannot be used for provider-to-provider exchange; only for patient-directed movement
  - Encrypted option – an encrypted method identified by the HIT developer (e.g., Direct, encrypted email, etc.)

ONC API Task Force: Addressing Privacy & Security Concerns about Open APIs

- **Identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in healthcare**
  - » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example, identity proofing and authentication are not unique to APIs*)
- **Identify perceived privacy concerns and real privacy risks that are barriers to the widespread adoption of open APIs in healthcare**
  - » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example, harmonizing state law and misunderstanding of HIPAA*)
- **Identify priority recommendations for ONC that will help enable consumers to leverage API technology to access patient data, while ensuring the appropriate level of privacy and security protection**

API TF testimony - Important Facts Shared on APIs

- API Resources can regulate how, when, and who uses the API
- APIs provide a well-documented, popular way for organizations to share access to data and services with third parties, while maintaining strict security controls.
  - Clear and Concise documentation is important for open standard APIs
- API is extremely precise and allows the opportunity for all the right levels of access and security, e.g. data granularity
- Technical solutions exist for technical problems
- Need consensus best practices to help secure the API
- Business & legal considerations may remain.
  - Does it matter if the discloser “owns” the PHI or not?
  - Provider liability and accountability for data usage and breach, even though OCR/ONC Fact sheets say a discloser is not liable for what a receiver does with data so long as the discloser discloses the data properly.

API TF testimony – Consumer Perspective

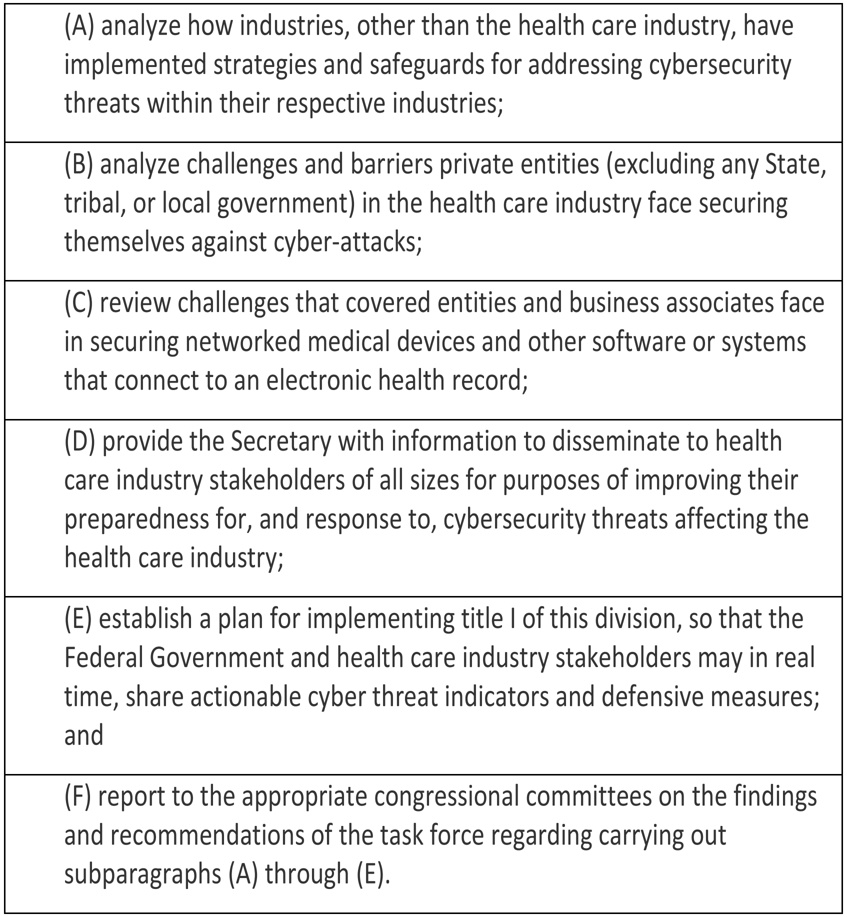
- More Access, More Patient Control, More Engagement
  - ✓ A panelist indicated access to his data helped save his own life, and asked “why can’t patients have access to more of their own data?”
- Choices should be given to patient, and patients are smart enough to make privacy & security choices that are right for them.
- Systems should account for diverse consumers:
  - » Some want personally to control every decision
  - » Some want health information to move where it needs to go without them having to manage that process
  - » Language needs and literacy levels vary
- Transparent data practices are important for consumers
- Role of HIPAA in protecting consumer vs. protections outside HIPAA
- Recordings/transcripts available here:
  - » Jan 26: https://www.healthit.gov/facas/calendar/2016/01/26/api-task-force-virtual-hearing
  - » Jan 28: https://www.healthit.gov/facas/calendar/2016/01/28/api-task-force-virtual-hearing

API TF testimony – Healthcare Organizations

- Support for Open Standards-based APIs.
- Who do you trust? How do you know that person is accessing your system?
  - Need to verify identity of person accessing system, even through an app.
  - Need to verify that the app is operating on behalf of a verified person
  - Who is accessing and which apps are in use varies by role
    - Patient/individual/caregiver
    - Provider
    - Information systems administrator
- Long term, protections will be in place to allow for varying levels of access.
- Business and legal issues.

Cyber Information Sharing Act of 2015

- Section 405(c) requires that HHS establish by March 17, 2016 a Health Care Sector Cybersecurity Task Force.
- Charged to



(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber-attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing title I of this division, so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

Open for Comment: Model Privacy Notice: Improving Transparency for Consumers

- What is the Model Privacy Notice?
  - Provides a standardized, easy-to-use framework to help developers clearly convey information about privacy and security practices to their users
  - ***Voluntary, openly available resource for developers and consumers***
- Why we're updating the MPN:
  - The 2011 version focused on Personal Health Records (PHRs), which were the emerging technology at the time
  - We plan to update the MPN to make it applicable to a broad range of consumer health technologies—beyond just PHRs
- For more information and to comment, visit:
  - Request for Information: https://federalregister.gov/a/2016-04239
  - ONC blog: https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/model-privacy-notice/
- Comment period closes 5 pm eastern on April 15, 2016

Open for Comment: ONC Health IT Certification Program: Enhanced Oversight and Accountability

- NPRM found at: https://www.federalregister.gov/articles/2016/03/02/2016-04531/onc-health-it-certification-program-enhanced-oversight-and-accountability
- Comments due by 5 pm eastern May 2, 2016
- The proposed rule would focus on three key areas:
- **Direct Review:** Enabling ONC to directly review certified health IT products, including certified electronic health records systems (EHRs), and take necessary action to address circumstances such as potential risks to public health and safety. This will complement existing ONC-Authorized Certification Bodies (ONC-ACBs) responsibilities.
- **Enhanced Oversight:** Increasing ONC oversight of health IT testing bodies to align with ONC's existing oversight of ONC-ACBs and provide the means for ONC to quickly, directly, and precisely address testing issues.
- **Greater Transparency and Accountability:** Making identifiable surveillance results of certified health IT publicly available to provide customers and users with valuable information about the overall performance of certified health IT, including illuminating good performance and continued compliance.

Additional Resources

2015 Edition Final Rule: Supporting the Needs of Diverse Consumers

Certification Criteria	What the Functionality Can Support
Documentation of social, psychological, and behavioral data (e.g., education level, stress, depression, alcohol use, sexual orientation and gender identity)	Allow providers and other stakeholders to better understand how these data can affect health, reduce disparities, and improve patient care and health equity
Exchange of sensitive health information (data segmentation for privacy)	Allow for the exchange of sensitive health information (e.g., behavioral health, substance abuse, genetic), in accordance with federal and state privacy laws, for more coordinated and efficient care across the continuum.
Accessibility of health IT	More transparency on the accessibility standards used in developing health IT
More granular recording and exchange of patient race and ethnicity	Allow providers to better understand health disparities based on race and ethnicity, and improve patient care and health equity.

OCR Patient Access Guidance and Related Blog Posts

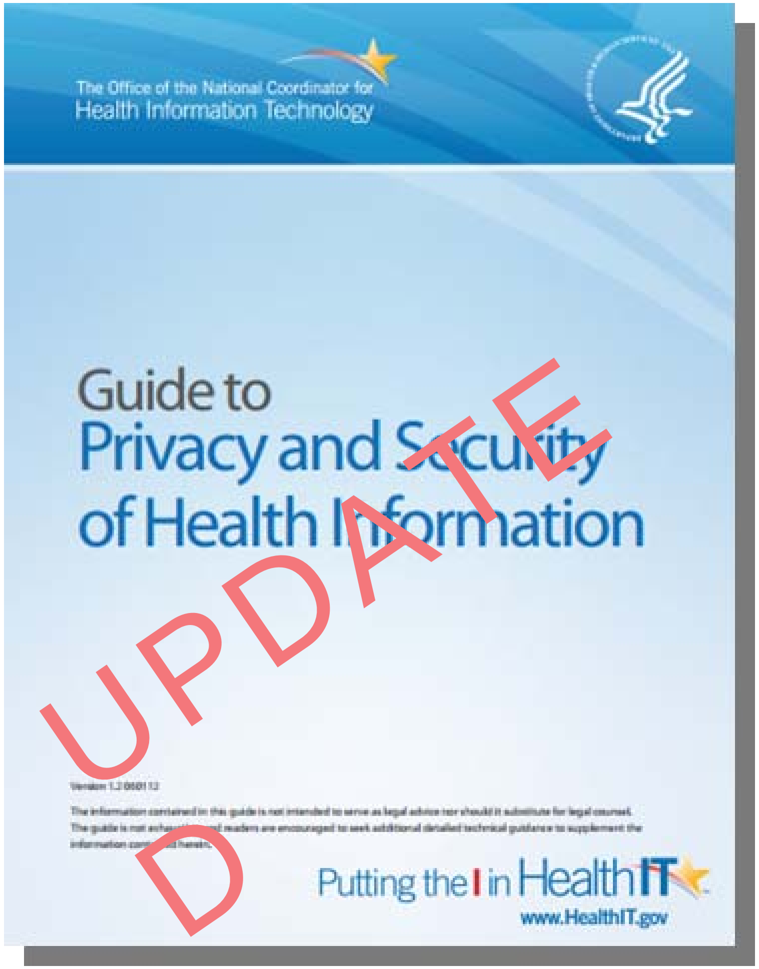
- OCR Patient Access Guidance
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- OCR Patient Access Blog Post
  - http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html#
- ONC Patient Access Blog Post
  - http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/your-rights-to-access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

Guide to Privacy and Security Of Health Information – Version 2.0

April 2015 Updated Guide focuses on:

- Privacy and security requirements for EHR Certification Criteria - 2014 Edition
- Updated privacy and security requirements resulting from HIPAA modifications
- New, practical examples of the HIPAA Privacy and Security Rules in action

Developed in coordination with HHS Office for Civil Rights and Office of General Counsel



The Office of the National Coordinator for
Health Information Technology

Guide to
Privacy and Security
of Health Information

Version 1.2 060112

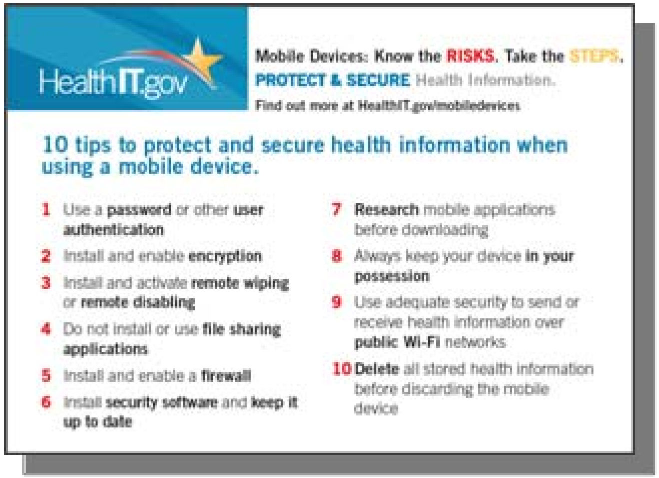
The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in Health IT
www.HealthIT.gov

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Mobile Device Materials Available Online

- Materials available on **HealthIT.gov/mobiledevices** include:
  - Fact sheets
  - Posters
  - Brochures
  - Postcard
  - Educational videos


HealthIT.gov

Mobile Devices: Know the **RISKS**. Take the **STEPS**.
PROTECT & SECURE Health Information.
Find out more at HealthIT.gov/mobiledevices

10 tips to protect and secure health information when using a mobile device.

1. Use a **password** or other **user authentication**
2. Install and enable **encryption**
3. Install and activate **remote wiping** or **remote disabling**
4. Do not install or use **file sharing applications**
5. Install and enable a **firewall**
6. Install **security software** and **keep it up to date**
7. **Research** mobile applications before downloading
8. Always keep your device **in your possession**
9. Use adequate security to send or receive health information over **public Wi-Fi** networks
10. **Delete** all stored health information before discarding the mobile device

Mobile Devices:
Know the **RISKS**.
Take the **STEPS**.
PROTECT and SECURE
Health Information.

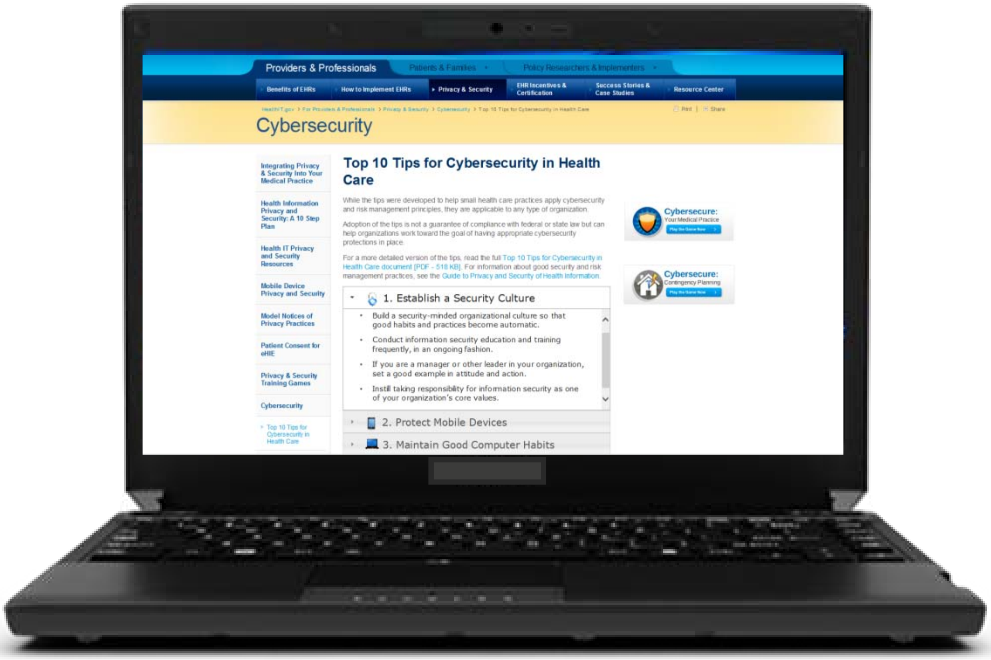
Is your information protected? Mobile devices are easily lost or stolen. Avoid losing or disclosing patient health information. Keep your mobile device with you.
Learn more at HealthIT.gov/mobiledevices.

Be a team player.
Understand and follow your organization's mobile device policy and procedures.
It's your responsibility.
Visit HealthIT.gov/mobiledevices

Mobile Devices:
Know the **RISKS**.
Take the **STEPS**.
PROTECT and SECURE
Health Information.

Cybersecurity Web Pages

- Cybersecurity Resources for the Health Care Sector
- Link to National Institute of Standards and Technology (NIST) Cybersecurity Framework


Providers & Professionals
Patients & Families
Policy Researchers & Implementers
Benefits of EHRs
How to Implement EHRs
Privacy & Security
EHR Incentives & Certification
Success Stories & Case Studies
Resource Center
HealthIT.gov > For Providers & Professionals > Privacy & Security > Cybersecurity > Top 10 Tips for Cybersecurity in Health Care
Print
Share
Integrating Privacy & Security Into Your Medical Practice
Health Information Privacy and Security: A 10 Step Plan
Health IT Privacy and Security Resources
Mobile Device Privacy and Security
Model Notices of Privacy Practices
Patient Consent for eHIE
Privacy & Security Training Games
Cybersecurity
Top 10 Tips for Cybersecurity in Health Care
Cybersecure: Your Medical Practice
Play the Game Now
Cybersecure: Contingency Planning
Play the Game Now

Cybersecurity

Top 10 Tips for Cybersecurity in Health Care

While the tips were developed to help small health care practices apply cybersecurity and risk management principles, they are applicable to any type of organization.

Adoption of the tips is not a guarantee of compliance with federal or state law but can help organizations work toward the goal of having appropriate cybersecurity protections in place.

For a more detailed version of the tips, read the full Top 10 Tips for Cybersecurity in Health Care document [PDF - 518 KB]. For information about good security and risk management practices, see the Guide to Privacy and Security of Health Information.

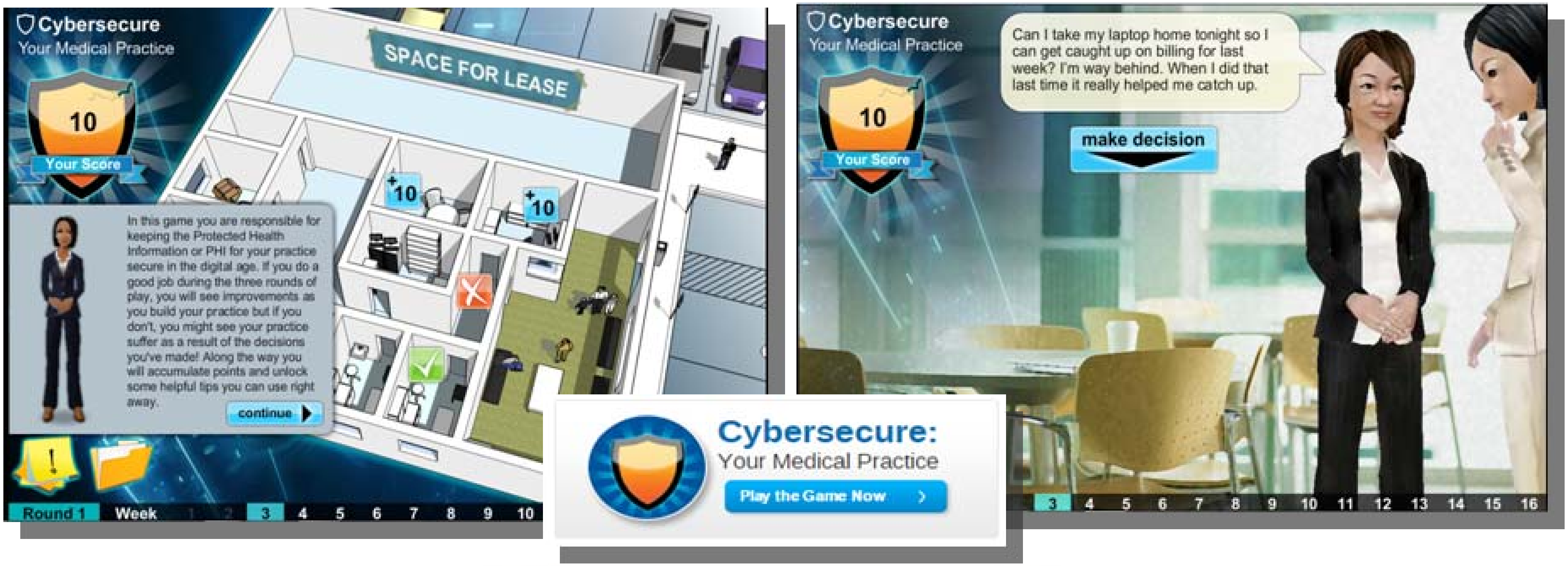
1. Establish a Security Culture
   - Build a security-minded organizational culture so that good habits and practices become automatic.
   - Conduct information security education and training frequently, in an ongoing fashion.
   - If you are a manager or other leader in your organization, set a good example in attitude and action.
   - Instill taking responsibility for information security as one of your organization's core values.
2. Protect Mobile Devices
3. Maintain Good Computer Habits

http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility

The Office of the National Coordinator for Health Information Technology

Cybersecure: Medical Practice

A training game that requires users to respond to privacy and security challenges often faced in a typical small medical practice.



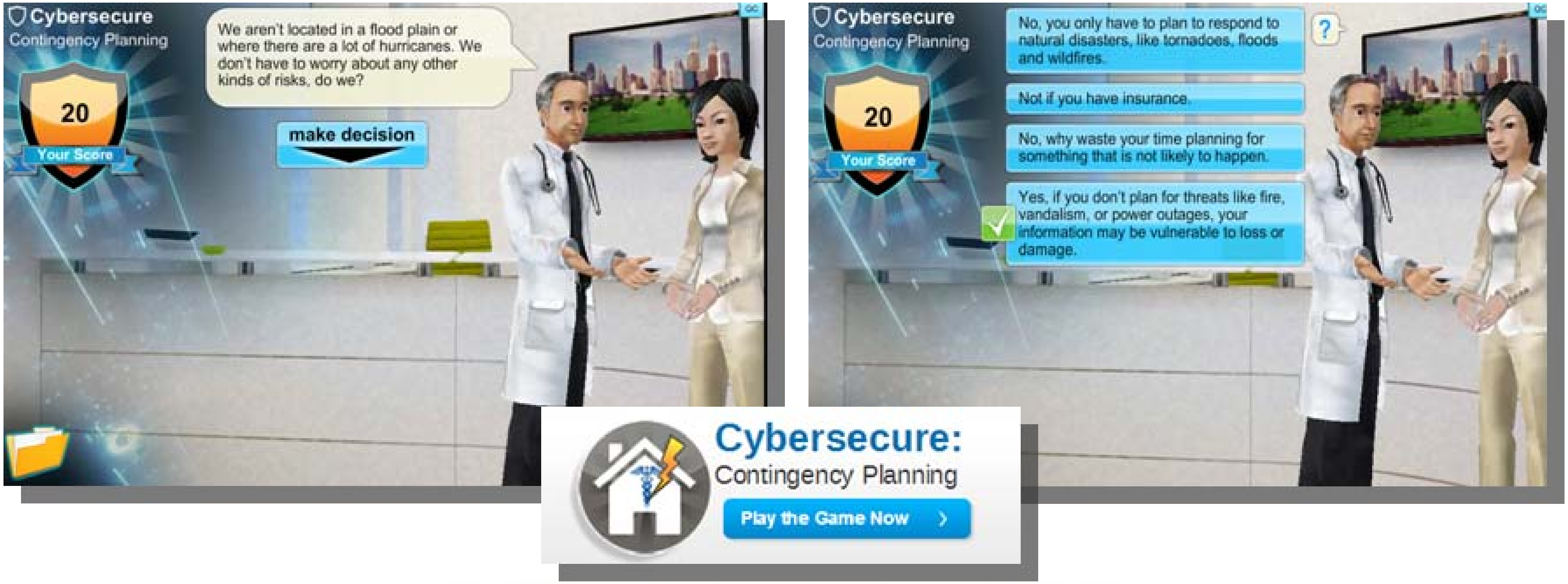
In this game you are responsible for keeping the Protected Health Information or PHI for your practice secure in the digital age. If you do a good job during the three rounds of play, you will see improvements as you build your practice but if you don't, you might see your practice suffer as a result of the decisions you've made! Along the way you will accumulate points and unlock some helpful tips you can use right away.

Can I take my laptop home tonight so I can get caught up on billing for last week? I'm way behind. When I did that last time it really helped me catch up.

http://www.healthit.gov/providers-professionals/privacy-security-training-games

Cybersecure: Contingency Planning

The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.



We aren't located in a flood plain or where there are a lot of hurricanes. We don't have to worry about any other kinds of risks, do we?

No, you only have to plan to respond to natural disasters, like tornadoes, floods and wildfires.

Not if you have insurance.

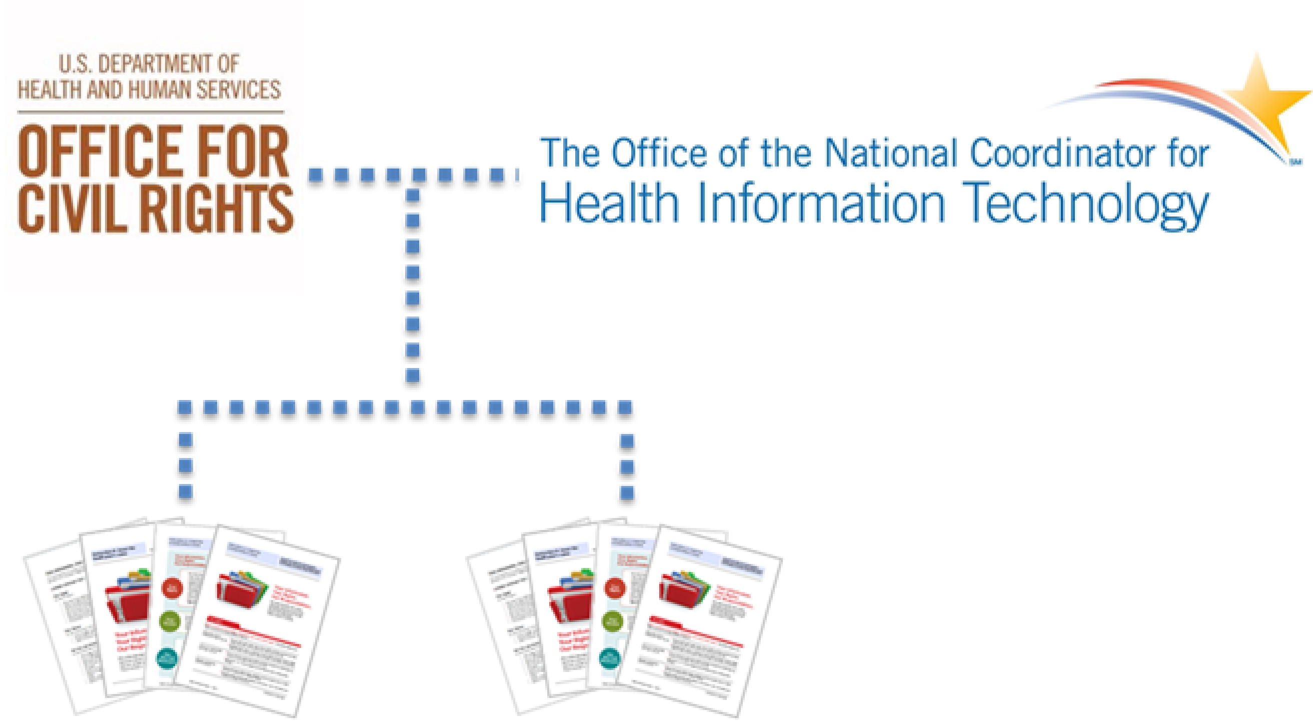
No, why waste your time planning for something that is not likely to happen.

✓ Yes, if you don't plan for threats like fire, vandalism, or power outages, your information may be vulnerable to loss or damage.

http://www.healthit.gov/providers-professionals/privacy-security-training-games

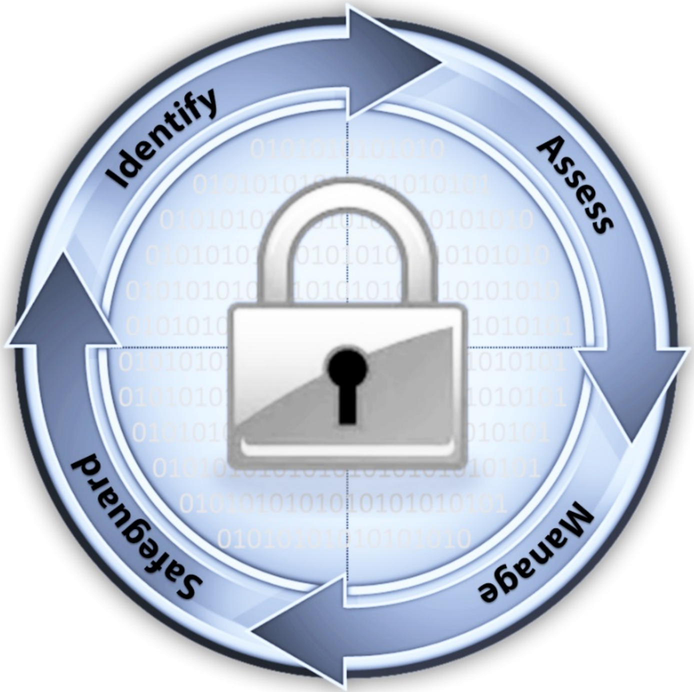
Models of Notice of Privacy Practices

The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:


U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS
The Office of the National Coordinator for Health Information Technology

- ✓ One set for health plans
- ✓ One set for health care providers

HHS Security Risk Assessment (SRA) Tool



- Downloadable SRA Tool designed to guide providers through the Risk Assessment process.
- Tool includes resources to:
  - explain the context of the question,
  - provide examples of potential impacts to PHI, if requirements are not met
  - identify examples of safeguards to help mitigate identified risks and vulnerabilities

www.HealthIT.Gov/Security-Risk-Assessment

Data Segmentation Resources and Website

- ONC successfully completed a three year project (the Data Segmentation for Privacy initiative) which developed and piloted standards to help integrate behavioral health-related information into the primary care setting.
- The HIT Policy Committee approved recommendations that the DS4P document-level standards be included as voluntary Certified EHR Technology (CEHRT) for Meaningful Use Program Stage 3.
- The information (including the balloted standards) is available on the healthit.gov website.

http://www.healthit.gov/providers-professionals/data-segmentation-and-you

Additional Information and Resources

- **2015 Edition Final Rule**: https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-certification-criteria-2015-edition-base-electronic
  - The 2015 Edition final rule provisions become **effective on January 14, 2016**, except for § 170.523(m) (adaptations/updates reporting) and (n) (complaints reporting), which are **effective on April 1, 2016**.
  - There is **no** comment period for this final rule.

- **For more information and guidance on the 2015 Edition Final Rule, please visit**: https://www.healthit.gov/policy-researchers-implementers/2015-edition-final-rule

- **2015 Edition Final Rule Test Procedures and Certification Companion Guides**: The 2015 Edition Test Method has been constructed in an outcome-focused format with additional companion guide documents to aid stakeholder development of Health IT Modules. The Certification Companion Guides are not undergoing a formal public comment period, but ONC will accept ongoing feedback. https://www.healthit.gov/policy-researchers-implementers/2015-edition-test-method

- **ONC Regulations**: https://www.healthit.gov/policy-researchers-implementers/health-it-regulations