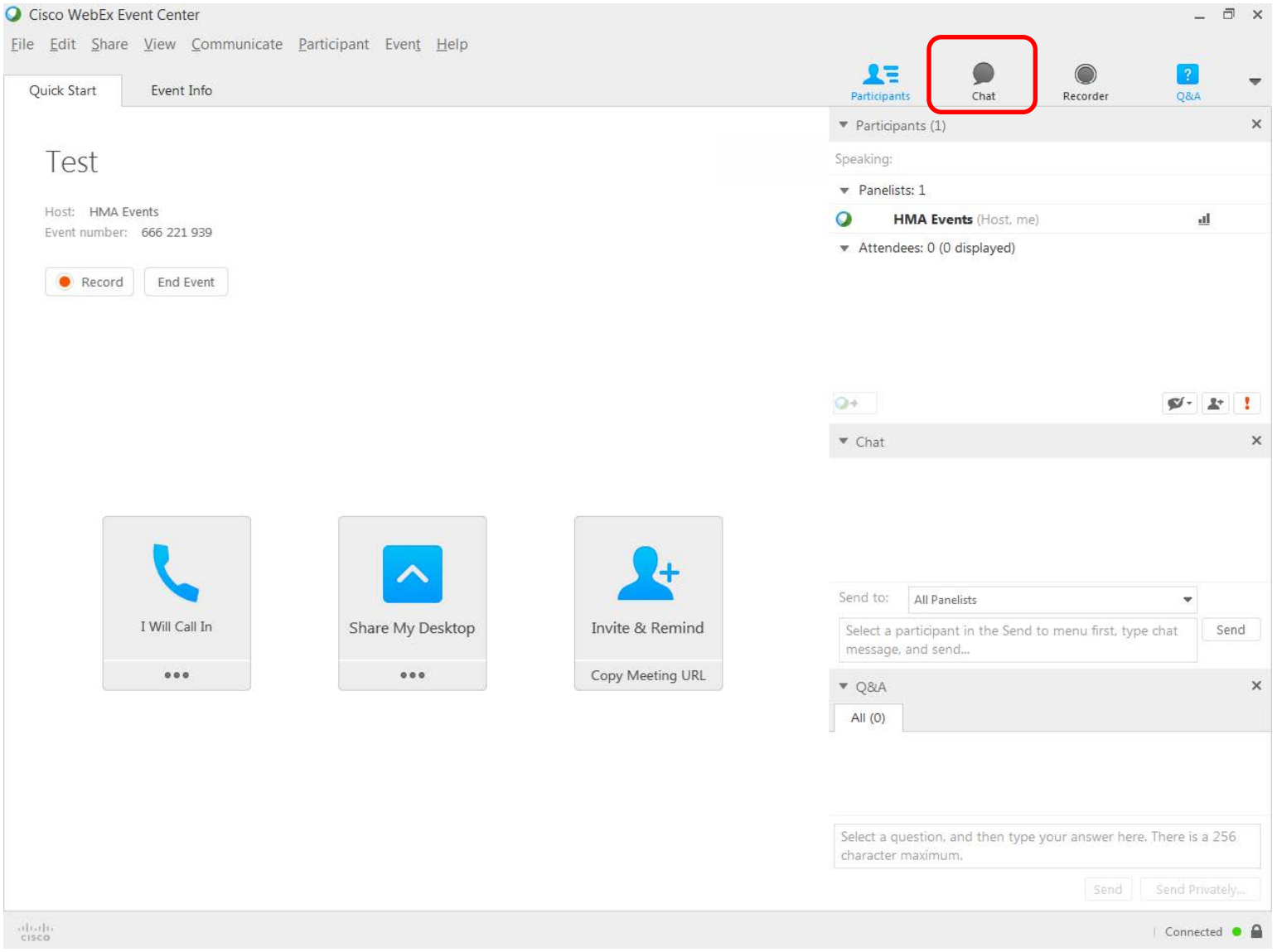
HEALTH MANAGEMENT ASSOCIATES

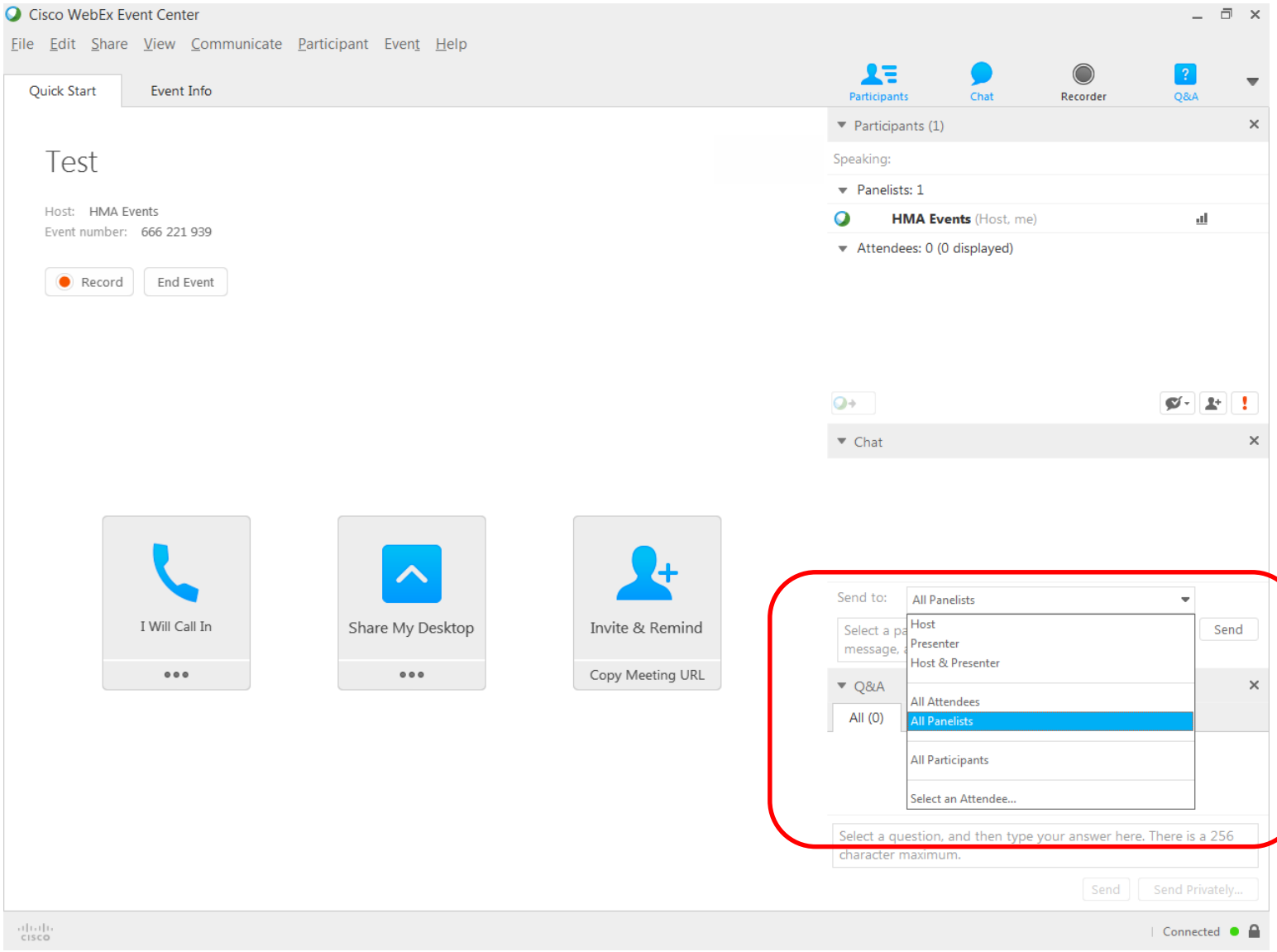
Business Associates Redefined:
What Healthcare Organizations Need to Know to Comply with Strengthened HIPAA Regulations

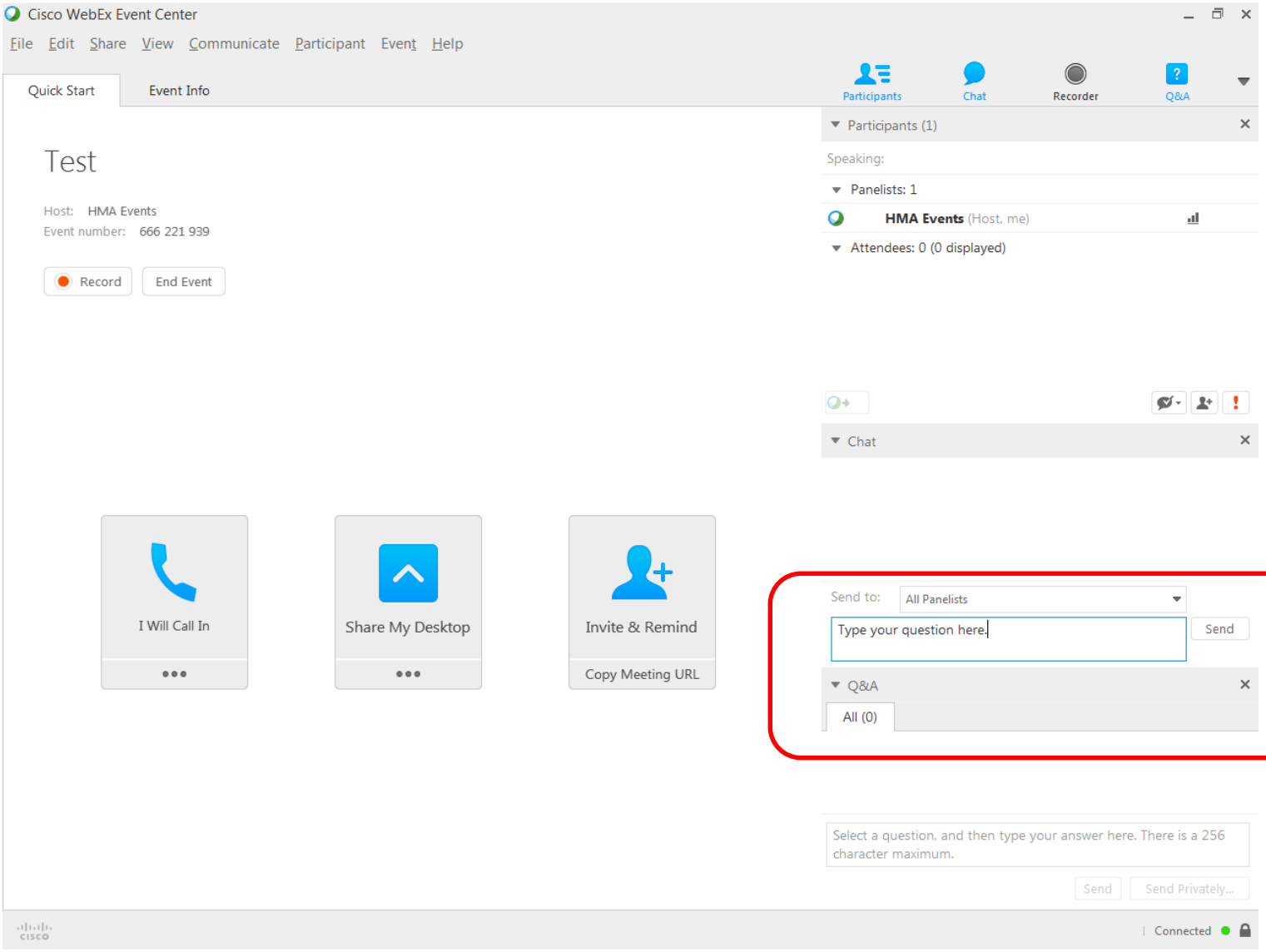
Speakers:

Margarita Pereyda, MD, Principal
Heidi Robbins Brown, JD, Principal

April 26, 2016

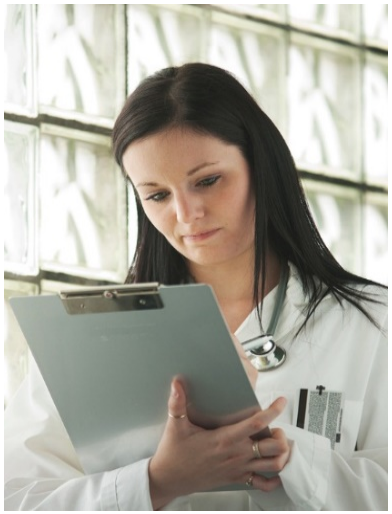

Cisco WebEx Event Center
File Edit Share View Communicate Participant Event Help
Quick Start
Event Info
Participants
Chat
Recorder
Q&A
Test
Host: HMA Events
Event number: 666 221 939
Record
End Event
I Will Call In
Share My Desktop
Invite & Remind
Copy Meeting URL
Participants (1)
Speaking:
Panelists: 1
HMA Events (Host, me)
Attendees: 0 (0 displayed)
Chat
Send to:
All Panelists
Select a participant in the Send to menu first, type chat message, and send...
Send
Q&A
All (0)
Select a question, and then type your answer here. There is a 256 character maximum.
Send
Send Privately...
Connected


Cisco WebEx Event Center
File Edit Share View Communicate Participant Event Help
Quick Start
Event Info
Participants
Chat
Recorder
Q&A
Test
Host: HMA Events
Event number: 666 221 939
Record
End Event
Participants (1)
Speaking:
Panelists: 1
HMA Events (Host, me)
Attendees: 0 (0 displayed)
Chat
I Will Call In
Share My Desktop
Invite & Remind
Copy Meeting URL
Send to:
All Panelists
Host
Presenter
Host & Presenter
All Attendees
All Panelists
All Participants
Select an Attendee...
Send
Q&A
All (0)
Select a question, and then type your answer here. There is a 256 character maximum.
Send
Send Privately...
Connected


Cisco WebEx Event Center
File Edit Share View Communicate Participant Event Help
Quick Start
Event Info
Participants
Chat
Recorder
Q&A
Test
Host: HMA Events
Event number: 666 221 939
Record
End Event
Participants (1)
Speaking:
Panelists: 1
HMA Events (Host, me)
Attendees: 0 (0 displayed)
Chat
I Will Call In
Share My Desktop
Invite & Remind
Copy Meeting URL
Send to: All Panelists
Type your question here.
Send
Q&A
All (0)
Select a question, and then type your answer here. There is a 256 character maximum.
Send
Send Privately...
Connected

Introduction

Revised HIPPA rules and audit protocol have created important new responsibilities and instituted new penalties related to business associates who handle personal health information or personal health records for covered entities.



Navigating the Regulatory Environment

- Understand the new enforcement tools and penalties established by the strengthened HIPAA regulations and identify your organizations most likely areas of vulnerability.

- Obtain best practices for HIPAA compliance and ensuring accountability.

- Know how the Office of Civil Rights selects audit targets, what to expect from an audit, and how to be best prepared.

HIPAA and HITECH

- HIPAA, the Health Insurance Portability and Accountability Act, was passed to allow people to carry insurance from one employer to another and to protect the privacy of patient's personal health information
- The stimulus bill, officially titled the American Recovery and Reinvestment Act (ARRA), includes a section called the Health Information Technology for Economic and Clinical Health Act (HITECH), which changed some of the provisions of HIPAA—especially in terms of enforcement
- You will learn how to comply with HIPAA as amended by the HITECH ACT

HITECH ACT

- Was mainly created to incentivize the healthcare industry to adopt Electronic Health Record systems (EHRs)
- Because EHRs have a greater risk of being compromised, increased safeguards were needed to ensure their protection
- HITECH ACT
  - Strengthened elements of the privacy rule
  - Directed HHS to conduct regular audits to ensure compliance
  - Authorized states Attorneys General to bring actions under HIPAA

HIPAA Omnibus Rule

Three critical enhancements to the original HIPAA legislation were added within the Omnibus Rule effective September 2013:

- Enhanced breach notification requirements
- Increased the kind of entities that are considered Business Associates and increased all Business Associates liability
- Increased and enhanced HHS fining authority for breach

Penalties for Non-Compliance

- Disciplinary Action
- Personal criminal penalties under the law and personal fines of up to $250,000
- For each incidence of non-compliance, organizations can be fined $50,000 for each occurrence and up to $1.5 Million per year for each standard violated

Who Has to Comply?

- Two types of organizations must comply with HIPAA----**Covered Entities (**healthcare providers, health plans and healthcare cleaning houses) and **Business Associates**
- Under HIPAA Covered Entities must:
  - Safeguard PHI when they store or transmit it
  - Request use or disclose PHI only as permitted by HIPAA
  - Provide individuals certain rights with respect to PHI as required by HIPAA
  - Provide a privacy notice that explains rights under HIPAA
  - Ensure group health documents comply with HIPAA, if applicable
  - Create HIPAA Privacy and Security policies and procedures
  - Appoint a Privacy Officer and Security Officer

Who Has to Comply?

- **Business Associates** - companies or individuals who perform services for covered entities and who have access to PHI from covered entities
- Examples of functions performed by **Business Associates** include:
  - Claims Processing
  - Pharmacy Benefit Manager
  - Management Consulting
  - Accounting Services
  - Administrative Services
  - Actuarial Services
  - Legal Services
  - Billing

Rules for Business Associates

- Before sharing PHI with a Business Associate (BA), the Covered Entity and BA must first sign a Business Associate Agreement (BAA)
- The BAA binds the BA to comply with all HIPAA Privacy and Security rules and regulations
- No PHI should be shared with a BA who has not signed a BAA contract
- HITECH additionally changed HIPAA so that many provisions of HIPAA are directly applicable to BA
- This means that BA:
  - Are subject to periodic audits
  - Are subject to fines, penalties and regulatory actions

MARCH 16, 2016 - $1.55 million settlement underscores the importance of executing HIPAA business associate agreements

- North Memorial Health Care of Minnesota paid $1,550,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to enter into a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information.
- "Two major cornerstones of the HIPAA Rules were overlooked by this entity," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). "Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure."

Scope of HIPAA

- HIPAA applies to both public and private sectors
- HIPAA applies nation wide
- States may have additional Privacy and Security standards that work alongside HIPAA, these may be stricter and it is important we always check specific state regulations when entering new markets
  - Texas House Bill 300
  - 201 Commonwealth of Massachusetts Regulations (CMR)17
  - Washington has a Health Care Information Act and laws restricting information sharing of health care, mental health, STD and domestic violence information)

Don't Forget: 42 CFR Part 2

42 CFR Part 2, Alcohol and Drug Treatment Program Information, pertains solely to alcohol and drug treatment programs which received federal assistance and limits their disclosure of information (called "Part 2 information") that could identify an individual, directly or indirectly, as having a current or past drug or alcohol problem or as a participant in a treatment program.

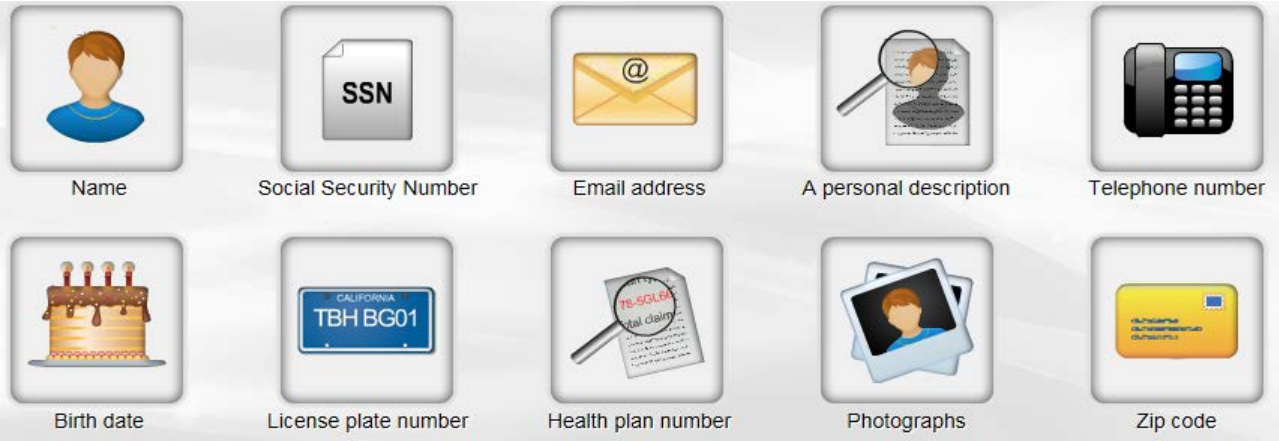
- Part 2 programs are categorized as health providers under HIPAA.
- Part 2 Information is PHI and because 42 CFR Part 2's requirements are more protective than HIPAA, where the two laws conflict, 42 CFR Part 2 takes precedent.

What Information is Protected?

- PHI is all information stored or transmitted by a covered entity or BA, in any form or media, whether electronic, paper or spoken that relates to:
  - An individuals past, present or future physical or mental health
  - The provision of healthcare to an individual
  - Past, present or future payment for the provisions of healthcare to an individual where the information identifies the individual or gives a reasonable basis for identifying the individual

Reasonable Basis for Identification

Below are examples of information that can identify an individual. If you are unsure whether information should be treated as PHI, contact our Privacy Officer



HIPAA Security Rule

Security Rule Requirements:

- All HIPAA covered entities must continue to be in compliance with the Security Rule; states are covered entities.

- The Security Rule creates generally accepted security standards and requirements for PHI.

"Security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entity organizations and technology change."

- CMS Security Website

HIPAA Security Rule

Covered Entities should consider the following:

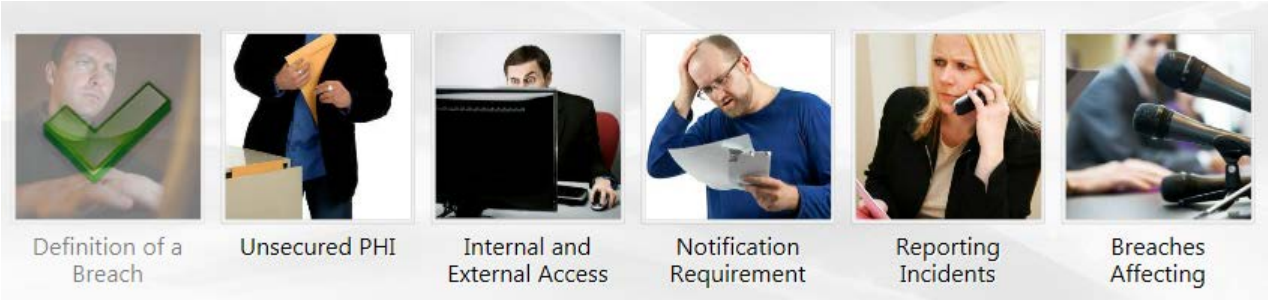
- Assess current security environment, current and potential risks, and identify gaps
- Develop an implementation plan
  - Read the Security Rule (the matrix at the end is very helpful);
  - Review and address implementation specifications; and
  - Determine security measures to address specific PHI uses
- Implement solutions – security measures reasonable and appropriate for the project that address administrative, physical and technical safeguards
- Document decisions
- Reassess periodically

Reporting and Mitigating HIPAA Breaches

- The Privacy Officer is responsible for collecting information about possible HIPAA breaches and notifying the proper parties when a breach occurs
- Because of the HITECH Act, in many instances, breaches notifications are mandatory
- If you suspect a breach occurred within our organization or with one we share PHI with, notify the Privacy Officer immediately

Privacy Breach Notification Requirements

When a breach occurs the Privacy Officer will notify the Covered Entity and a breach notice will be sent to the affected individual(s), media (if applicable), and HHS as required by the HITECH Act



Definition of a Breach

- A breach has occurred when unsecure PHI has been acquired, accessed, used, or disclosed in violation of the Privacy Rule and the disclosure compromises the security or privacy of the PHI, unless one of three exceptions applies (these will be discussed in detail later in the presentation):
  - Innocent access in the course of your duties
  - Innocent internal disclosure
  - Retention is not possible

Unsecured PHI

- Unsecure PHI is PHI that has not been rendered unusable, unreadable, or indecipherable through either encryption or destruction
- Example: Dr. Pereyda leaves her laptop at the airport Starbucks and is freaking out about the volumes of PHI she has on it. Is this a breach?
  - Luckily the data is encrypted and the encryption key does not appear to have been broken……so no, this is not a breach
  - What if instead of a laptop, she left a folder with lists of individuals who have been referred via e-consult?

Internal and External Access

- The notification requirement applies not only to unauthorized disclosures to outside parties, but also to intentional unauthorized access to PHI by people within our organization
- An employee intentionally snooping through files could trigger the notification process
- Employee conduct is one of the most vulnerable areas for organizations and HHS has levied serious fines:
  - New York Presbyterian and Columbia University

Notification Requirement

- A Covered Entity must notify affected individuals of any breach of privacy
- **A BAA must notify the Covered Entity it serves of a breach so the Covered Entity can notify the affected individuals**
- In addition Personal Health Record vendors must notify affected individuals

Reporting Incidents

- If you discover PHI has been accessed without appropriate authorization, you should notify the Privacy Officer immediately
- Our organization is required to conduct and document an analysis of the use or disclosure to determine if a breach occurred

Breaches Affecting More than 500 Individuals

- A Covered Entity with a breach affecting more than 500 individuals must notify HHS immediately and will be listed on the HHS website
- Prominent media outlets must also be notified of the breach
- **BAs must notify the Covered Entity and they are responsible for notifying HHS, individuals and the media**

Exceptions to the Breach Notification Requirement

- The Privacy Officer will determine whether a breach occurred and who needs to be notified
- Only the Privacy Officer or designee should have contact with the media
- The 3 Exceptions:
  - Innocent access in the course of your duties
  - Innocent internal disclosure
  - Retention is not possible

Determining if an Incident is a Breach

- First we determine if there has been impermissible use, acquisition or disclosure
- Second we determine if the information was unsecured
- Third we conduct a risk analysis to determine if the breach poses a significant risk to the individual, taking into account:
  - Nature of the unauthorized recipient (subject to privacy laws vs not)
  - Nature of the PHI (specific information on treatment or diagnosis vs just fact someone was seen at a hospital)
  - Whether the PHI went further than the unauthorized recipient (reliable unauthorized recipient)

Exception #1: Innocent Access in Course of Work

- If you unintentionally and in good faith access PHI in the course of your duties and do not further disclose it---generally not considered a breach
- HOWEVER, it is still an unauthorized use or disclosure and should be reported to our Privacy Officer
- Even though not a breach and therefore does not require notification, we are expected to document the violation and our reasons for why it is not a breach. This also allows us to ***proactively*** look for risks in our processes

Exception#2: Innocent Internal Disclosure

- If you are authorized to use PHI and you inadvertently disclose to another person in our organization who is also authorized to use PHI (but not the one you disclosed), it is not considered a breach, so long as that person does not impermissibly use or disclose the information
- The key here is that the person works for our organization and is authorized to use some PHI

Exception #3: Retention is Not Possible

- If you disclose PHI to an unauthorized person but that person could not have reasonably retained the information, it is not a breach
- Like other impermissible uses and disclosures, it still has to be reported to the Privacy Officer
- For example: A covered entity lacking reasonable safeguards sends out Explanation of Benefits to wrong addresses. They receive the envelopes back as "returned mail" and they have not been open.

Authorization

- Examples of when we need a signed authorization before we release PHI
  - When releasing to an employer information about a pre-employment screening
  - When releasing information to a pharmaceutical company for marketing purposes
- Examples of when we need a signed authorization before PHI is released to us
  - When we are helping get a plan participant get his or her claim paid

When Authorization is NOT Required

- Disclosing an individuals records to him or her
- Disclosing records for purposes of HIPAA enforcement
- Conducting public health and safety disclosures required by law
- Accessing, using, or disclosing PHI as necessary for treatment, payment, and healthcare operations

IN ALL OTHER CIRCUMSTANCES AUTHORIZATION IS REQUIRED

Exceptions to Authorization: Treatment

- Authorization is not required for treatment
- Treatment is providing, coordinating, or managing healthcare and related services for an individual
- Examples of treatment services include:
  - Examination and diagnosis
  - **Consultation among providers regarding an individual**
  - Lab services
  - Pharmaceutical services

Exceptions to Authorization: Payment

- Payment includes:
  - Activities by providers to get payment for healthcare
  - Activities by health plans to provide payment for healthcare
- Examples of Payment Activities include:
  - Determining eligibility or coverage under a health plan and adjudicating claims
  - Risk adjustment
  - Billing and collections

Exceptions to Authorization: Healthcare Operations

- Quality assessment and improvement activities including case management and care coordination
- Competency assurance activities including provider or health plan performance evaluation, credentialing and accreditation
- Conducting or arranging for medical reviews, audits, or legal services including fraud abuse and detection and compliance programs
- Specified insurance functions such as underwriting, risk rating and reinsuring risk
- Business planning, development, management and administration
- **Business management and general administrative activities of the entity including de-identifying PHI, creating a limited data set, and certain fund raising for the benefit of the entity**

Minimum Necessary Rule

- As a BA, the first goals is to use a limited data set to accomplish the work
- A limited data set is PHI that has been stripped of most identifiers such as name, social security number, email address and employer
- Whenever possible work with limited data sets and when this is not feasible, request and have access only to the minimum PHI necessary to complete our work

Exceptions to Minimum Necessary Rule

- Healthcare providers treating individuals
- Disclosures to individuals about their personal information
- Uses or disclosures authorized by the individual
- Disclosures to HHS for purposes of HIPAA enforcement
- Uses or disclosures required by law

Federal Audits: Office of Civil Rights

- HIPAA established important national standards for the privacy and security of protected health information.
- Health Information Technology for Economic and Clinical Health Act (HITECH) established breach notification requirements to provide greater transparency for individuals whose information may be at risk.
- HITECH requires the HHS Office for Civil Rights (OCR) to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

Federal Audits: Phase 1

- **Phase 1 OCR Pilot Audits**: In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements.
- OCR also conducted an extensive evaluation of the effectiveness of the pilot program.
- Drawing on that experience and the results of the evaluation, OCR is implementing phase two of the program, which will audit both covered entities and business associates.

Federal Audits: Phase 2

- OCR will ***audit both covered entities and business associates.***
- OCR is developing enhanced protocols (sets of instructions) to be used in the next round of audits and pursuing a new strategy to test the efficacy of desk audits in evaluating the compliance efforts of the HIPAA regulated industry.
- The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.

OCR Audit Protocol

Audit Protocol - Current

- The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits.
- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards
- The protocol covers requirements for the Breach Notification Rule.
- See complete Audit Protocol Table at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

Audit Target Selection Process

- Every covered entity and business associate is eligible for an audit.
- OCR is identifying pools of covered entities and business associates that represent a wide range of health care providers, health plans, health care clearinghouses and business associates.
- Sampling criteria for auditee selection will include size of the entity, affiliation with other healthcare organizations, the type of entity and its relationship to individuals, whether an organization is public or private, geographic factors, and present enforcement activity with OCR.
- OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review.
- You will know you are a potential auditee when you receive a questionnaire designed to gather data about the size, type, and operations.

Audit Target Selection Process (cont.)

- OCR will be asking covered entity auditees to identify their business associates and encourages covered entities to prepare a list of each business associate with contact information so that they are able to respond to this request.
- OCR will choose auditees through random sampling of the audit pool. Selected auditees will then be notified of their participation.
- If a covered entity or business associate fails to respond to information requests, OCR will use publically available information about the entity to create its audit pool. An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

How Will the Audit Program Work

- OCR plans to conduct desk and onsite audits for both covered entities and their business associates. The first set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates.
- These audits will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules and auditees will be notified of the subject(s) of their audit in a document request letter. All desk audits in this phase will be completed by the end of December 2016.
- The third set of audits will be onsite and will examine a broader scope of requirements from the HIPAA Rules than desk audits. Some desk auditees may be subject to a subsequent onsite audit.

The Audit Process

- The audit process will employ common audit techniques. Entities selected for an audit will be sent an email notification of their selection and will be asked to provide documents and other data in response to a document request letter.
- Audited entities will submit documents on-line via a new secure audit portal on OCR's website. These will be mostly desk audits unless OCR deems it necessary to be onsite.
- Auditors will review documentation and then develop and share draft findings with the entity. Auditees will have the opportunity to respond to these draft findings; their written responses will be included in the final audit report. Audit reports generally describe how the audit was conducted, discuss any findings, and contain entity responses to the draft findings.

Safeguarding PHI: Best Practices

Privacy Notices: Different Rules for Different Entities

- Direct Service Providers have the most extensive Privacy Notice requirements, including Privacy Notice Acknowledgements
- **Business Associates need not provide a Privacy Notice**
- Health Plans must provide a Privacy Notice but need not obtain acknowledgement that the Privacy Notice was received

Right to Inspect, Copy and Amend PHI

- Covered Entities are responsible for informing individuals on how to request to inspect, copy or amend their PHI and to field those requests and provide access to their records within 30 days. State law may provide a shorter deadline.
- **Business Associates must assist Covered Entities with this by providing access to PHI they hold**
- HHA can directly penalize BA for failing to assist the CE

Right to Inspect, Copy, and Amend: Exceptions

- Depending on state law, information held by prisons regarding inmates
- Research information when the individual has agreed to limit his/her access but only during the clinical trial
- Certain psychotherapy notes that are not part of the record
- Documents prepared in anticipation of litigation, but not the underlying PHI itself
- A situation where access would harm the individual (subject to review of an outside professional)
- A situation where a personal representative of an individual requests the PHI but allowing access could cause substantial harm to the individual or someone else

Right to Amend

- The covered entity must make the corrections within 60 days or deny the request and comply with HIPAA denial formalities
- In so far as the incorrect information is in our possession, we must make the corrections too when notified by the CE

Our Responsibility for Informing Others of Corrections

- Covered Entities are responsible for asking individuals who else they should inform of the correction and for informing them
- Covered Entities must also notify entities they have shared the incorrect information with
- Our responsibilities in this case will depend on our BAA

Right to Request Electronic Copies

- Individuals have a right to request an electronic copy of records if the entity stores the information electronically
- Entities can charge a fee, unless otherwise prohibited by state law
- The fee cannot exceed reasonable charges
- Individual can request the records be sent to another individual or entity

Right to Request Restrictions on Disclosures

- Individuals have a right to restrict how a Covered Entity uses PHI for purposes of treatment, payment and operations
- By HIPAA standards the CE does not have to agree to the restrictions, however it and any associated BA are bound to any restrictions they agree to
- CE must agree to the restriction if:
  - The individual requests PHI not be disclosed to a health plan AND
  - The PHI pertains only to services paid for in full out of pocket

Right to Request Accounting of Disclosures and Access Report

- HIPAA gives individuals right to an accounting of certain disclosures that we have made of their PHI for up to six years preceding the request
- Critical we track all disclosures we make if they pertain to:
  - Public health activities
  - Judicial and administrative proceedings
  - Law enforcement activities
  - Activities to avert a serious threat to health or safety
  - Military and Veteran's activities
  - The Department of State's medical suitability determination
  - Government programs involving public benefits

Right to Request Accounting of Disclosures and Access Report: Exceptions

- That are part of a limited data set
- Pertaining to treatment, payment or operations, unless the PHI was part of an electronic health record
- To the individual or his/her personal representative
- To the individuals friends or family if the individual is present or due to an emergency
- For prisons regarding inmates
- For national security or intelligence purposes

Access Rights of Parents

- A parent is generally a personal representative of a minor child under the Privacy Rule and therefore has the same rights of access to PHI
- The rule is the same for a guardian or other person acting in "loco parentis" of child

Access Rights of Parents: Exceptions

- State Law
- Court or legal requirements
- Parental agreement
- Emancipation of minor
- Abuse and neglect

Right to Confidential Communications

- Under the Privacy Rule, individuals can request that a direct care provider or health plan communicate with them by alternative means or alternative locations
- Direct care providers must accommodate these requests so long as they are reasonable
- Health Plans must accommodate these requests so long as they are reasonable and the individual states that disclosure could endanger them
- As a Business Associate we are bound by the rules governing the CE we are serving

Right to Complain of Violations

- Despite our best efforts it is inevitable that individuals will occasionally object to our privacy practices or identify an instance of non-compliance
- We appreciate complaints
- Complaints enable us to perfect our Privacy policy and monitor our HIPAA compliance

Filing Complaints

- Complaints can be filed with our Privacy Officer or with the U.S. Department of Health and Human Services' Office for Civil Rights
- If a person complains to you:
  - Take the complaint seriously
  - Express your concern
  - Refer them to the Privacy Officer
  - Inform the Privacy Officer

Intimidating and Retaliatory Acts

- Our policy requires we abstain from intimidating or retaliatory acts in all circumstances
- Individuals cannot be threatened for filing a complaint with us or with the HHS or for participating in an investigation
- Examples of threatening behavior include:
  - Threatening monetary, physical, or other retaliation to prevent the filing of a complaint or exercising his/her rights under HIPAA
  - Offering bribes

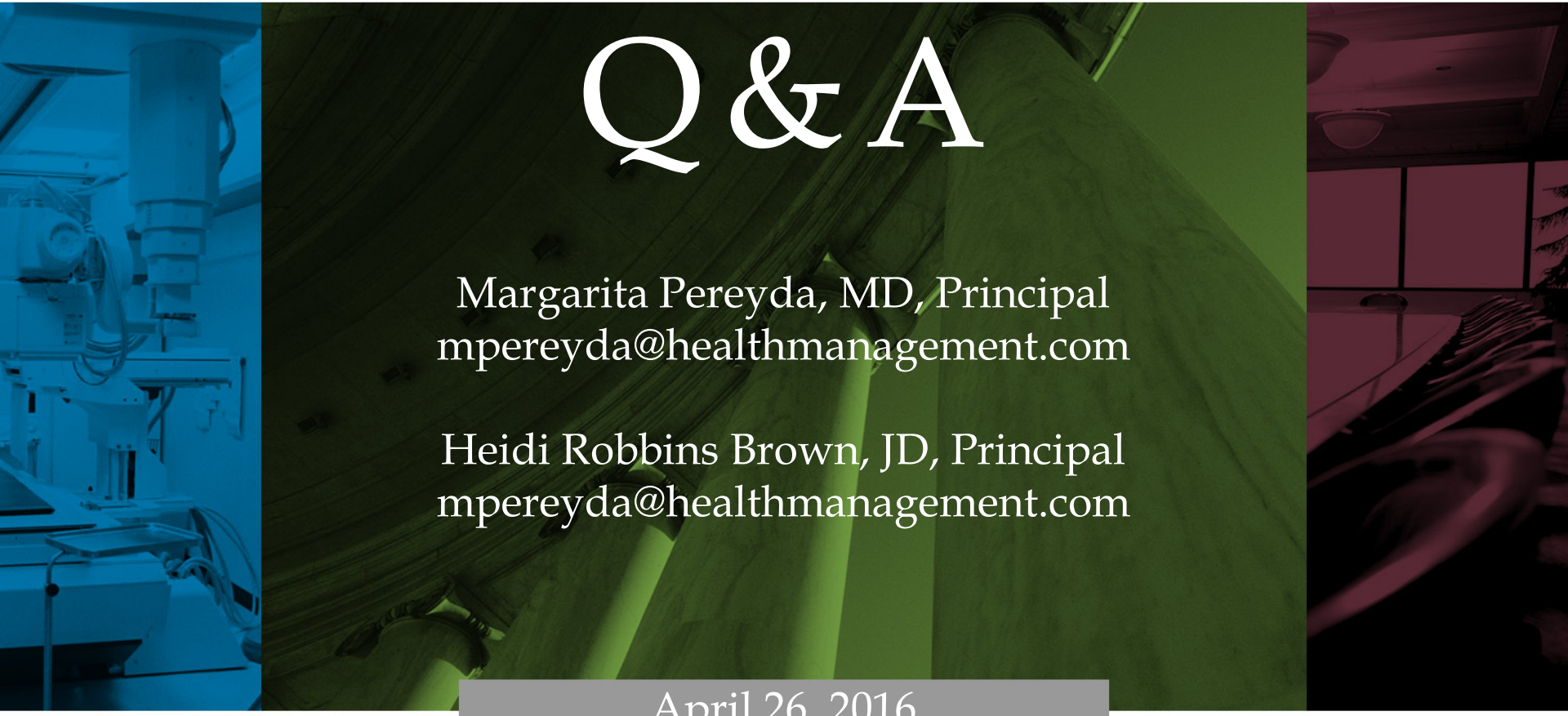
Waiver of Rights

- Our policy also prevents us from forcing individuals to waive their rights under HIPAA as a condition of service

Best Practice Recommendations

- Covered Entities and their Business Associates must have a Business Associates Agreement in place and then ensure that the sharing of PHI is secure.
- Follow the HIPAA Security Implementation Plan, perform regular risk assessments and update policies and procedures and agreements regularly
- Ensure proper disposal of PHI occurs and that your BA ensures your partners dispose appropriately
- When a breach occurs, know what to do and mitigate immediately and follow instructions for reporting
- Respond to patient requests in a timely and respectful manner.
- MOST Importantly: Train your staff regarding personal liability, minimum necessary practices, identifying and reporting breaches and respectful handling of PHI

HEALTH MANAGEMENT ASSOCIATES



Q & A

Margarita Pereyda, MD, Principal
mpereyda@healthmanagement.com

Heidi Robbins Brown, JD, Principal
mpereyda@healthmanagement.com

April 26, 2016