eHEALTHDC

A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

Helping Healthcare Providers Adopt Electronic Health Records and Achieve Meaningful Use

DCPCA

DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION

MU Security Risk Assessment Webinar

July 31, 2018

1:00 – 2:00 PM EST

INTRODUCTIONS & WELCOME

- Moderator
  - Raakhee Sharma, eHealthDC Project Manager, District of Columbia Primary Care Association
- Speakers
  - Patricia (Trish) M. Wagner, Chief Privacy Officer, Epstein, Becker and Green, Washington, DC; 202.861.4182; pwagner@ebglaw.com
    - Bio
  - Leliveld (Lee) Emeni, eHealthDC Technical Assistance (TA Lead), eHealthDC

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

AGENDA

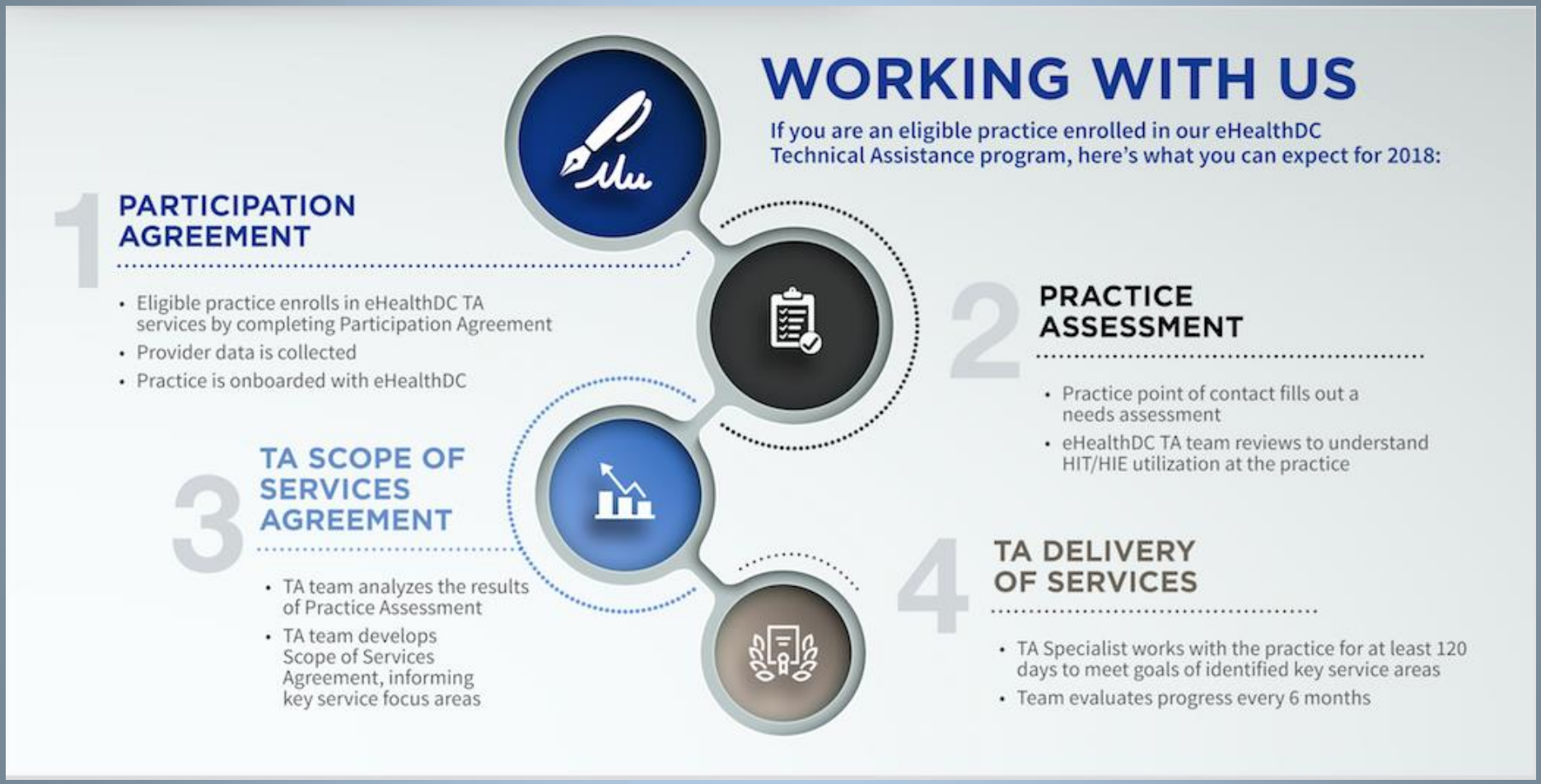
- Who is eHealthDC
  - Our role in Security Risk Assessments
- Overview of Security Risk Assessment (SRA)
  - Importance of and Need for Security Risk Assessments
  - HIPAA Security Rule
  - Understanding Security Risk Assessment annual requirements
- Ransomware and Breaches
- How to perform a Security Risk Assessment
  - Tools available – ONC SRA Toolkit
  - Parts of the assessment
- Demonstration of ONC SRA Toolkit
- Questions and Answers

eHealthDC Overview

- eHealthDC is a DC Primary Care Association program funded by the District of Columbia Department of Health Care Finance (DHCF)
- A multi-year technical assistance (TA) and outreach program designed to:
  - Raise awareness of Meaningful Use (MU) and Health Information Exchange (HIE) resources in the District
  - Encourage health care providers to show "meaningful use" of Certified Electronic Health Record Technology (CEHRT) by attesting to federally mandated objectives and measures
  - Provide hands-on support to help DC Medicaid eligible providers attest for Meaningful Use incentive payments through the District's State Level Registry (SLR) system
  - Support eligible providers in adopting and using Health Information Exchange (HIE)

Your "One-Stop Shop" for Meaningful Use and HIE resources in the District

TA PROCESS



IMPORTANCE OF SECURITY RISK ASSESSMENTS

- Patients trust their doctor to keep their e-PHI safe
  - Transformation to a “fully digital” world
- Hacking and ransomware is prevalent
- Cybersecurity is paramount
- Security and privacy risk assessments enable health care organizations to strengthen their foundational security to protect the privacy of its employees and patients

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

HIPAA SECURITY RULE

- Security Rule = How we protect e-PHI
- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce
- The Security Rule is broken down into “Required” and “Addressable” implementation requirements
  - Practice Tip: the "addressable" designation does not mean that an implementation specification is optional

RANSOMWARE AND BREACHES

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

BREACH NOTIFICATION- RANSOMWARE

- If PHI is breached, OCR requires notification to the individuals and to OCR
- Under HIPAA, a breach is defined as "…the acquisition, access, use or disclosure of PHI in a manner not permitted under [HIPAA] which compromises the security or privacy of the PHI"
- According to HHS guidelines, the burden of proof in determining whether there was a reportable breach of patient data during a ransomware attack is on the provider
- Difficult when providers can't rule out that the hacker did not have access to patient information
- Any breach of more than 500 patients is automatically investigated (OCR asks for policies, procedures, risk assessment etc.)
- Smaller breaches can be investigated as well

BREACH CAN LEAD TO FINES

- MAPFRE LIFE Insurance Company of Puerto Rico (Jan 2018)
  - Reached a $2.2 million settlement with OCR to resolve potential noncompliance with HIPAA Privacy and Security Rules
  - In 2011, MAPFRE filed a breach report acknowledging theft of a USB data storage device containing the ePHI of 2,209 individuals
  - OCR alleged that MAPFRE failed to conduct it's risk analysis and implement risk management plans, contrary to its prior representations, and had failed to deploy encryption or any equivalent alternative measure on its laptops and removable storage media until about September 2014

FINE FOR FAILURE TO PERFORM ADEQUATE RISK ANALYSIS

- Cardio Net (April 2017)
  - Reached $2.5 million settlement with OCR
  - In 2012 CardioNet reported theft of a laptop that was not encrypted. Laptop had ePHI of 1391 individuals
  - OCR alleged CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft, that CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented

OCR GUIDANCE ON RANSOMWARE

- OCR issued guidance to help companies understand and report breaches
- Explains that any encryption of ePHI by a third party as a result of a ransomware attack means that a breach is presumed
- Entity affected would need to show low probability that information was accessed in order to avoid breach reporting
- https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

RANSOMWARE THREAT

- In 2017, 25% of all events reported to OCR were a result of a ransomware incident https://www.healthcareitnews.com/news/cybercriminals-turning-smaller-providers-and-health-iot-2018

- "The emergence and refinement of advanced ransomware tools lowers both the cost and the time for cyberattackers to target smaller healthcare institutions – now they can cost effectively reach physician practices, surgical centers, diagnostic laboratories, MRI/CT scan centers, and many other smaller yet critical healthcare institutions," (https://www.cryptonitenxt.com/resources/#pg-resources-partners)

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

BREACH CAUSED BY PHISHING

- Metro Community Provider Network (April 2017)
  - Reached a $400,000 settlement for lack of security management process to safeguard e-PHI
  - In January 2012, Hacker accessed multiple employee's email accounts and obtained e-PHI of 3,200 individuals
  - OCR alleged that although MCPN took the necessary corrective action to address the phishing incident, MCPN failed to conduct a risk management until February 2012
  - Prior to the breach, OCR contended that MCPN had failed to conduct any risk analysis to assess the risks and vulnerabilities in its e-PHI environment, and consequentially, had not implemented any corresponding risk management plans to address the risks and vulnerabilities that would be identified in a risk analysis
  - When MCPN did conduct a risk analysis, OCR contended it was insufficient to meet the requirements of the Security Rule

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

RANSOMWARE BREACH

- California providers notifying 85,000 patients due to a ransomware attack on its IT vendor
- Hackers launched a ransomware attack on the computer systems – locking the systems and encrypting the patient data on them
- Notification occurring even though the investigation couldn't determine whether the data was exfiltrated

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

SAMPLE OF HEALTHCARE PROVIDER BREACHES IN 2018

- Hacker accessed employee workstation and breached records of more than 270,000 patients
- Hacker accessed a patient data base and accessed a patient list containing personal data
- Phishing attack on provider allowed hackers to access emails containing e-PHI (42,600 patients affected)
- Malware attached potentially exposed information of 500,000 patients
- Phishing attack jeopardized PHI of 16,000 patients
- https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far

SECURITY RISK ASSESSMENT ANNUAL REQUIREMENTS

WHAT IS A SECURITY RISK ASSESSMENT

- Risk assessment of your practice, as **required by HIPAA** to reveal where protected health information (PHI) can be at risk and ensures compliance
  - **HIPAA Security Rule** requires covered entities (CE) and business associates (BA) to conduct annual risk assessments
  - Three elements to privacy and security risk assessments
    - Physical safeguards
    - Administrative safeguards
    - Technical safeguards
- Provides tips for protecting and securing patient health information on mobile devices
- Educates staff on privacy and security awareness
- Provides tools and guidance for:
  - Planning an EHR implementation or major system upgrades
  - Attesting for Meaningful Use

SRA ANNUAL REQUIREMENTS

- Risk analysis requirements under the Security Rule requires organizations to ***"implement policies and procedures to prevent, detect, contain and correct security violations"***
- Each year your practice needs to assess your risk in these common areas:
  - What e-PHI do you create, receive, maintain or transmit?
  - What external sources of e-PHI exist in your organization?
  - What are the threats to your information systems that contain e-PHI?
- Your risk assessment policies and procedures and risk assessment documentation **MUST** be updated annually to comply with these requirements

MEANINGFUL USE OBJECTIVE AND MEASURES #1

Objective # 1: Protect electronic protected health information (e-PHI)

- Implement technical, administrative, and physical safeguards

Measures:

(1) Conduct or review a security risk analysis annually **45 CFR 164.308(a)(1)**
(2) Data security (includes encryption) **45 CFR164.312(a)(2)(iv)**
(3) Implement security updates and correct security deficiencies **45 CFR 164.306(d)(3**

Source: CMS Security Risk Analysis Tip Sheet, March 2016

PHYSICAL SAFEGUARDS

- Security Rule definition
  - *"Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion"*

Physical Safeguards
Facility Access Control
Workstation Use
Workstation Security
Device and Media Controls

Source: HHS Guidance on Risk Analysis

ADMINISTRATIVE SAFEGUARDS

- Security Rule definition
  - *"Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information"*

Administrative Safeguards		
Security Management Process	Information Access Management	Contingency Plan
Assigned Security Responsibility	Security Awareness and Training	Evaluation
Workforce Security	Security Incident Procedures	Business Associate Contracts and Other Arrangements

Source: HHS Guidance on Risk Analysis

TECHNICAL SAFEGUARDS

- Security Rule definition
  - *"The technology and the policy and procedures for its use that protect electronic protected health information and control access to it"*

Technical Safeguards
Access Control
Audit Controls
Integrity
Person or Entity Authentication
Transmission Security

Source: HHS Guidance on Risk Analysis

HOW TO CONDUCT A SECURITY RISK ASSESSMENT

PERFORMING A SECURITY RISK ASSESSMENT

- Utilize a Security Risk Assessment Tool (ONC SRA Tool) to perform and document your Security Risk Assessment
  - Designed for small to medium size practices and business associates
  - Available on Windows and iOS platforms
  - Guides health care providers and business associates through the standards and implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues

ONC SRA TOOL DEMONSTRATION (1 OF 3)

- Downloading and Installing the SRA Tool
  - SRA tool components
    - General overview
      - Users
      - About practice
      - Business associates
      - Asset inventory
    - Assessment Tool
      - Things to consider
      - Threats and vulnerabilities
      - Examples of Safeguards

ONC SRA TOOL DEMONSTRATION (2 OF 3)

- Downloading and Installing the SRA Tool
  - Reporting and additional tools
    - Report
    - Glossary
    - Navigator
    - Related information
    - Export

ONC SRA TOOL DEMONSTRATION (3 OF 3)

- Safeguards – Key Points
  - Understanding risks to e-PHI and how to address it within the practice
  - Making sure staff understand privacy and security and your policies
  - Disaster recovery and business continuity
  - Practice user and role management to systems including EHR
- Physical Safeguards
  - Practice/Facility access and controls
  - Workstation security
  - Understanding workstation policies
- Technical Safeguards
  - Restrict access e-PHI (authorized personnel)
  - Data integrity (alteration and destructions)
  - Transmission (protect data when transmitted)

SRA BEST PRACTICES

- Avoid using “checklist” options when performing your initial and subsequent SRA submissions
- Conduct an initial SRA and identify any areas that are lacking or could use improvement
- Once these areas are identified, create an action plan to address these areas prior to your next SRA submission
- Even if you have installed and implemented a certified EHR, you must perform a full security risk analysis to fulfill HIPAA Security rule requirements
- Perform subsequent SRA submissions at least on an annual basis thereafter – this means conducting a SRA is not a one and done process

Source: Healthcare Compliance Pros – 5 Best Practices for your Security Risk Analysis

eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM

LINKS & RESOURCES

- ONC Security Risk Assessment Tool
- ONC Security Risk Assessment Videos
- ONC Top 10 Myths of Security Risk Analysis
- ONC - Top 10 Tips for Cybersecurity in Health Care
- ONC Guide to Privacy and Security. Version 2. April 2015
- ONC - Mobile Devices and Privacy and Security
- Health IT Playbook - Section 7: Privacy & Security
- CMS Security Risk Analysis Tip Sheet. March 2016
- HIS HIPAA Security Checklist
- OCR - Model Notices of Privacy Practices
- OCR Guidance on Risk Analysis Requirements

QUESTIONS?