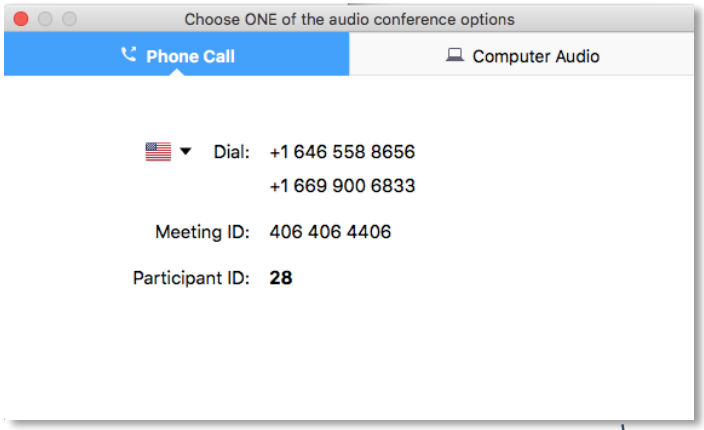
Patient Rights, Information Blocking and HIPAA

Presented by: Susan Clarke,
Health Care Information
Security and Privacy Practitioner
1PM, March 26, 2019

Zoom tips and tricks!



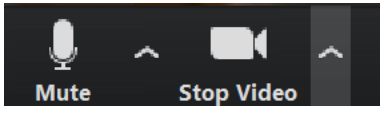
CHAT: Please jump in if you have something to share, but we also have this nifty chat function.

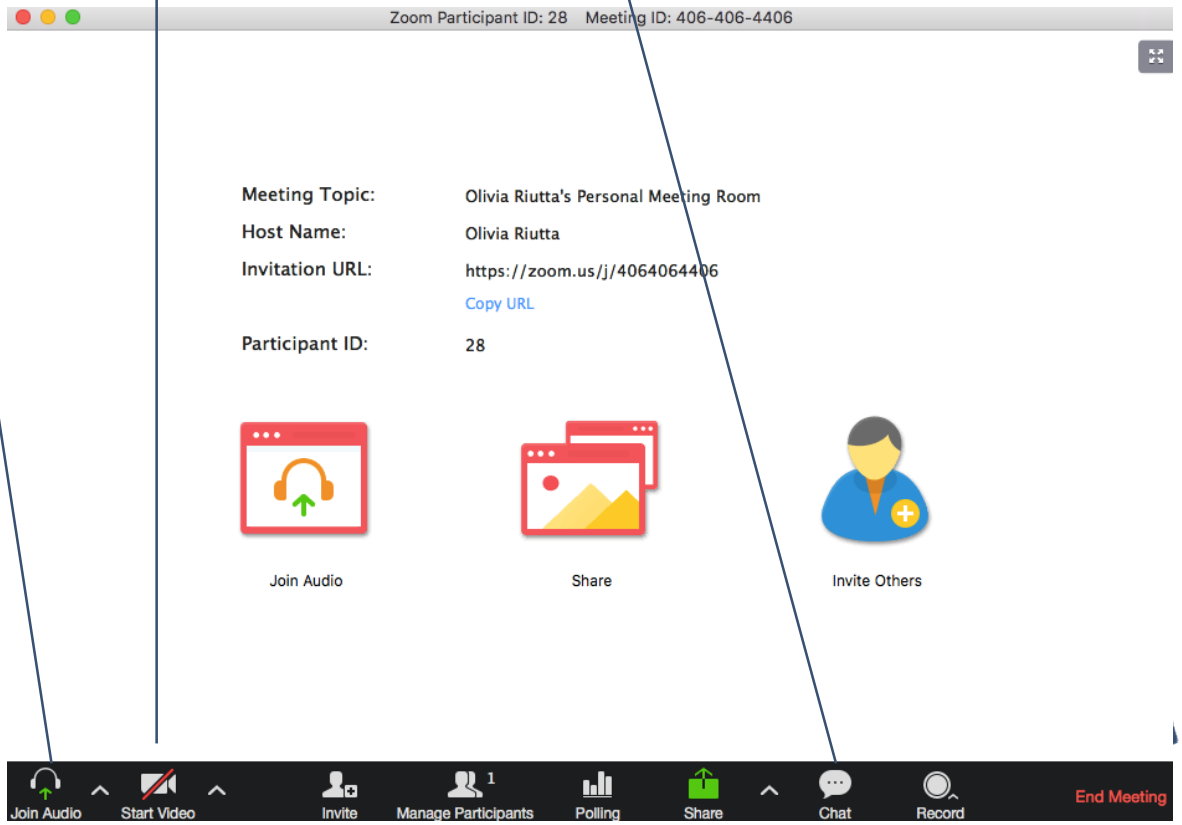
ATTENDANCE: If there are multiple attendees together on the call, please list the names and your location in the chat box

VIDEO: We want to see you! If your camera isn't on, start your video by clicking here.

AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click "Join Audio," this "Choose one…" box will pop up. If you dial in, just make sure you include your audio code.

MUTE/UNMUTE: *6 or click the mic on the bottom left of your screen.





Susan Clarke, HCISPP

- $(ISC)^2$ certified Healthcare Information Security and Privacy Practitioner and Computer Scientist.
- 20 years of Healthcare Experience.
- 10 years design and coding EHR software including HL7 Healthcare application development.
- Served on IT Security, Disaster Recovery and Joint Commission steering committee at Mayo Clinic affiliated Healthcare system.
- Served as communications unit lead during Healthcare system's ready and complete alerts.

Mountain-Pacific

Mountain-Pacific Quality Health is a private, non-profit, community-based organization that has dedicated more than three decades to improving health and health care in: Alaska, Hawaii (including some U.S. Pacific Territories), Montana and Wyoming. Our goal is to increase access to high-quality health care that is affordable, safe and of value to the patients we serve.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users patient needs.

Acronyms…

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis

Agenda

- Origin of data blocking
- Examples of data blocking
- HIPAA privacy rule review.
- Permitted and authorized disclosures.
- Rights of patients under HIPAA.
- Q&A

FOR IMMEDIATE RELEASE
February 11, 2019

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Proposes New Rules to Improve the Interoperability of Electronic Health Information

New innovations in technology promote patient access and could make no-cost health data exchange a reality for millions

The U.S. Department of Health and Human Services (HHS) today proposed new rules to support seamless and secure access, exchange, and use of electronic health information. The rules, issued by the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC), would increase choice and competition while fostering innovation that promotes patient access to and control over their health information. The proposed ONC rule would require that patient electronic access to this electronic health information (EHI) be made available at no cost.

https://www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health

Information Blocking

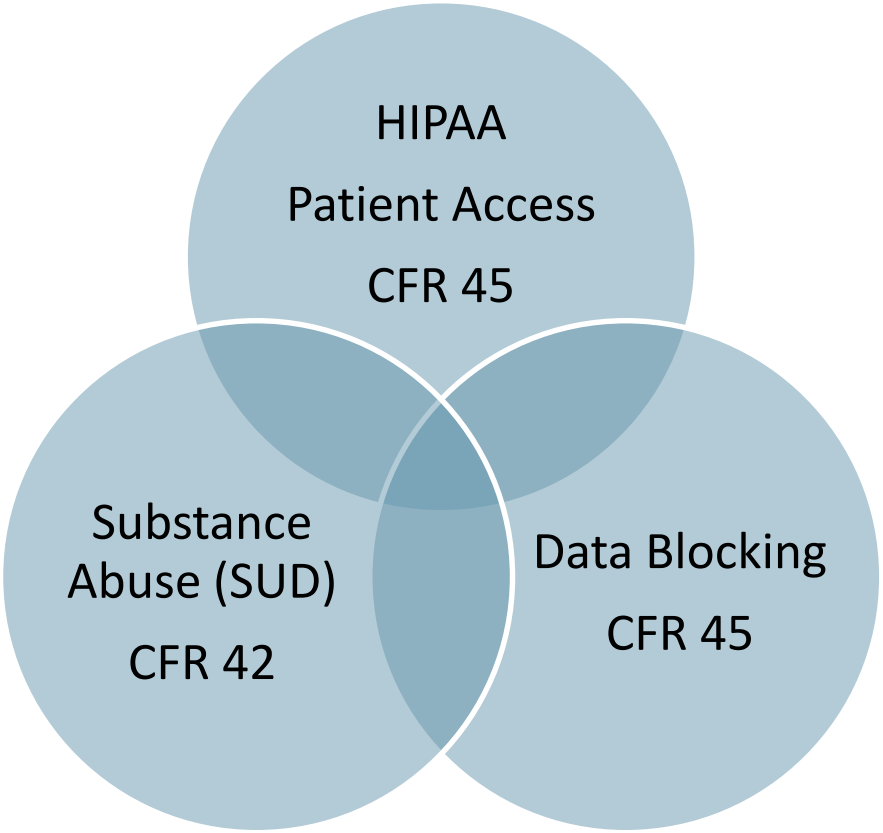
Health IT Legislation

21st Century Cures Act

There are many provisions of the 21st Century Cures Act (Cures Act) that will improve the flow and exchange of electronic health information. ONC is responsible for implementing those parts of Title IV, *delivery*, related to advancing interoperability, prohibiting information blocking, and enhancing the usability, accessibility, and privacy and security of health IT. ONC works to ensure that all individuals, their families and their health care providers have appropriate access to electronic health information to help improve the overall health of the nation's population.

In addition to supporting medical research, advancing interoperability, clarifying HIPAA privacy rules, and supporting substance abuse and mental health services, the Cures Act defines interoperability as the ability exchange and use electronic health information without special effort on the part of the user and as not constituting information blocking.

How are HIPAA, SUD, and Information Blocking Regulations Related?



What is Information Blocking?

Information blocking occurs when a person or entity – typically a health care provider, IT developer, or EHR vendor – knowingly and unreasonably interferes with the exchange and use of electronic health information, which is a right protected by the HIPAA.

https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_InformationBlockingFact-Sheet20171106.pdf

HIMSS Feb 2019

"A new rule issued today by the Office of the National Coordinator for Health Information Technology involves the patient, not as a person being "acted upon," said Elise Sweeney Anthony, director of Office of Policy for the ONC, but as someone in control of his or her electronic health records.

If a patient requests their record, and it's not given to them electronically and for free, that's information blocking, Sweeney said during HIMSS19.

The Centers for Medicare and Medicaid Services would also require that healthcare providers and plans implement open data sharing technologies to support transitions of care as patients move between these plan types"

Examples of Information Blocking

- Fees that make data exchange cost prohibitive.
- Organizational policies or contract terms that prevent sharing information with patients or health care providers.
- Technology is designed or implemented in non-standard ways that inhibit the exchange of information.
- Patients or health care providers become “locked in” to a specific technology or health care network because data is not portable.

Not Information Blocking

Example: Health care providers restrict access to a patient's sensitive test results until the clinician who ordered the tests, or another designated health care professional, has reviewed and appropriately communicated the results to the patient.

(Keeping with the HIPAA Privacy Rule, the restriction does not apply to the patient or to anyone else to whom the patient has requested in writing to provide this information.)

Patient Safety Comes First

- Some actions that impede the exchange of electronic health information do not constitute information blocking. For example, when an act or course of action is necessary to protect patient safety, privacy, or other compelling interests.
- As long as the restrictions imposed by the health care provider were based on the health care provider's patient assessment of their patient's best interests (rather than a blanket policy) and were not an excuse for restricting health information exchange.

FEDERAL REGISTER

The Daily Journal of the United States Government

PR Proposed Rule

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

A Proposed Rule by the Health and Human Services Department on 03/04/2019

This document has a comment period that ends in 39 days. (05/03/2019)

SUBMIT A FORMAL COMMENT

https://www.federalregister.gov/documents/2019/03/04/2019-02224/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification

Understanding Some of HIPAA's Permitted Uses and Disclosures

- Health records are used and share to provide good care to patients, to evaluate the quality of care and to assure proper payment from health plans.
- Relevant players in the health care system – including the patient – need to be able to quickly and easily access health records to make decisions, and to provide the right care at the right time
- The Privacy, Security, and Breach Notification Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) were intended to support information sharing by providing assurance that sensitive health records would be maintained securely and shared only for appropriate purposes or with express authorization of the patient.
- Although the regulations have been in effect for quite some time, health care providers frequently still question whether the sharing of health information, even for routine purposes like treatment or care coordination, is permissible under HIPAA.
- Confusion about the rules has been cited by many as a potential obstacle to interoperability of digital health information.

Patient Rights

- Notice of Privacy Practices
- Access: inspect and copy
- Amendment
- Accounting
- Alternative communications
- Request restriction
- Complaints to Covered Entity and Secretary

Patient Amendment

A patient has the right to request that a covered entity (CE) amend protected health information (PHI) about the patient in a designated record set [DRS] as long as the DRS is maintained.

45 CFR § 164.526

Patient Accounting

A patient has the right to receive an accounting of disclosures of PHI made by a covered entity in the six years or less prior to the request.

45 CFR § 164.528

Alternative Communication for Patients

- A covered health care provider must permit the patient to request and must accommodate reasonable requests to receive communications of PHI by alternative means and at alternative locations.

- The requirement applies to health plans if the patient clearly states that the disclosure could endanger the patient.

45 CFR § 164.522(b)

Patient Right to Request Restrictions

- A covered entity must permit a patient to request that the covered entity restrict uses and disclosures of PHI for treatment, payment, or health care operations purposes, and for disclosures to family and friends (opportunity to agree or object disclosures).

- Covered entities are not required to agree to the request (unless to a health plan under certain circumstances).

45 CFR § 164.522(a)

Patient Right to Request Restrictions

- Covered entity must agree to patient's request to restrict disclosure of PHI to health plan if:
  - PHI pertains solely to health care for which patient (or person on behalf of patient other than health plan) has paid the covered entity in full out of pocket
  - Disclosure is not required by other law

45 CFR § 164.522(a)

Patient Right to Request Restrictions

Scope of restriction to health plan extends to health care item or service paid for out of pocket

- Restriction on follow-up care – patient must pay out of pocket and request restriction for follow-up care
- Restriction on downstream providers – patient has obligation to request restriction from downstream providers but providers encouraged to assist patient in notifying downstream providers of patient's desire to restrict

Patient Right to Request Restrictions

- Can't require patient to restrict all or none of a provider's health care items or services; however, recognize issues with bundled items or services
- If original form of payment dishonored, must make reasonable efforts to obtain payment prior to billing health plan
- How to address other legal requirements

Notice of Privacy Practices for Patients

A patient has a right to adequate written notice of:

- uses and disclosures of PHI that may be made by the Covered Entity, and
- patient's rights and Covered Entity's legal duties with respect to PHI

Just a reminder, permitted uses and disclosures must be addressed in a covered entity's Notice of Privacy Practices. HHS offers model notices of privacy practices for health care providers. These model notices are available for free download, in English and in Spanish, at http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices

45 CFR § 164.520

Elements for Notice of Privacy Practices

- Header – specific language in Rule
- Description of uses and disclosures
- Patient rights and how to exercise those rights
- Covered Entity duties and contact name or title & telephone number to receive complaints
- Effective Date

Notice of Privacy Practices for Patients

Content must include:

- Statements regarding sale of PHI, marketing, and other purposes that require authorization
- For covered entities engaging in fundraising, statement that patient can opt out of fundraising communications
- For providers, statement that covered entity must agree to restrict disclosure to health plan if patient pays out of pocket in full for health care service
- Statement about patient's right to receive breach notifications

Delivery of Notice

- **By Direct Treatment Providers**
  - First service delivery after compliance date
  - Good faith effort to obtain a written acknowledgment of receipt
- **By Health Plans**
  - At compliance date and thereafter at enrollment to new enrollees
  - Every 3 years, must tell enrollees of availability of Notice and how to obtain
  - *Health plans may distribute materially revised NPPs*:
    - By posting on web site by effective date of change and including in next annual mailing to patients; or
    - Mailing to patients within 60 days of material revision
- **By All Covered Entities**
  - On request to **any person**

Patient Complaints

- Covered Entity must provide process for patients to complain concerning Covered Entity's privacy and breach notification policies or procedures
- No provisions on how Covered Entity's complaint process must operate other than to document complaints and their disposition
- Patients may also complain to OCR

45 CFR § 164.530(d)

Patient Right of Access

- Designated record set broadly includes medical, payment, and other records used to make decisions about the patient
  - Doesn't matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports and underlying information (including genomic information)

45 CFR § 164.524

Patient Right of Access

- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about patients (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require patient to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that patient may not understand or be upset by the PHI not sufficient to deny access

Patient Right of Access

- Covered entity may require written request
- Can be electronic
- Reasonable steps to verify identity
- BUT cannot create barrier to or unreasonably delay access
  - E.g., cannot require patient to make separate trip to office to request access

Patient Right of Access

- patient has right to copy in form and format requested if "readily producible"
  - If PHI maintained electronically, at least one type of electronic format must be accessible by patient
  - Depends on capabilities, not willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by email (or mail), including unsecure email if requested by patient (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity's systems

Patient Right of Access

- Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner
- Limited fees may be charged for copy
  - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
  - No search and retrieval or other costs, even if authorized by State law
  - Entities strongly encouraged to provide free copies

Patient Right of Access

- Providing access through certified EHR technology (*i.e.,* View, Download, Transmit)
- Administrative overhead costs for outsourcing access requests to a business associate
- Viewing and inspecting PHI only

Patient to Designated 3rd Party

- patient's right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR § 164.524)
- patient may also authorize disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR § 164.508)

VALID AUTHORIZATION CHECKLIST

Please use this checklist to determine the validity of an Authorization under the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Refer to the Privacy Rule at 45 C.F.R. § 164.508 for more information.

An Authorization must contain at least the following elements:

☐	A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
☐	The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
☐	The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
☐	A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of purpose.
☐	An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information (PHI) for research, including for the creation and maintenance of a research database or a research repository.
☐	The signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

Source for Valid Authorization Checklist=Office for Civil Rights

☐	A statement adequate to place the individual on notice that he/she has a right to revoke the authorization in writing **AND EITHER:**
	☐ A statement indicating the exceptions to the right to revoke and a description of how the individual may revoke the authorization; **OR**
	☐ A statement referring the individual to the covered entity's Notice of Privacy Practices (NPP) if the NPP includes the information that would be contained in a statement indicating the exceptions to the right to revoke and a description of how the individual may revoke the authorization
☐	A statement adequate to place the individual on notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization by **EITHER**:
	☐ A statement that the covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization: this statement should be used when a covered entity has determined that none of the exceptions in 45 C.F.R. § 164.508(b)(4) apply to it; **OR**
	☐ A statement explaining the consequences to the individual of a refusal to sign the authorization: this statement should be used when a covered entity has determined that one of the exceptions in 45 C.F.R. § 164.508(b)(4) applies to it and allows it to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such an authorization.
☐	A statement adequate to place the individual on notice of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the Privacy Rule.
☐	Be written in plain language.

A valid authorization may contain elements or information in addition to the elements in the checklist above, provided that such additional elements or information are not inconsistent with the elements required in 45 C.F.R. § 164.508.

A parting thought…a well trained employee can be your biggest asset.

HOSPITAL / SCHOOL / UNIVERSITY Campus Safety

News School University Hospital Technology Clery / Title IX

Hospital Security

Northwestern Memorial Fires 60 Employees for Accessing Celebrity's Records

The former employees say they were fired for inappropriately accessing 'Empire' actor Jussie Smollett's medical records, which many are denying.

Thanks for your valuable time today

For assistance please contact:

Susan Clarke: sclarke@mpqhf.org, (307) 248-8179

Questions