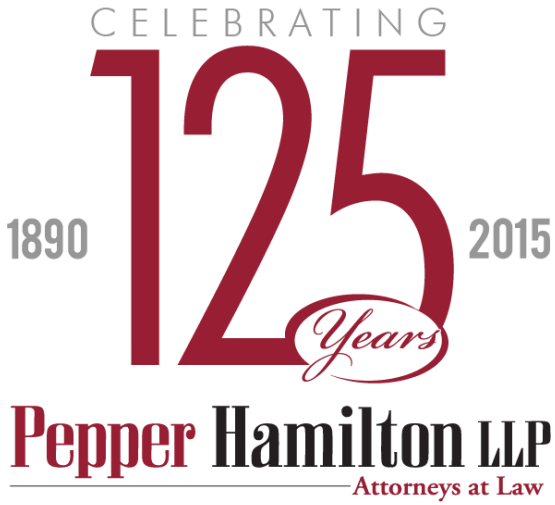
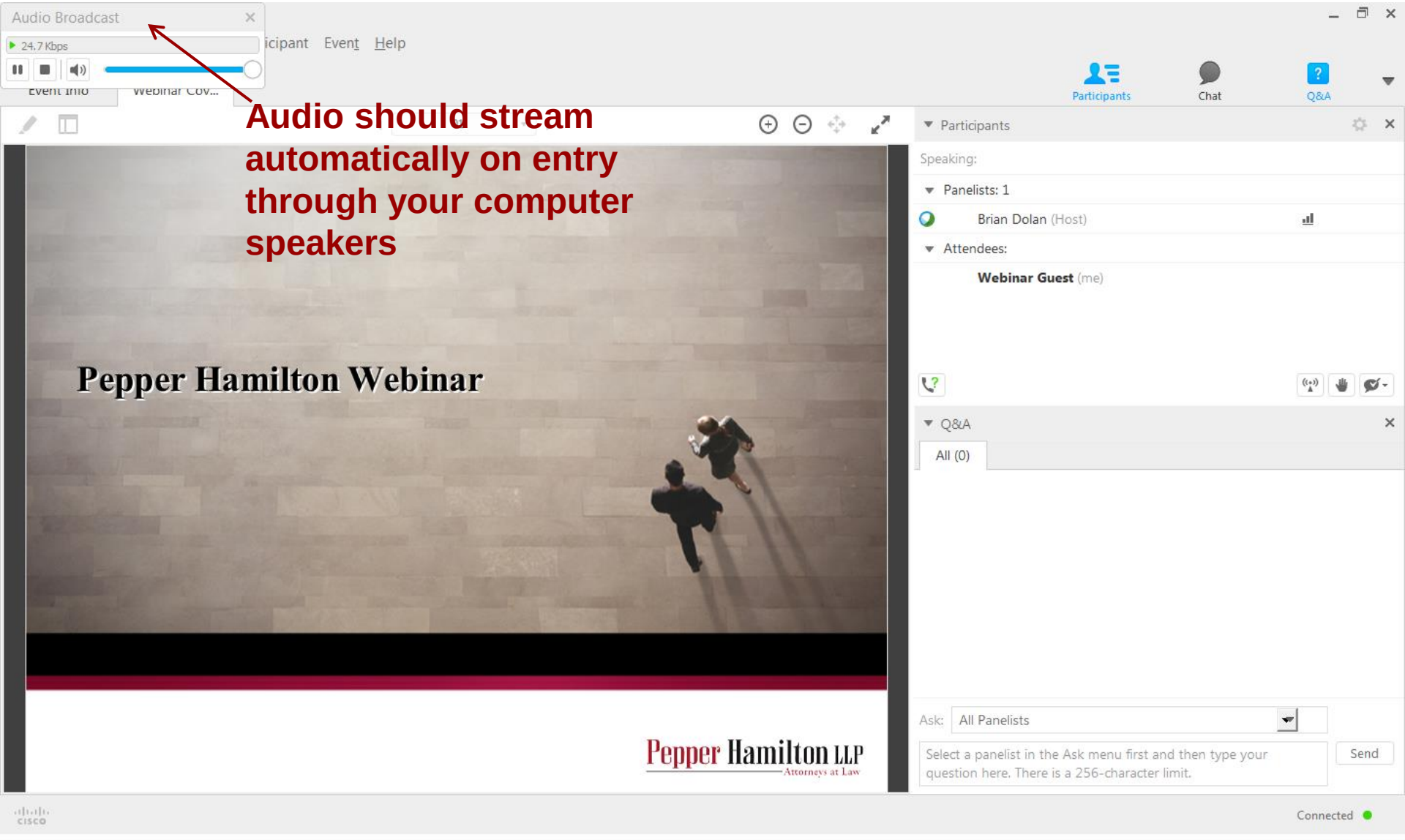
Beam It Up Safely:
Navigating Data Privacy and Security In Telemedicine's Uncharted Territory

Sharon Klein, Esq.
Rebekah Monson, Esq.
Dayna Nicholson, Esq.

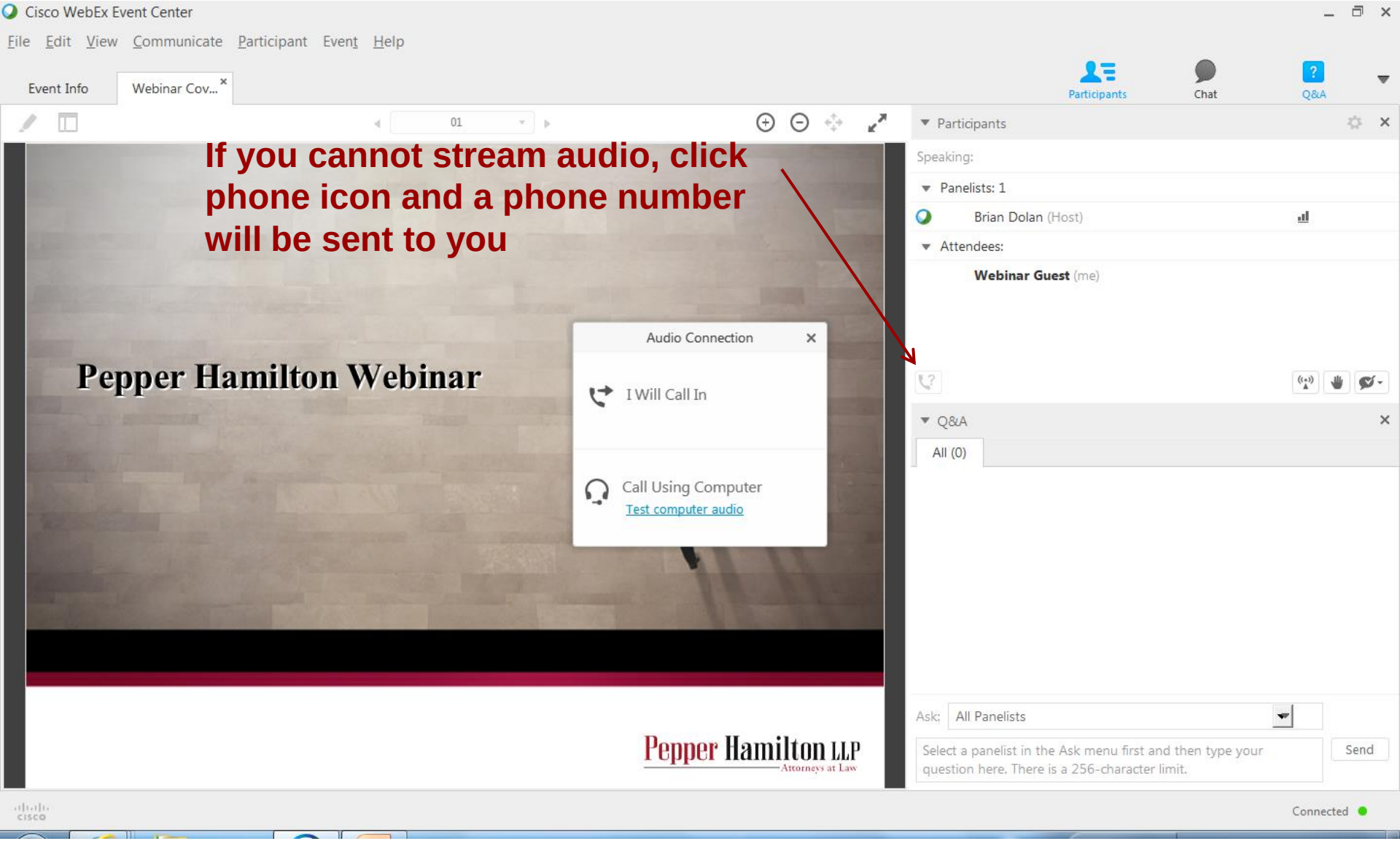


Pepper Webinar | September 17, 2015

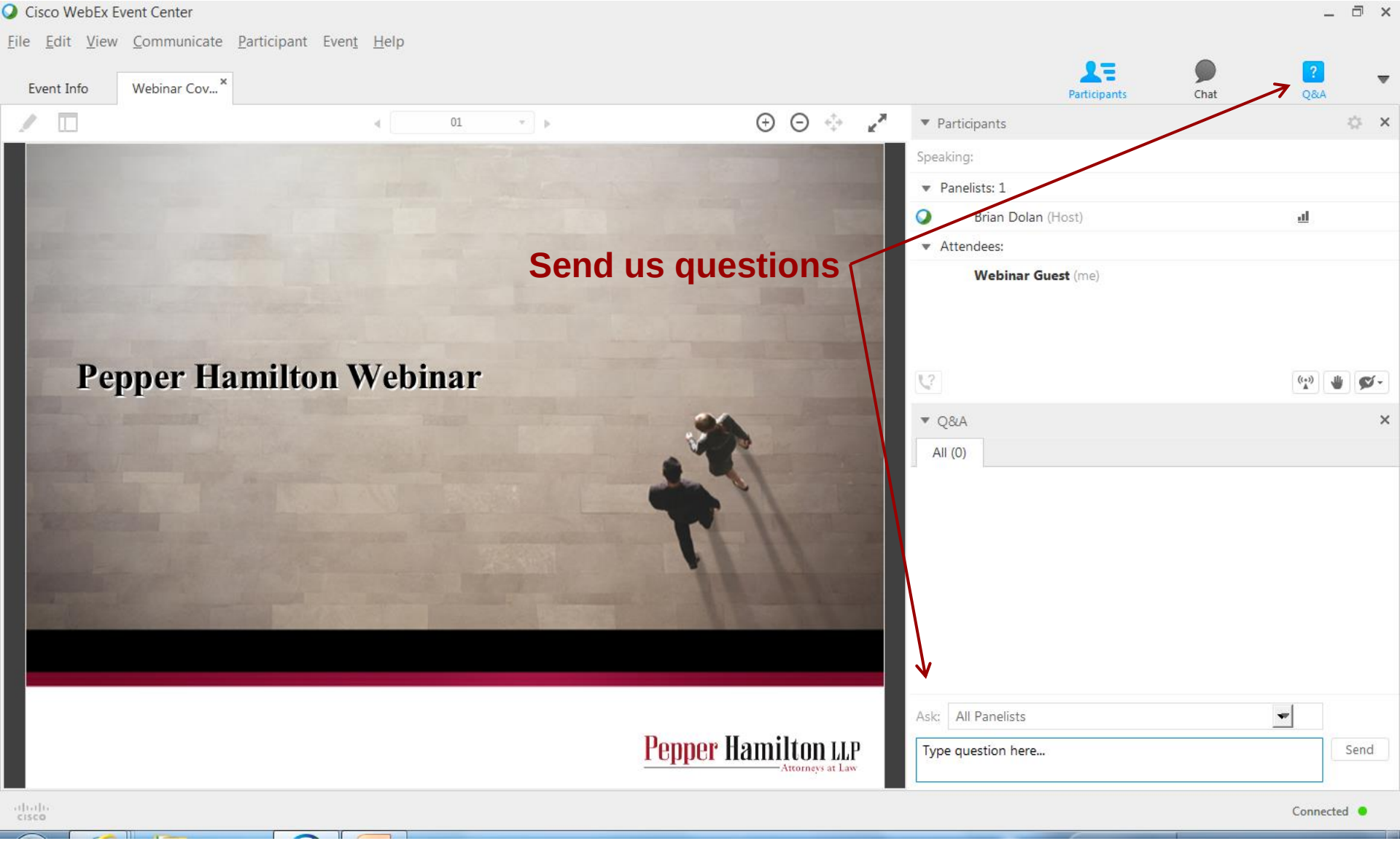
Audio


Audio Broadcast
24.7 Kbps
Event
Help
Participants
Chat
Q&A
Audio should stream automatically on entry through your computer speakers
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Pepper Hamilton Webinar
Pepper Hamilton LLP
Attorneys at Law
Ask:
All Panelists
Select a panelist in the Ask menu first and then type your question here. There is a 256-character limit.
Send
Connected

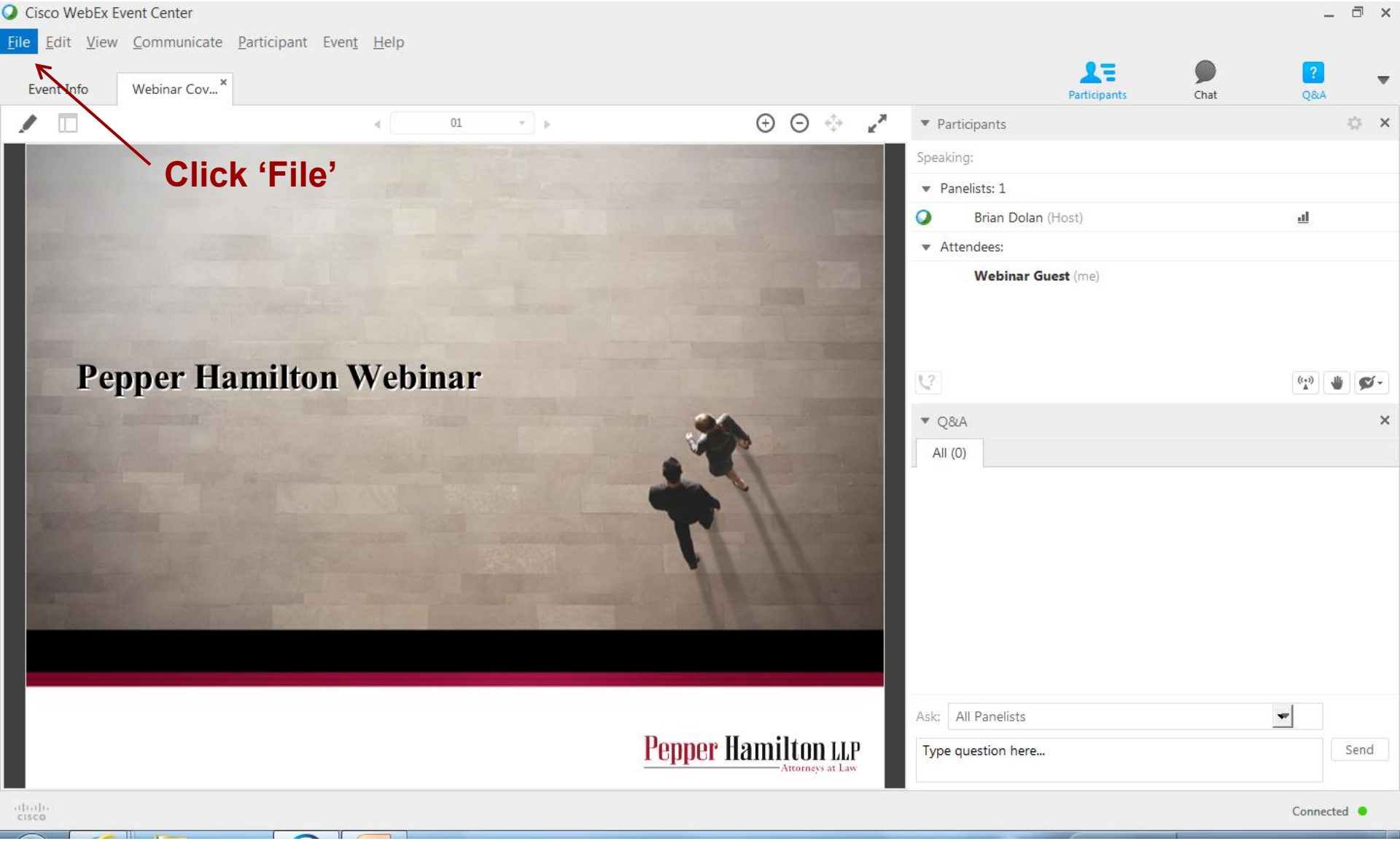
Audio


Cisco WebEx Event Center
File Edit View Communicate Participant Event Help
Event Info
Webinar Cov...
Participants
Chat
Q&A
If you cannot stream audio, click phone icon and a phone number will be sent to you
Pepper Hamilton Webinar
Audio Connection
I Will Call In
Call Using Computer
Test computer audio
Pepper Hamilton LLP
Attorneys at Law
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Ask: All Panelists
Select a panelist in the Ask menu first and then type your question here. There is a 256-character limit.
Send
Connected

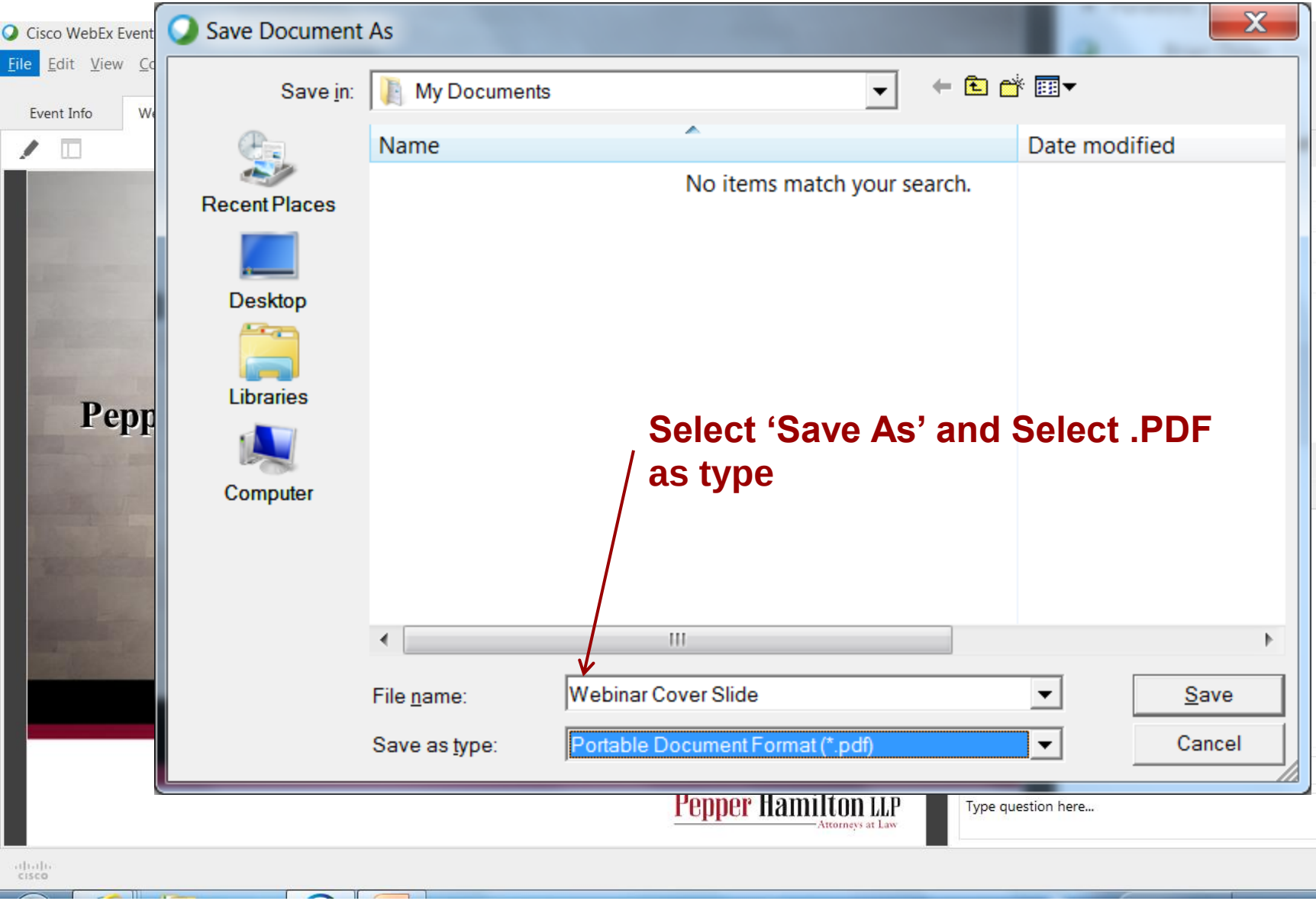
Q&A


Cisco WebEx Event Center
File Edit View Communicate Participant Event Help
Event Info
Webinar Cov...
Participants
Chat
Q&A
Send us questions
Pepper Hamilton Webinar
Pepper Hamilton LLP
Attorneys at Law
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Ask:
All Panelists
Type question here...
Send
Connected

Download PPT Slides



Download PPT Slides



CLE credit available in CA, NY, PA, VA (pending), NJ (credit available through reciprocity).

Contact Brian Dolan at dolanb@pepperlaw.com for CLE form

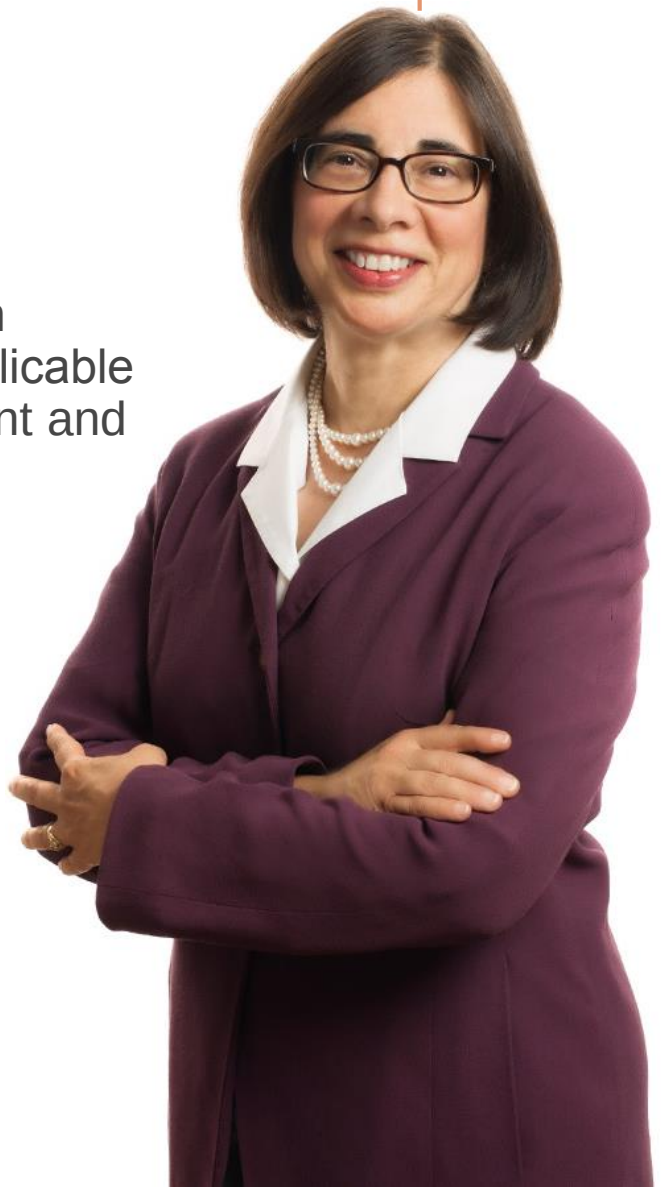
Sharon R. Klein

Partner and Chair | Privacy, Security and Data Protection Practice Group
Member | Health Care Services Practice

949.567.3506

kleins@pepperlaw.com

- Advises businesses on planning, drafting and implementing privacy, security and data protection policies and “best practices”, compliance with applicable laws, regulations and rules, and crisis management and litigation strategies for non-compliance.
- Represents health care industry clients in the licensing of information technology and medical devices
- Certified as an information privacy professional by the International Association of Privacy Professionals (IAPP).
- Frequent writer and presenter on privacy, security and data protection matters.



CELEBRATING 1890 125 Years 2015 Pepper Hamilton LLP Attorneys at Law

Rebekah A. Z. Monson

Senior Attorney | Privacy, Security and Data Protection Practice Group
Member | Health Care Services Practice
215.981.4031
monsonr@pepperlaw.com

- Advises health care providers (including physicians and physician groups) on the issues presented by the implementation of information technologies in the health care industry, including telemedicine, computerized patient records, electronic medical communications and electronic health records and the associated legal issues, such as privacy, identity theft, compliance, licensing and payment concerns.
- Regularly counsels clients on compliance with the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act and other federal and state laws relating to privacy, confidentiality and security of health information.

Associate | Privacy, Security and Data Protection Practice Group

Member | Health Care Services Practice

213.928.9807

nicholsond@pepperlaw.com

- Focuses her practice on health care–related matters, such as licensing and other regulatory compliance, peer review and credentialing and corporate and medical staff governance.
- Clients include hospitals, medical staffs, managed care organizations, medical groups, medical device retailers and other health care providers.
- Experienced in patient information privacy issues, appeals of state-issued administrative penalties, Medicare and Medi-Cal certification, emergency care requirements and litigation arising out of peer review matters.

Agenda

- Basic Principles of Telemedicine
- Privacy and Security Considerations
- Telemedicine in Action
- Best Practices
- Questions?

Basic Principles

Key Definitions

- Telemedicine is the practice of medicine using electronic communications, information technology or other means between a licensee in one location, and a patient in another location with or without an intervening health care provider. (Federation of State Medical Boards)
- Telehealth is a broader term than telemedicine because the term does not always refer to clinical services. Telehealth includes remote monitoring, telepharmacy, regional health information sharing, and non-clinical services, such as education programs, administration, and public health.

Basic Principles

Telemedicine vs. Telehealth

- Types of Telemedicine:
  - **Non-simultaneous**: involve after-the-fact interpretation or assessment, such as teleradiology services
  - **Simultaneous**: involve "real-time" interpretation or assessment, such as telestroke and teleICU services
- (Generally) NOT Telemedicine:
  - Informal consultations between practitioners
  - Telephone conversation, e-mail/instant messaging conversation, or fax
- Telemedicine and telehealth are **tools** in medical practice, not a distinct service.

Basic Principles

Telemedicine Participants

- Patient
- On Site Provider – health care provider that is with the patient at the time of service
  - Treating Provider
  - Allied Health Professionals
- Remote Provider
  - Treating Provider – provider that has a treatment relationship with the patient at the originating site
  - Consulting Provider – provider at a distant site that is being consulted by the treating provider; often specialty telemedicine consultations

Basic Principles

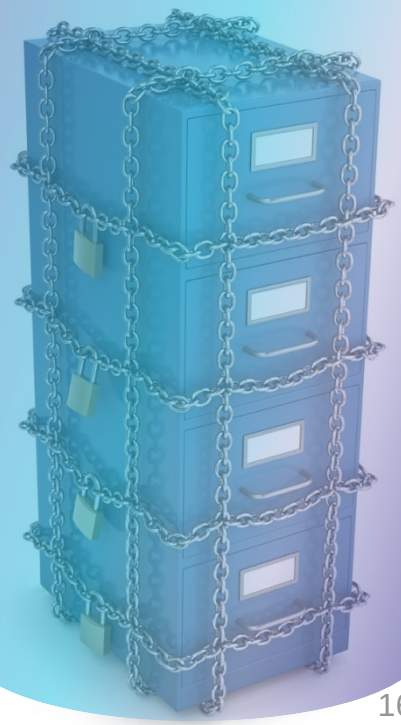
Telemedicine Participants

- Technology Vendor
  - Device – the hardware that is being used to conduct the telemedicine session (*e.g*. iPad, cell phone, computer)
  - Software/Application – the program or application that is being used to conduct the telemedicine session
- Telecom Carrier
- Payor – Medicare, Medicaid, private payors

HIPAA Privacy and Security Considerations

HIPAA/HITECH Privacy and Security Laws & Regulations

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH) (American Recovery and Reinvestment Act of 2009)
- HIPAA Rules: 45 C.F.R. Parts 160, 162, 164 (Final Omnibus Rule: 01/25/13, Compliance date: 09/23/13)
- Enforcement
  - Civil and criminal penalties
  - HHS/OCR, DOJ, SAG



HIPAA Privacy and Security Considerations

What is PHI?

- "individually identifiable health information" (IIHI), including demographic information collected from an individual, that:
  - is created or received by a health care provider, health plan, employer or health care clearinghouse, and
  - relates to: (a) the past, present, or future physical or mental health or condition of an individual; (b) the provision of health care to an individual; or (c) the past, present or future payment for the provision of health care to an individual; and
  - identifies the individual OR there is a reasonable basis to believe the information can be used to identify the individual; and
  - is transmitted or maintained by electronic media or in any other form or medium

HIPAA Privacy and Security Considerations

What is Not PHI?

- Exception for de-identified information
  - Information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual – is not PHI
  - Safe harbor for de-identification of PHI
    - Removal of 18 specified direct identifiers (*e.g.*, name, DOB, SSN, medical record number, phone number, etc.)
    - Medical information expert determination
- Guidance Regarding Methods for De-Identification of Protected Health Information (November 2012)

HIPAA Privacy and Security Considerations

Who is Responsible?

- Covered Entity (CE)
  - Health care provider who conducts electronic transactions
    - Institutional providers
    - Non-institutional providers
    - “any other person or organization who furnishes, bills, or is paid for health care in the normal course of business”
  - Health plan
  - Health care clearinghouse

HIPAA Privacy and Security Considerations

Who is Responsible?

- Business Associate (BA)
  - Creates, receives, maintains or transmits PHI on behalf of a Covered Entity

    OR
  - Provides certain services (identified in the Rule) involving PHI, to or for, a Covered Entity
    - Examples: actuarial, legal, accounting, consulting, management, administrative, financial
- Data transmission providers
  - Routine access to PHI versus mere conduit

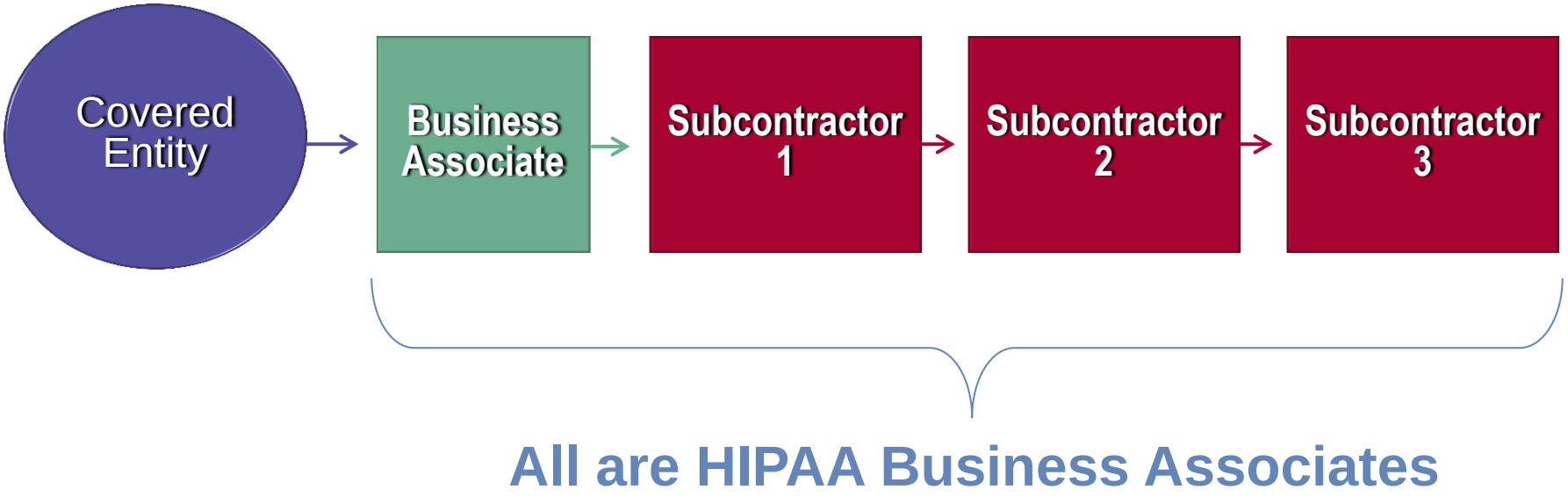
HIPAA Privacy and Security Considerations

Subcontractor Business Associates

- Business associate includes: (iii) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate
- Subcontractor – person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate

HIPAA Privacy and Security Considerations

Down the Chain



HIPAA Privacy and Security Considerations

What is a Business Associate Agreement?

- Business Associate Agreement (BAA) = Contract between a CE and a BA (or a BA and a Subcontractor) that defines the BA's (Subcontractor's) obligations to protect PHI
- Business Associates/Subcontractors must execute a BAA with the Covered Entity/upstream Business Associate:
  - prior to the use/disclosure of PHI from a Covered Entity to the business associate, and
  - prior to the use/disclosure of PHI to a subcontractor

HIPAA Privacy and Security Considerations

Key Concept: What goes into Business Associate Agreements?

- Required provisions include:
  - All uses/disclosures must be permitted by contract or required by law
  - BA will use appropriate safeguards, including compliance with the Security Rule
  - BA must comply with Privacy Rule to extent BA carries out CE's privacy obligations
  - BA required to report to the CE (or upstream BA) breaches of unsecured PHI
  - Must have a BAA with Subcontractors that is as (or more) restrictive
- Other Negotiable provisions
- Transition period – September 22, 2014

HIPAA Privacy and Security Considerations

Key Concept: Individual Rights and Notice of Privacy Practices

- HIPAA provides individuals with certain rights regarding their health information maintained by a Covered Entity
  - Right of access
  - Right of amendment
  - Right to request privacy protections
    - restrictions
    - communication by alternate means
  - Right to an accounting of disclosures
- Notice of Privacy Practices

HIPAA Privacy and Security Considerations

Key Concept: HIPAA Security

- Privacy Rule – includes mini security rule
  - administrative, technical and physical safeguards to protect privacy of PHI
- Security Rule regulations for secure storage, maintenance and transmission of ePHI
- Security Rule requirements:
  - administrative, technical and physical safeguards for e-PHI
  - document requirements of policies, procedures, etc.
  - required and addressable implementation specifications
- Key administrative safeguard:
  - implement a Security Management process
    - Risk assessment a critical component

HIPAA Privacy and Security Considerations

Key Concept: Breach Notification

- A Breach of PHI = the acquisition, access, use or disclosure of PHI in a manner that:
  - Is not permitted by HIPAA, and
  - Compromises the security or privacy of PHI
- A non-permitted use, disclosure, etc. of PHI is presumed to be a breach, unless a risk assessment shows that there is a "low probability" that PHI has been compromised
- Notification required for breaches of "unsecured PHI"

Other Privacy and Security Considerations

State Law Issues

- Laws requiring private or government entities to notify individuals of security breaches of personally identifiable information are on the books in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands
- States with no security breach law: AL, NM, SD
- Many (not all) of the applicable laws are listed here: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (National Conference of State Legislatures)

Other Privacy and Security Considerations

- Telemedicine vs. mHealth
  - Chat messaging software between patients and health care providers
  - Health applications with patient-entered data
  - Remote patient monitoring devices and privacy collection
- Is it a HIPAA issue?
  - Federal Trade Commission
    - Internet of Things
  - Food and Drug Administration
  - Federal Communications Commission

Telemedicine in Action

Practical Goals from CMS' Telemedicine Rule

1. Enable patients to receive medically necessary interventions in a more timely manner
2. Enhance patient follow-up in the management of chronic disease conditions
3. Provide more flexibility to small hospitals and CAHs in regions with a limited supply of primary care and specialized providers
4. Create a more cost-effective alternative to traditional service delivery approaches
5. Improve patient outcomes and satisfaction

Telemedicine in Action

Recent Telemedicine Trends

- Arrangements between two health care entities
- Partnerships between health insurers and integrated health care delivery systems connecting specialists to rural communities
- Agreements between telemedicine entities and health insurers/employers to include coverage for virtual visits
- Agreements among retail pharmacies, vendors, and health care entities or physician groups
- Concierge and on-demand virtual clinical encounters
- Rapid development of mobile technology and mobile medical applications

Telemedicine in Action

Scenarios: Questions to Consider

- Does HIPAA apply?
  - Is there PHI?
  - Are there Covered Entities?
- Are there Business Associates?
- Business Associate Agreement v. Service Agreement
- Physical security issues
- Data collection, transmission, access/use, disclosure, storage, ownership
- State law
- FTC Section 5

Telemedicine in Action

Scenarios: Web/Mobile App

Patient

Physician

Telecom Provider

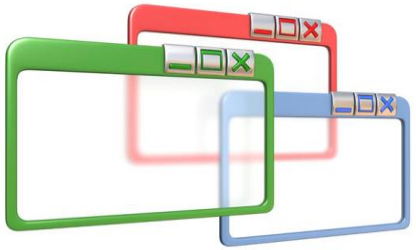
Telecom Provider

Website / Mobile Application

Telemedicine in Action

Scenarios: Teleradiology

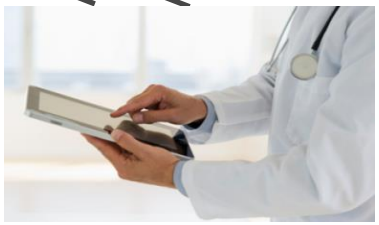
Patient



diagnosis

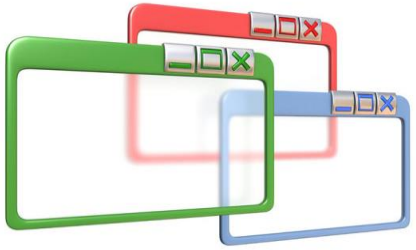
Hospital ED

Software
(Vendor)



Teleradiology
Physician

data



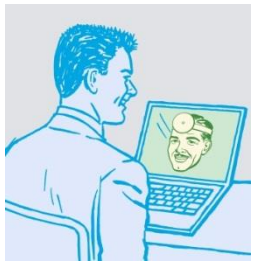
Telemedicine in Action

Scenarios: Walk-In Clinic/Video Exam

AHPs

Walk-In Clinic

data



Video Exam

data

Physician

Patient

Best Practices

Preparing for the Relationship

- Telemedicine Policies and Procedures
  - Licensing and credentialing of health care providers
  - Patient privacy during the telemedicine session
  - Scope of telemedicine encounters and types of transactions that will be permitted at the facility
  - Patient intake and consent process
  - Medical record documentation requirements for telemedicine sessions
  - Clinical guidelines
  - Equipment safety
  - Updating and revising policies and procedures
- Internal risk assessment/data mapping/technology inventory of your current operations

Best Practices

Preparing for the Relationship

- Policies and procedures specific to data privacy and security.
  - HIPAA and HITECH (administrative, physical, and technical safeguards)
  - Breach Notification Requirements
  - FTC Guidance (transparency and clear notice to consumers)
  - State-specific rules
- Create compliant business associate agreements and implement required business associate practices.

Remember: All subcontractors having access to protected health information (no matter how far down the chain) must now comply with the full spectrum of requirements applicable to business associates.

Best Practices

Setting up the Relationship

- Types of Telemedicine Agreements
  - Provider / Telemedicine Service Agreement
  - Equipment Agreement
  - Technology / Software Licensing Agreement
  - Business Associate Agreement
  - Management Services Agreement
  - Collaborative or Supervising Agreement
  - Terms of Use

Best Practices

Setting up the Relationship

- Business Associate and Service Agreements
  - Identify business associates in the telemedicine chain: who will have access to information, including vendors and subcontractors
  - General issues between covered entities and business associates
  - Service Agreement issues between covered entities
- Data mapping
  - What information is being collected, communicated, and stored, and for what purpose
  - How should information be shared and where it will be stored
  - How will distant-site telemedicine practitioners use, store and maintain PHI for patient care and health care liability purposes
- Risk assessment must address the “lifetime” of the PHI in the relationship

Best Practices

Managing the Relationship

- Periodic audits/assessments
- Breach notification
- Communication and Training

Best Practices

Terminating the Relationship

- Reasons for termination
  - Poor performance in security audit
  - Frequent security incidents or breaches
  - Failure to mitigate a breach
- Post-termination obligations
  - Access to medical records for health care professionals
  - Destruction of protected health information for business associates

Questions?

Sharon Klein, Esq.
kleins@pepperlaw.com
949.567.3506

Rebekah Monson, Esq.
monsonr@pepperlaw.com
215.981.4031

Dayna Nicholson, Esq.
nicholsond@pepperlaw.com
213.928.9807

CLE credit available in CA, NY, PA, VA (pending), NJ (credit available through reciprocity).

Contact Brian Dolan at dolanb@pepperlaw.com for CLE form