



HIPAA PASS Privacy and Security Solutions

COVID-19 Insights on the HIPAA Privacy Proposed Rule

Presented by Susan Clarke

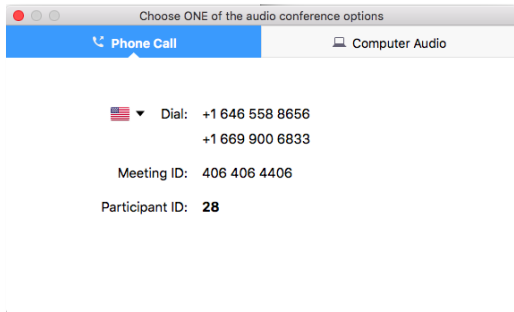
Health Care Information Security and Privacy Practitioner

Thursday, March 25 | 11:00-12:00 p.m.



Zoom tips and tricks!

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

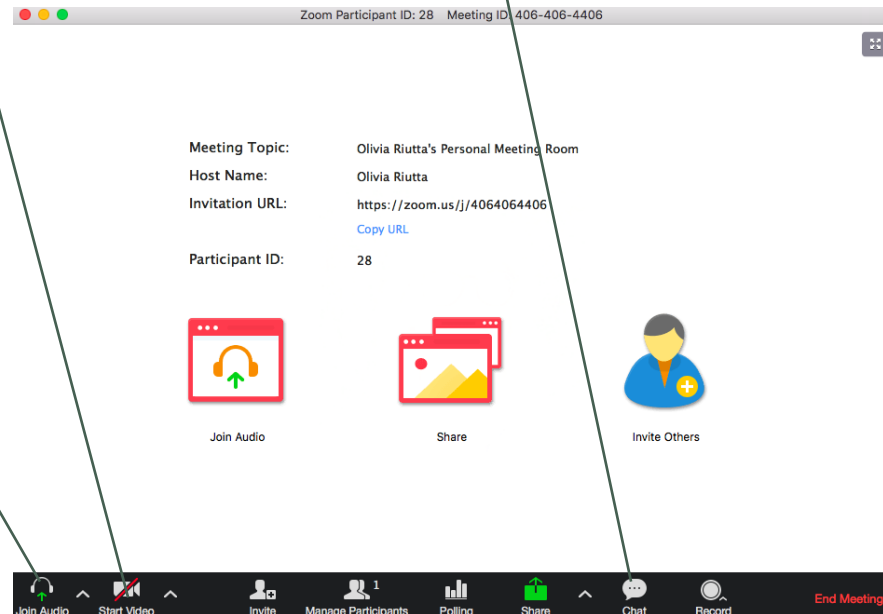


AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click “Join Audio,” this “Choose one...” box will pop up. If you dial in, just make sure you include your audio code.

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



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



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

Upcoming HCCN Sessions

TELEHEALTH TUESDAY SESSIONS

3rd Tuesday of each month at 11:00 a.m.

April 20: Telehealth Workflows and
Staffing Optimization

May 18: Remote Patient Monitoring for
Patient Care

June 15: Privacy and Security
Considerations of Telehealth

HIPAA Webinar Series with Susan Clarke

Thursday, June 17 at 11:00 a.m.

Thursday, September 16 at 11:00 a.m.

Thursday, December 16 at 11:00 a.m.

OTHER HCCN EVENTS

**Hypertension Control and Remote Patient
Monitoring Peer Learning Meeting**

March 26 at 10:00 a.m.

ImMTrax Learning Collaborative

April 7th 11:00 a.m.

Azara DRVS User Group

April 8th at 10:00 a.m.

**CURES Act Compliance: Policy Review
Webinar**

April 21st 11:00 a.m.

Big Sky Care Connect Outreach & Q&A

April 29 at 1:00 p.m.

MPCA Events



Susan Clarke, HCISPP



(ISC)² Healthcare Information Security and Privacy Practitioner and Computer Scientist at Mountain-Pacific Quality Health.

Conducts privacy and security risk analysis in addition to HIPAA and 42 CFR, Part 2 training.

20 years' experience in health care operations.

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 health care system.

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

BAA: Business Associate Agreement

CE: Covered Entity

CEHRT: Certified Electronic Health Record Technology

CMS: Centers for Medicare & 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

NPP: Notice of Privacy Practices

NPRM: Notice of Proposed Rulemaking

PHA: Personal Health Application

PHI: Protected Health Information

SP: Special Publication

SRA: Security Risk Analysis

Learning Objectives

1. Overarching Privacy Trends
2. Patient's Right to Access and Sharing
3. Care Coordination and Case Management
4. COVID Driven Family and Caregiver Evolvement
5. Enhanced Flexibility during Emergencies
6. Reducing Administrative Burden

HIPAA Safe Harbor Bill



Signed January 5, 2021



Amends HITECH Act
("recognized
cybersecurity practices")



Lenient fines if basic
safeguard requirements met

- HIPAA Security Rule
- Security risk analysis



Current Outlook



The Bigger Picture

New proposed HIPAA privacy rule:



“Our proposed changes to the HIPAA Privacy Rule will break down barriers that have stood in the way of commonsense care coordination and value-based arrangements for far too long,” said HHS Secretary Alex Azar. “As part of our broader efforts to reform regulations that impede care coordination, these proposed reforms will **reduce burdens on providers and empower patients and their families** to secure better health.”

New Proposed HIPAA Privacy Rule Brought on or Heightened by COVID

Includes changes in
Notice of Proposed
Rulemaking for
HIPAA Privacy Rule
released by HHS on
December 10, 2020



Public Comment Date Moved



Extended to
May 6, 2021

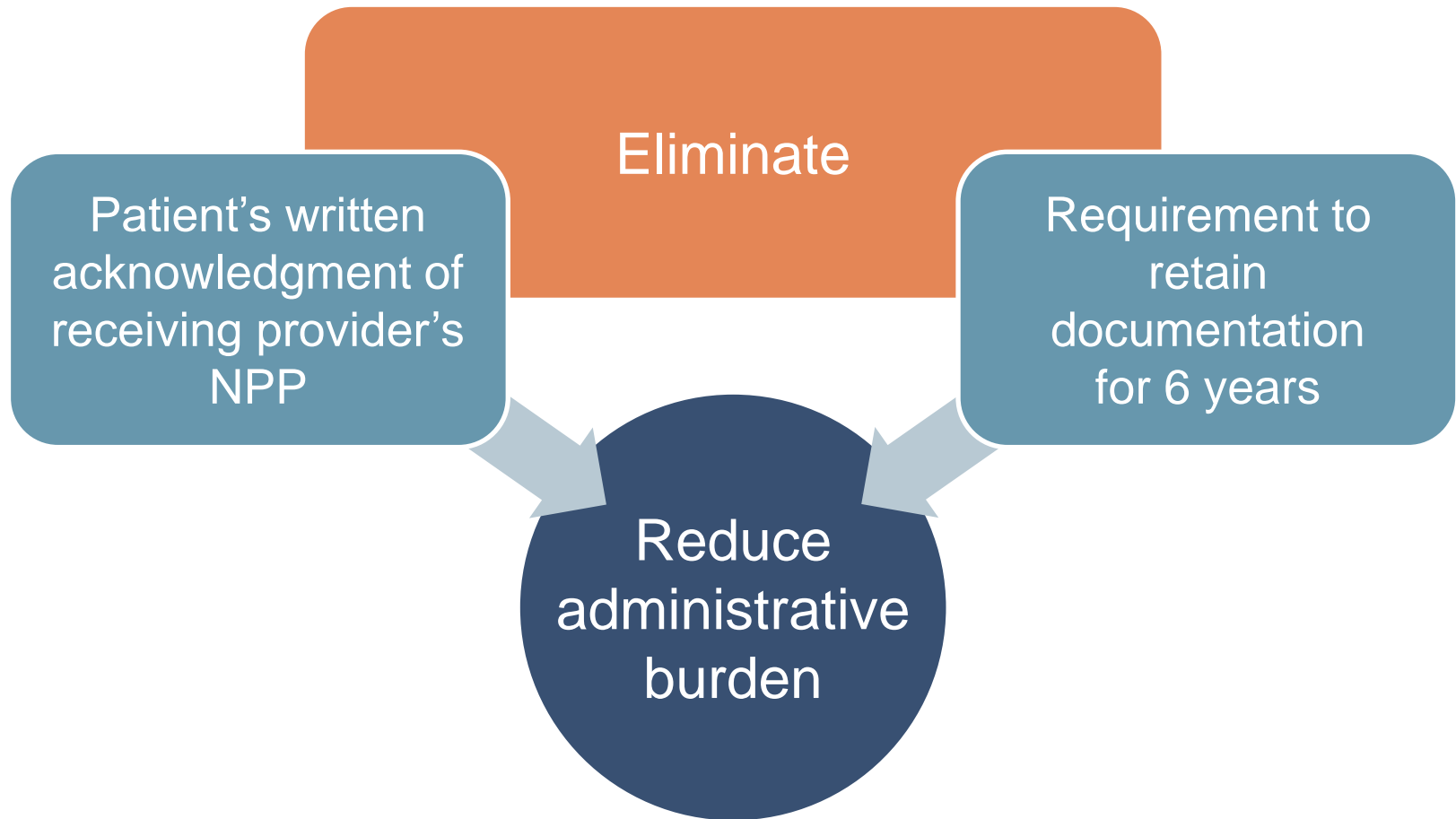
Comment at:

<https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care>



Key Proposed Changes

Notice of Privacy Practices (NPP)



NPP Content Change

The content requirements of the NPP would be modified to clarify patient's rights with respect to their protected health information (PHI) and how to exercise those rights, related to required language regarding:

- (1) How to access health information.
- (2) How to file a HIPAA complaint.
- (3) Patient's rights to receive a copy of the notice and to discuss its contents with a designated person.

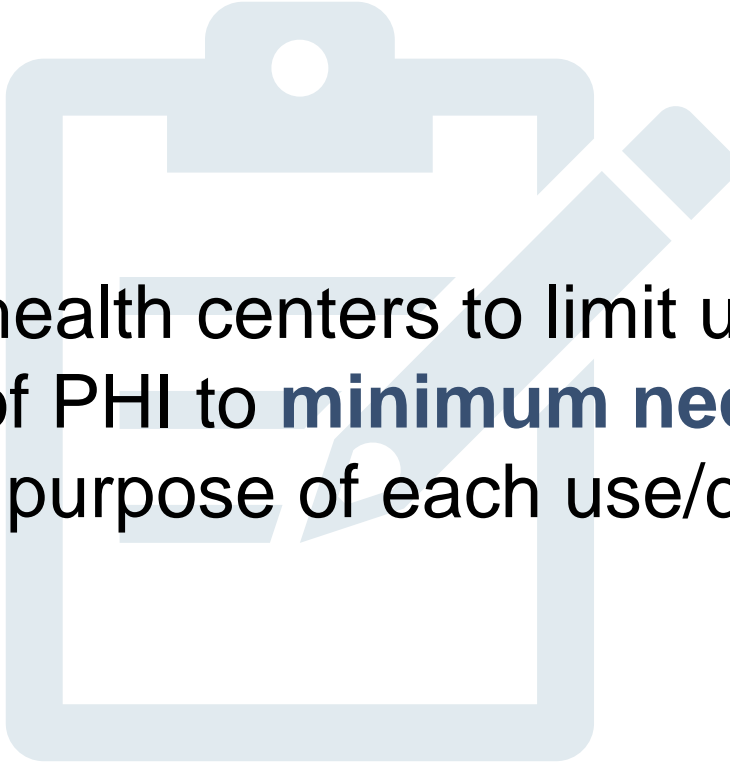
Care Coordination Clarifications

NPRM proposes to change definition of “health care operations”



Includes care coordination and case management for patients

Minimum Necessary Today



Requires health centers to limit uses and disclosures of PHI to **minimum necessary** to accomplish purpose of each use/disclosure

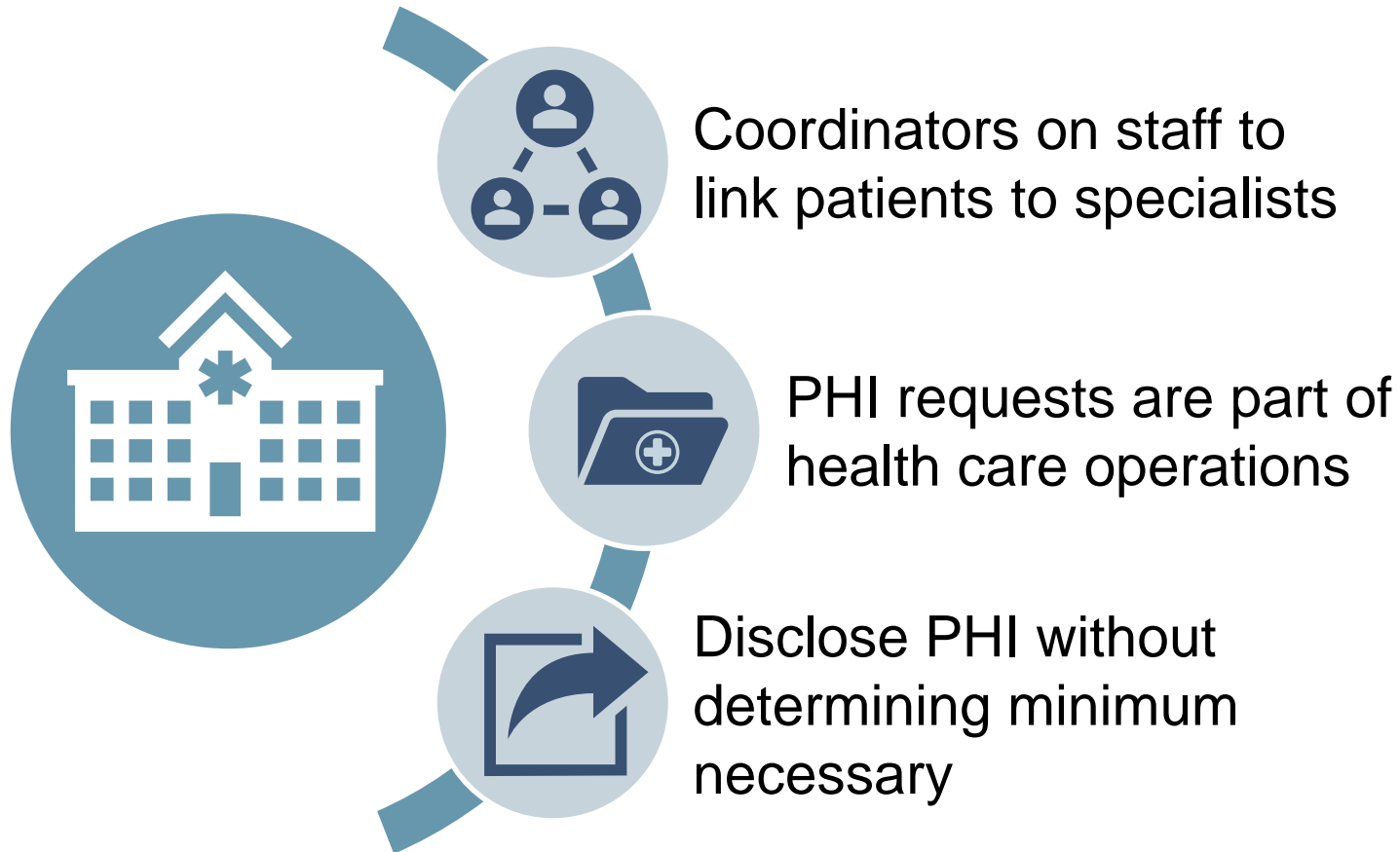
Exceptions to Minimum Necessary Standards



Add express exception for disclosures to health plan or covered health care provider **for care coordination and case management**

Example:

Exceptions to Minimum Necessary Standards



Expressly Permitted

Health centers can disclose PHI to

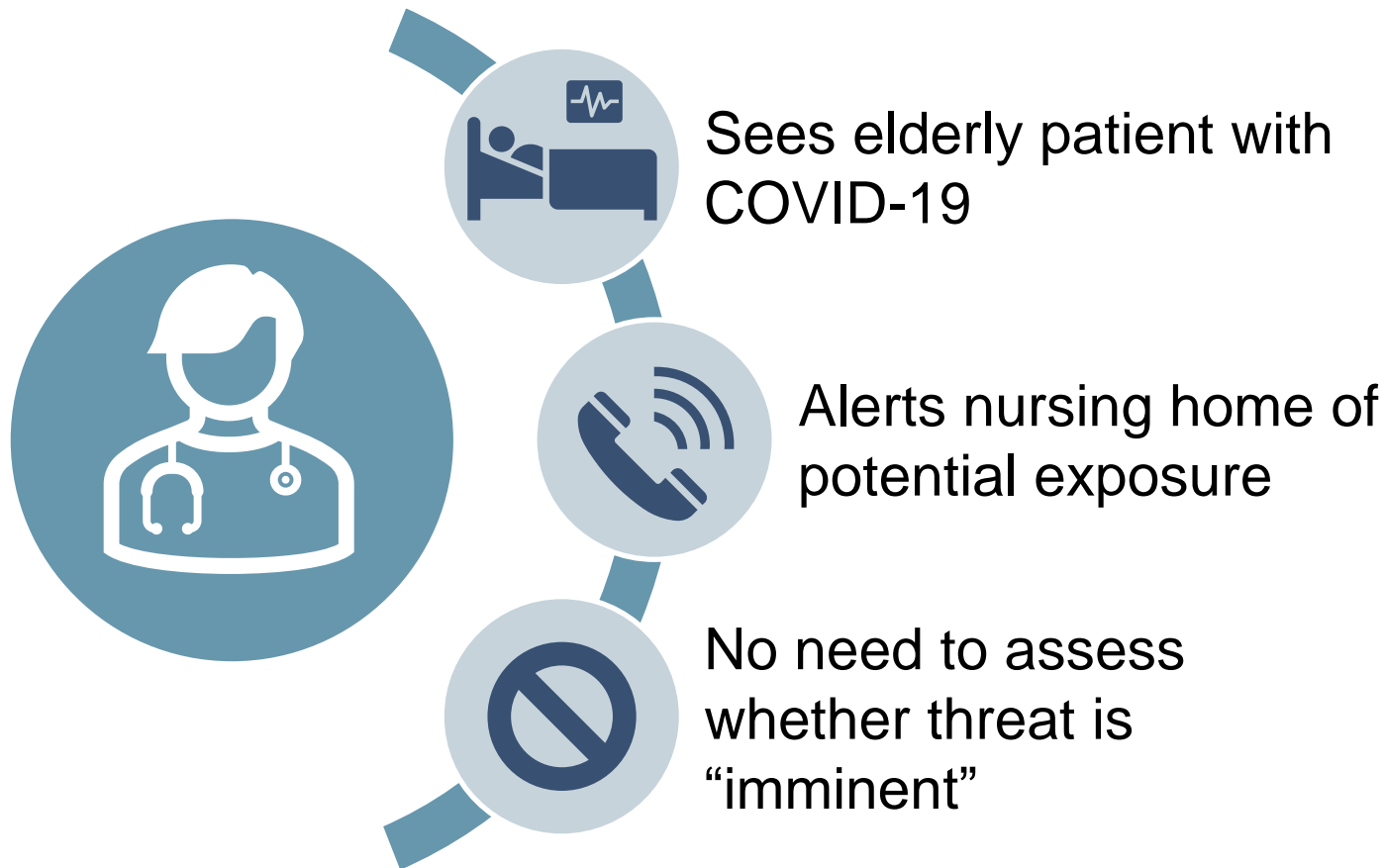
- Social services agencies
- Community-based organizations
- Home- and community-based service providers
- Other similar third parties that provide health-related services

Disclosures to Prevent Harm

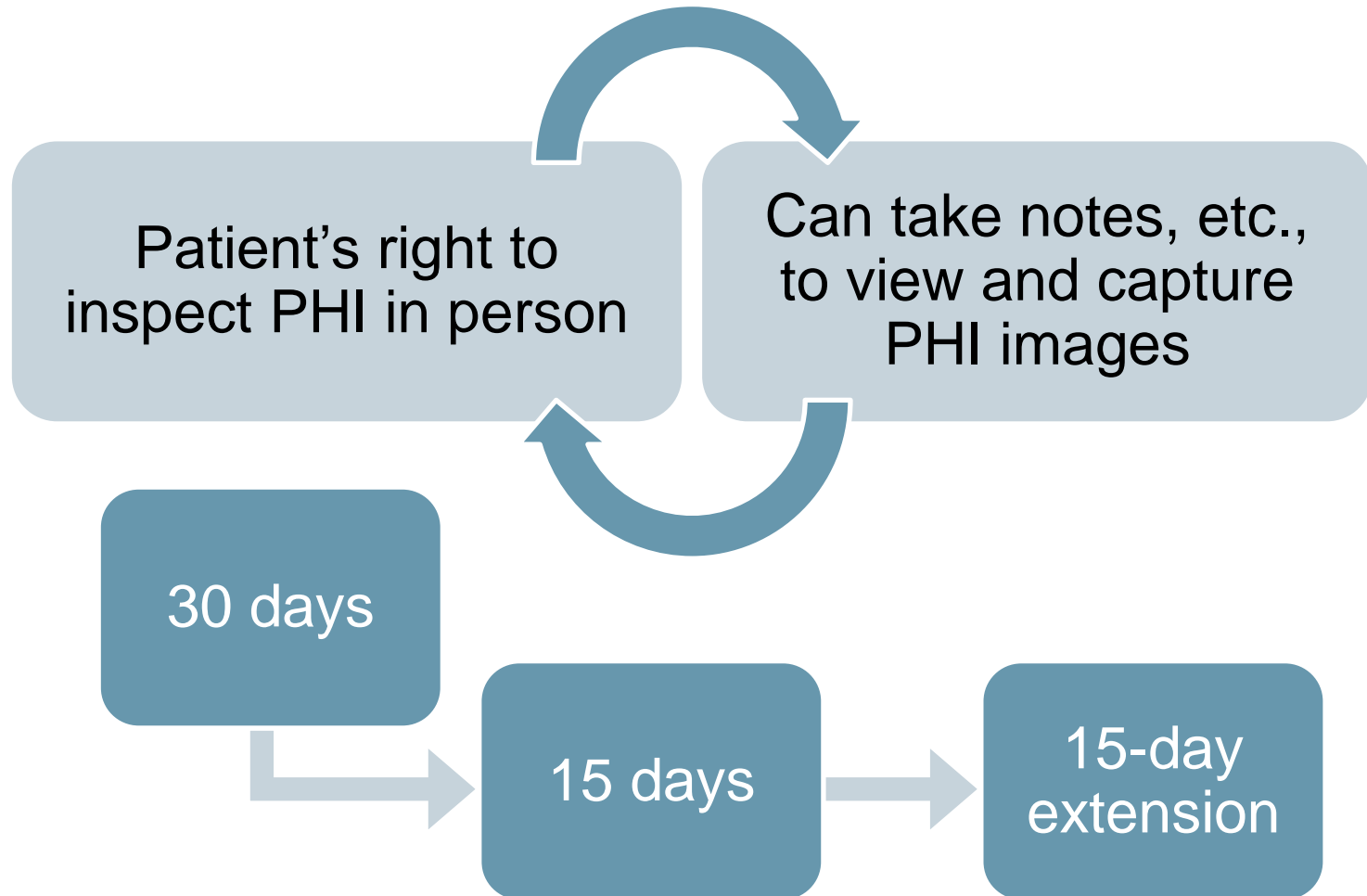
Health centers can disclose PHI to

- Avert threat to health or safety when harm is “serious and reasonably foreseeable”
- Instead of current, stricter standard which requires “serious and imminent” threat
- Can be used to help combat COVID-19

Example: Disclosures to Prevent Harm



Patient's Right to Access: Time



Patient's Right to Access: Fees

NPRM:



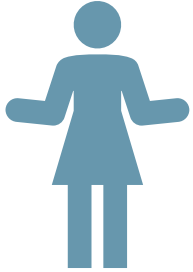
- Defines permissible and impermissible charges. Inspecting is always free.
- Can charge third-party direct copy fee.
- **Do not violate State Law.**

Patient's Right to Access: Ease



Reduce requirements for
identity verification of patients
requesting access

Patient's Right to Access: Sharing



Patients can direct sharing of their health records in an electronic health record (EHR) among covered health care providers and health plans.



Covered health care providers and health plans must submit patient's access request to another health care provider and receive electronic copies in an EHR.

Patient's Right to Access: Sharing

NPRM:



Patient's right of access would be limited to direct transmission to a third party to only include electronic PHI, i.e., must be part of an EHR

NPRM Definition Changes

Electronic Health Record (EHR):

An electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff

Personal Health Application:

An electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer

Final Thoughts

- 1 NPRM includes changes to reduce unnecessary administrative burdens and add clarity to HIPAA Privacy Rule
- 2 How will proposed changes impact patient's privacy and health center's operations?
- 3 Growing number of defined data sets adds complexity, e.g.,
 - Interoperability policy
 - Electronic health records
 - Traditional HIPAA's "designated record set"
 - ONC Interoperability and Information Blocking Rule's "electronic health information"
 - FTC Breach Notification Rule's "personal health record"
- 4 Health centers should consider providing feedback – Comment period extended to May 6, 2021

Resources Used

- The National Law Review
<https://www.natlawreview.com/article/comment-period-extended-extensive-changes-to-hipaa-privacy-rule>
- Proposed Mods to the HIPAA Privacy Rule
<https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care>



Please let me know how I can help.

For assistance please contact:

Susan Clarke

sclarke@mpqhf.org | (307) 248-8179

**THANKS FOR YOUR
VALUABLE TIME TODAY!**

