Healthy People, Healthy Communities
Providing Better Care at Lower Cost

MIPS Tips

Security Risk Analysis—Jan. 17, 2019

Presented by HealthInsight and Mountain Pacific Quality Health

Supporting You

HealthInsight and Mountain-Pacific Quality Health are providing support to practices as subcontractors to NRHI, the Network for Regional Healthcare Improvement.

HealthInsight

Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES

Mountain-Pacific
Quality Health

nrhi
Network for
Regional Healthcare
Improvement

Slide Deck Available

- Today's slide deck and recording will be made available a few days following the event. Watch your email to be notified when they are available or visit https://healthinsight.org/qpp#webinars to find all past MIPS Tips and QPP webinar recordings.

Mark Norby, CHP, CISA

- Certified HIPAA Profession
- Certified Information Systems Auditor
- 16 years of IT and HIPAA compliance experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Assisted more than 250 hospitals and clinics with HIPAA compliance

Susan Clarke, HCISPP

- (ISC)^2 certified health care information security and privacy practitioner and computer scientist
- 20 years of health care experience
- 10 years design and coding EHR software including HL7 health care application development
- Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic affiliated health care system
- Served as communications unit lead during health care system’s ready and complete alerts

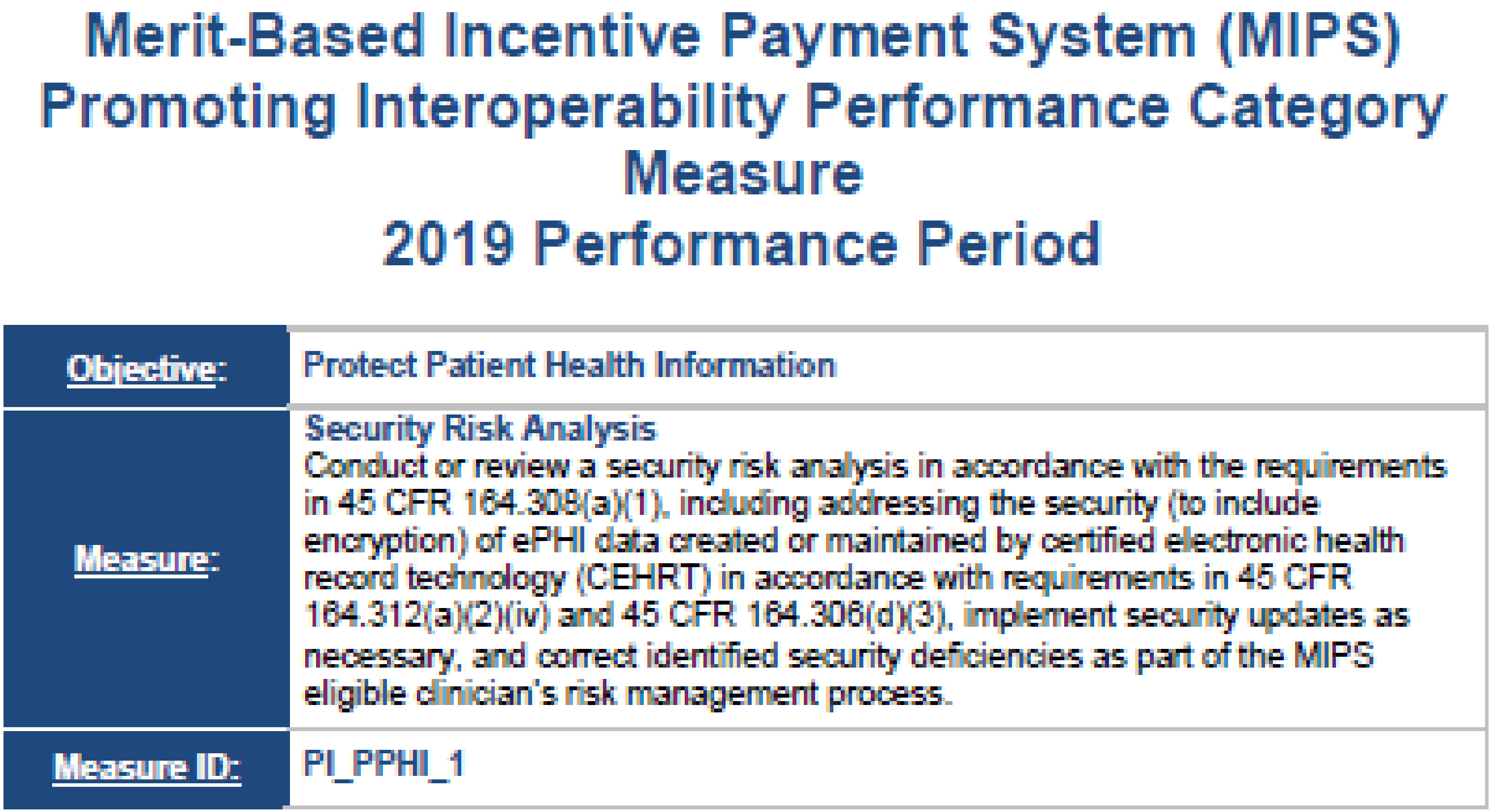
Disclaimers

- The presenter is not an attorney and does not give legal advice
- There are many different interpretations of HIPAA regulations
- Materials referenced are meant to serve as examples and may not be suitable for every organization

Objectives

- Improve understanding of the Security Risk Analysis (SRA) requirement in the Promoting Interoperability (PI) category of MIPS
- Clarify the PI encryption expectations
- Correcting identified deficiencies
- Understand SRA options and best practice
- Understand Information Blocking and how it impacts your organization

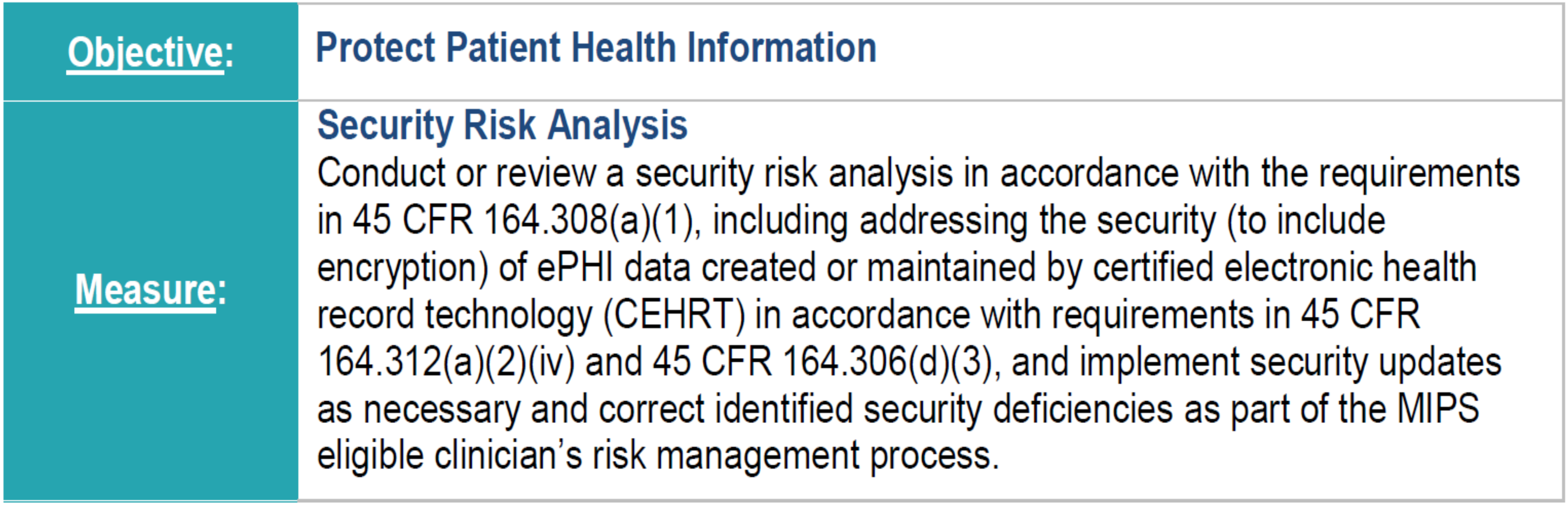
SRA Measure Same as 2018



Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2019 Performance Period

Objective:	Protect Patient Health Information
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.
Measure ID:	PI_PPHI_1

Protect Patient Health Information



Objective:	**Protect Patient Health Information**
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

Security Risk Analysis (SRA)

"Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1)"

45 CFR 164.308(a)(1):

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

Timing of the SRA

- It is acceptable for the security risk analysis to be conducted or reviewed outside the performance period; however, the analysis must be unique for each performance period, the scope must include the full MIPS performance period, and it must be conducted within the calendar year of the MIPS performance period (January 1st – December 31st).

- The SRA must be unique for each calendar year

When 2015 Edition CEHRT is Implemented

- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each MIPS performance period.
- Any security updates and deficiencies that are identified should be included in the clinician's risk management process and implemented or corrected as dictated by that process.

“Addressing” Encryption

“including addressing the security (to include encryption) of ePHI data created or maintained by CEHRT in accordance with requirements in 45 CFR164.312(a)(2)(iv) and 45 CFR 164.306(d)(3)”

45 CFR164.312(a)(2)(iv) *Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

45 CFR 164.306(d)(3) When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity or business associate must—

“Addressing” Encryption

- Implement the specification if reasonable and appropriate;
  OR
- Document why it would not be reasonable and appropriate;
  AND
- Implement an equivalent alternative measure if reasonable and appropriate

1) Data in Transit

Data in transit, or **data in motion**, is data actively moving from one location to another such as across the internet or through a private network.

For protecting data in transit, enterprises often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, WPA, VPN, etc) to protect the contents of data in transit.

2) Data at Rest

Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.

For protecting data at rest, enterprises can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself.

Your version of Windows makes a difference!

§ 170.314(d)(7) End-user device encryption

- EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops.
- Unless, EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.

Implement Security Updates

"and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process. 45 CFR 164.308(a)(1)"

45 CFR 164.308(a)(1):

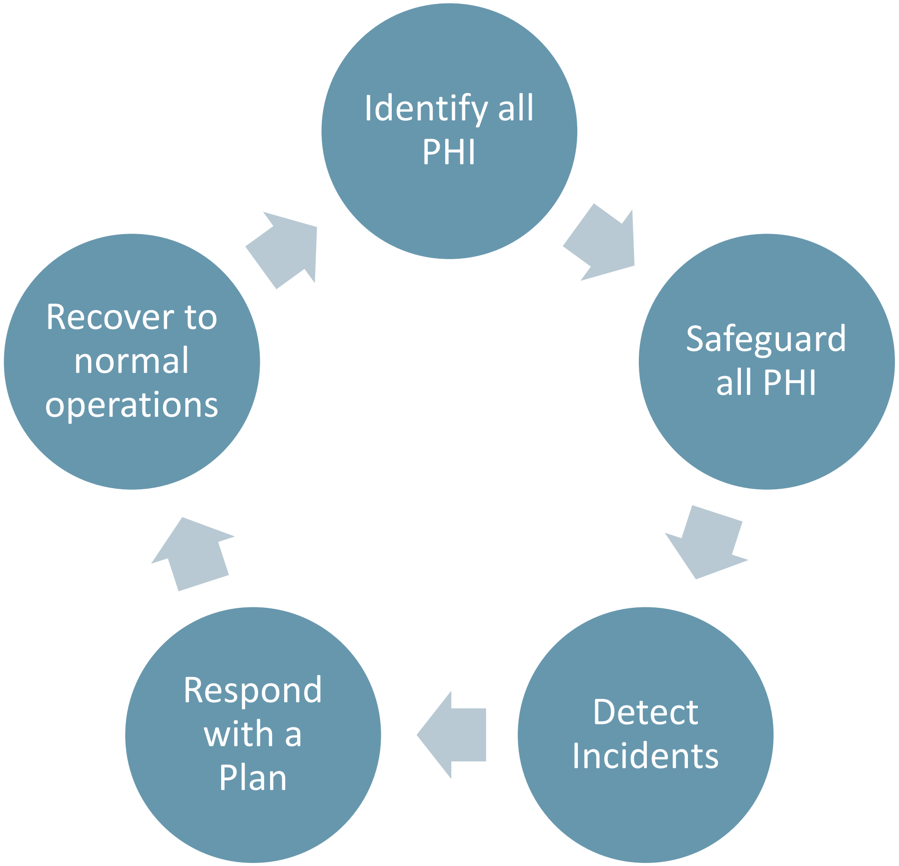
(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

Great news! Once you have your SRA done and risk management plan in place you will know what you need to do to become HIPAA compliant and pass an OCR or CMS audit.

Failure to Meet this Measure

- Same as 2018, the Security Risk Analysis is still required.
- However, in 2019 the scoring methodology has changed; CMS will be scoring the four objectives independently. Each of the four objectives must be reported or excluded, or a score of zero will result for the entire category.

Oversight & Governance



- Risk Assessment and Management
- Patch & Vulnerability Management
- Data Inventory
- Identity Management
- Third-Party Assessment
- Effectively Communicate your Program
- **Develop a mature Compliance program over time, not once and done.**

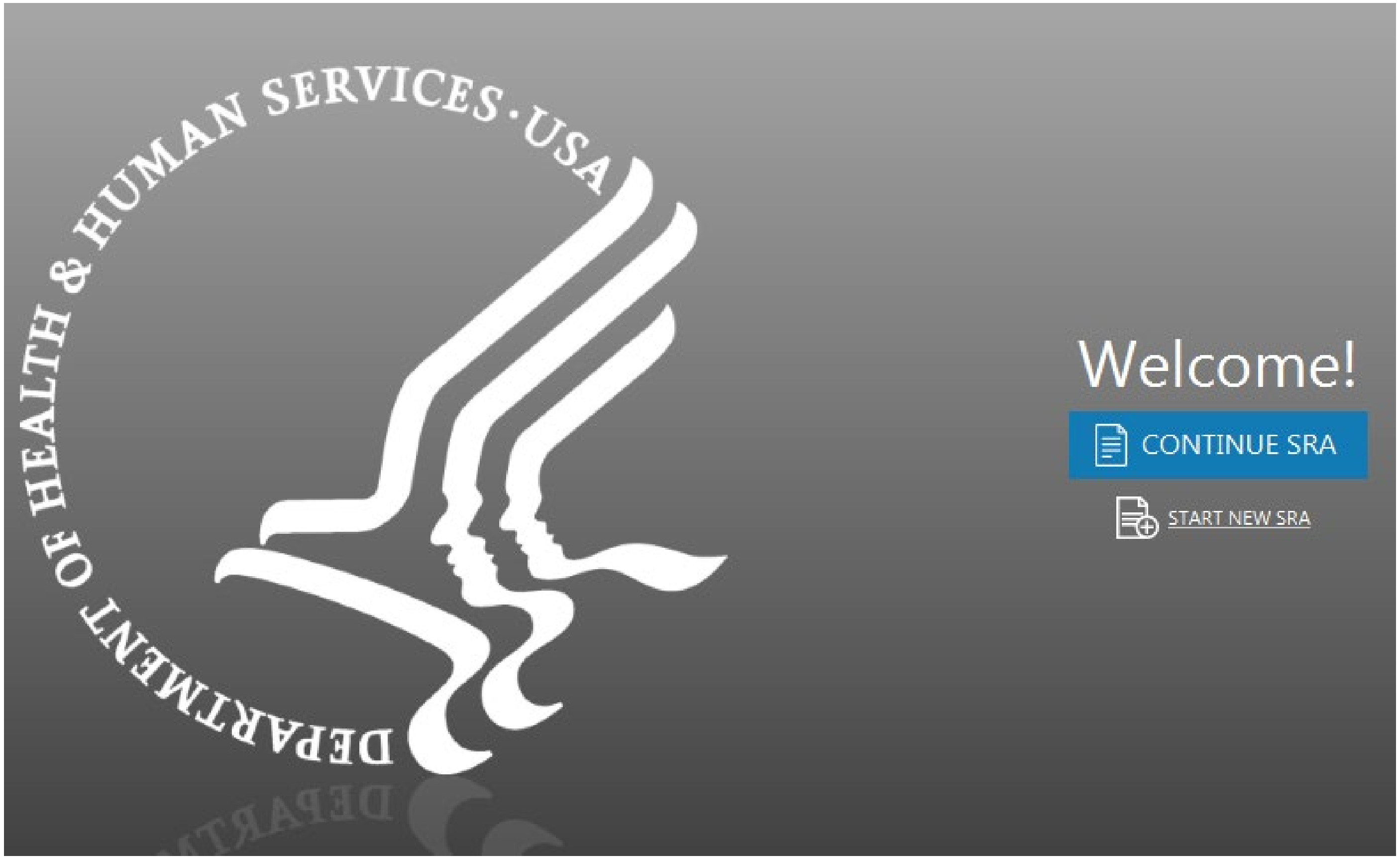
If you are not a HIPAA guru….

Mountain-Pacific Quality Health and HealthInsight have teamed up to provide a comprehensive, budget friendly solution.

We recommend you hire a quality professional that will provide you with:

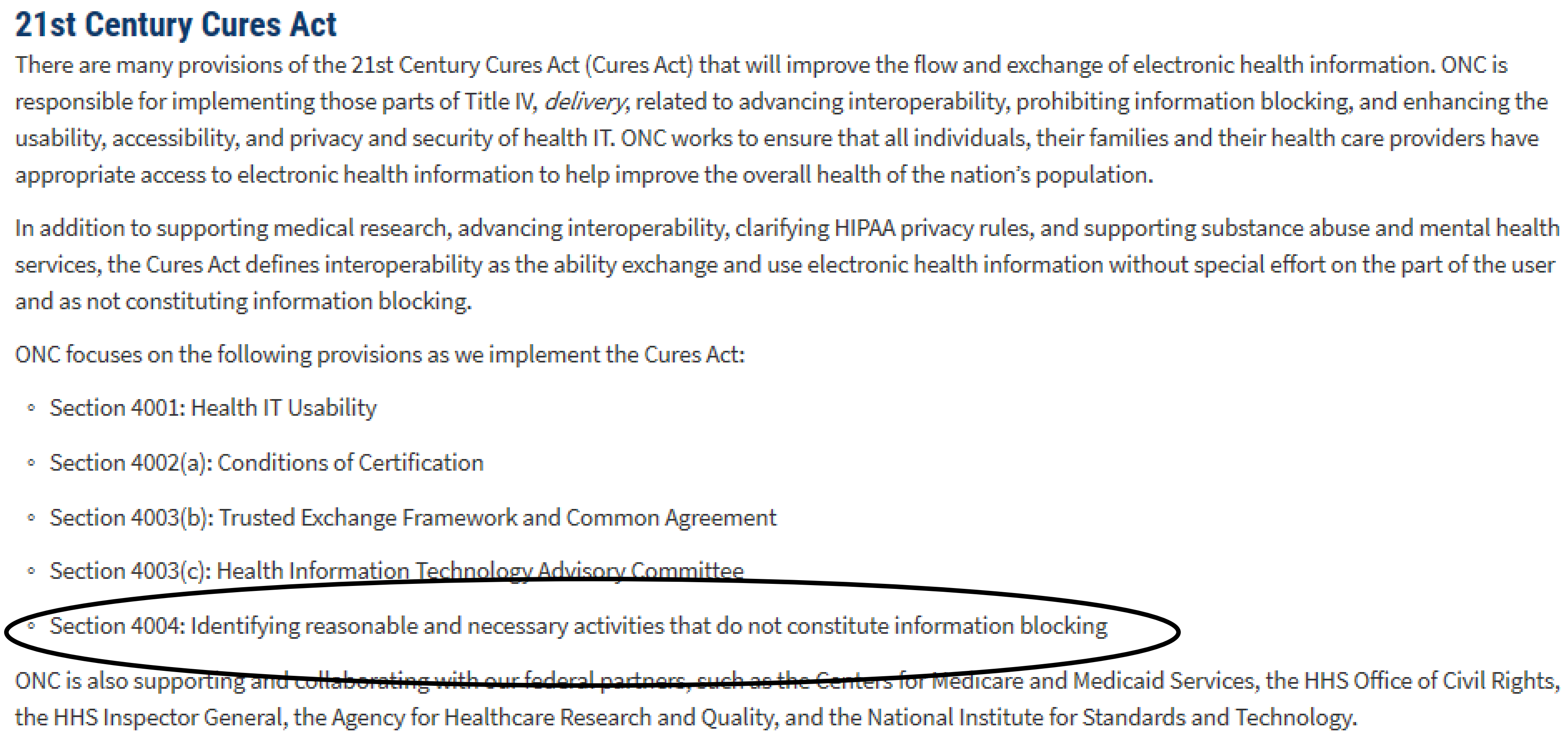
- ✓ Security Risk Analysis
- ✓ Risk Management Plan
- ✓ Training Plan
- ✓ Policies and Procedures
- ✓ Customer Support

New! Security Risk Assessment Tool Version 3.0



https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

Information Blocking



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.

ONC focuses on the following provisions as we implement the Cures Act:

- Section 4001: Health IT Usability
- Section 4002(a): Conditions of Certification
- Section 4003(b): Trusted Exchange Framework and Common Agreement
- Section 4003(c): Health Information Technology Advisory Committee
- Section 4004: Identifying reasonable and necessary activities that do not constitute information blocking

ONC is also supporting and collaborating with our federal partners, such as the Centers for Medicare and Medicaid Services, the HHS Office of Civil Rights, the HHS Inspector General, the Agency for Healthcare Research and Quality, and the National Institute for Standards and Technology.

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

Impact to Providers and Hospitals

To prevent actions that block the exchange of health information, eligible professionals (EPs), eligible hospitals and critical access hospitals (CAHs) that participate in both the Medicare and Medicaid Promoting Interoperability (PI) Programs to show that they have not knowingly and willfully limited or restricted the compatibility or interoperability of their certified electronic health record technology (CEHRT).

All or None

- If you are a MIPS eligible clinician who reports on the Promoting Interoperability performance category you must attest to the prevention of information blocking attestation.
- If you are reporting as a group, the prevention of information blocking attestation by the group applies to all MIPS eligible clinicians within the group.
- ***Therefore, if one MIPS eligible clinician in the group fails to meet the requirements of the Prevention of Information Blocking Attestation, then the whole group would fail to meet the requirement.***

Good Faith Attestation

EPs, eligible hospitals and CAHs are required to show that they are meeting this requirement by attesting to three statements about how they implement and use CEHRT. Together, these three statements are referred to as the "Prevention of Information Blocking Attestation."

Three Attestation Statements

Statement 1: Did not knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT.

Statement 2: Implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that the CEHRT was, at all relevant times; 1)connected 2) able to exchange 3) timely 4) timely, secure and trusted exchange of structured data.

Statement 3: Responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers, and other persons, regardless of the requestor's affiliation or technology vendor.

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

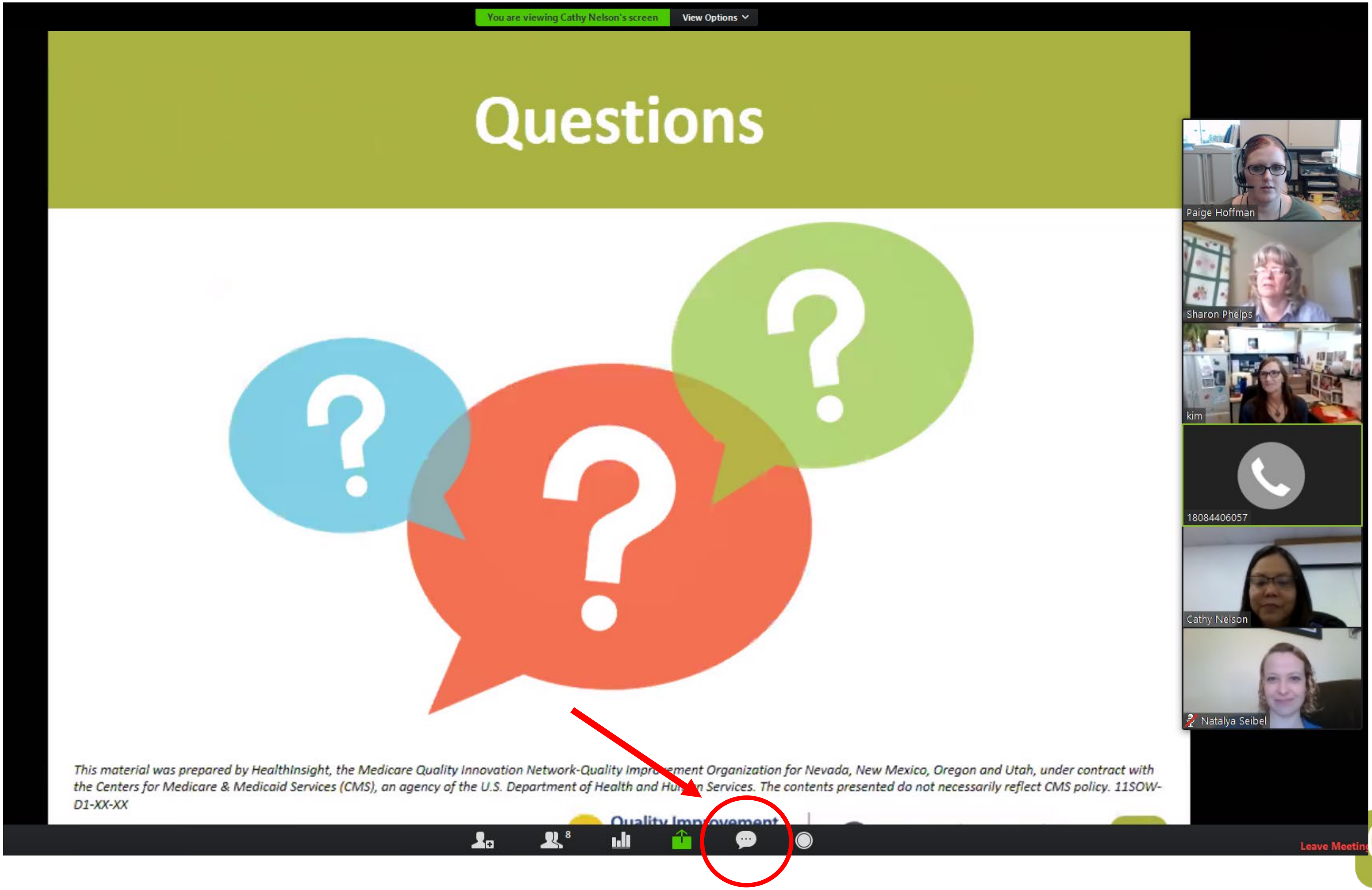
Example: Health care providers restrict access to a patient’s sensitive test results until the clinician who ordered the tests, or another designated health care professional, has reviewed and appropriately communicated the results to the patient.

(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 individualized assessment of their patient’s best interests (rather than a blanket policy) and were not an excuse for restricting health information exchange.

How to Ask a Question



Questions

This material was prepared by HealthInsight, the Medicare Quality Innovation Network-Quality Improvement Organization for Nevada, New Mexico, Oregon and Utah, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. 11SOW-D1-XX-XX

Please Fill Out Our Evaluation

- An evaluation link for this session is currently being place in the chat. Please take a few minutes before you leave the meeting today to fill out an evaluation and help us improve our offerings.

This material was prepared by HealthInsight, the Medicare Quality Innovation Network-Quality Improvement Organization for Nevada, New Mexico, Oregon and Utah, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. 11SOW-D1-19-03

Assessment

- Get customized support for your practice by filling out a short assessment
- HealthInsight: https://healthinsight.org/qpp-assessment
- Mountain-Pacific: http://mpqhf.com/QIO/qpp-enroll/

CMS Learning Modules

CMS has created several learning modules aimed at helping you understand and succeed in the QPP program. You can find those modules here: https://learner.mlnlms.com/Default.aspx

For More Information Contact a QPP Expert in Your State

Mountain-Pacific Quality Health

Please contact us for assistance!

QualityPaymentHelp@mpqhf.org

Montana
Amber Rogers
arogers@mpqhf.org
(406) 544-0817

Wyoming
Brandi Wahlen
bwahlen@mpqhf.org
(307) 472-0507

Alaska
Preston Groogan
pgroogan@mpqhf.org
(907) 561-3202

Region/Senior Account Manager
Sharon Phelps
sphelps@mpqhf.org
(307) 271-1913

Hawaii and Territories
Cathy Nelson
cnelson@mpqhf.org
(808) 545-2550

Visit us online at www.mpqhf.org.

For More Information Contact a QPP Expert in Your State

HealthInsight QPP Support

Call: 801-892-6623

Email: qpp@healthinsight.org

Web: www.healthinsight.org/qpp

Nevada
Aaron Hubbard
Call: 702-948-0306
Email: ahubbard@healthinsight.org

New Mexico
Ryan Harmon
Call: 505-998-9752
Email: rharmon@healthinsight.org

Oregon
Seema Rathor
Call: 971-409-3872
Email: srathor@healthinsight.org

Utah
Sandra DeBry
Call: 801-892-6605
Email: sdebry@healthinsight.org

HealthInsight and Qualis Health

In April 2018, HealthInsight and Qualis Health announced a formal merger, combining the two organizations and operations across the U.S. Both HealthInsight and Qualis Health have been engaged in health care quality consulting and providing quality improvement services for more than 40 years.

If you are a practice in Washington or Idaho and are seeking QPP support please contact:

Idaho
Deanna Graham
Call: 208-383-5951
Email: deannag@qualishealth.org

Washington
Jeff Sobotka
Call: 206-288-2529
Email: jeffs@qualishealth.org

Contact Us!

Mark Norby

- Certified HIPAA Professional and HIPAA Counselor
- mnorby@healthinsight.org
- (307)258-5322

Susan Clarke

- Certified Health Care Information Security and Privacy Practitioner
- sclarke@mpqhf.org
- (307) 248-8179

Thank you and have a wonderful day!