Part 8: Wrap up and Final Review

Presented by: Susan Clarke,
Health Care Information Security and Privacy Practitioner

June 5 & 6, 2018
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 individual needs.
Learning Objectives

A very brief overview of HIPAA and opportunity for some final thoughts, lessons learned and feedback.
• 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
Covered Entities (CE)

- Includes health plans, health care clearing houses and most health care providers
- Applies to most health care providers because they transmit health information electronically (e.g. billing)
Business Associates

- Individuals and organizations that perform services for or on behalf of your practice that involve routine access to Protected Health Information (PHI)
Organizations frequently underestimate the proliferation of ePHI within their environments.
Protected Health Information (PHI)

Refers to individually identifiable health information that relates to the individual’s past, present, future physical or mental condition that is:

• Transmitted by electronic media,
• Maintained in electronic media,
• Transmitted or maintained in any other form or medium.
Three Legs of 45 CFR

1) HIPAA **Privacy Rule** – April 2003

45 CFR [Part 160](#) and Subparts A and E of [Part 164](#)

2) HIPAA **Security Rule** – April 2005

45 CFR [Part 160](#) and Subparts A and C of [Part 164](#)

3) HIPAA **Breach Notification Rule** – September 2009

45 CFR [164.400-414](#)
HIPAA Privacy Rule

- Establishes standards for the use and disclosure of PHI
- Protects PHI whether electronic, oral or paper
- Establishes standards for providing patient rights
- Outlines civil and criminal penalties for failure to comply
Examples of Patient Rights

• The right to inspect, review and receive a copy of their health information
• The right to request amendments
• The right to an accounting of disclosures
• The right to confidential communications
• Access to Notice of Privacy Practice
HIPAA Security Rule

- Protects individuals’ **electronic** PHI that is created, received, maintained or transmitted by CE
- Protects confidentiality, integrity and availability (CIA) of ePHI
- Consists of administrative, physical and technical safeguards
IT Security and CIA Triad

Confidentiality

What if my health record isn’t kept private?

Integrity

What if my health record isn’t accurate?

Availability

What if my health record isn’t there when needed?

Information Assets
Compliance Does Not Equal Security

We are faced with an unprecedented security risk. Organizations need to bring EVERYONE along and develop a mature compliance AND security program over time.
Breach Notification Rule

• Requires CE’s to promptly notify individuals and the Secretary of HHS of the compromise of **unsecured** PHI

• Don’t forget about State Law
42 CFR Part 2

On January 3, 2018, the Substance Abuse and Mental Health Services Administration (SAMHSA) issued a final rule to revise 42 CFR Part 2, the federal regulations governing confidentiality of certain substance use disorder patients' records.

After 30 years Part 2 was substantively revised.
Qualified Service Organizations (QSO)

• Under Part 2 a qualified service organization (QSO) is an individual or entity providing a service to Part 2 treatment programs pursuant to a written agreement.
THANK YOU SO MUCH FOR YOUR TIME!

For assistance please contact:

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