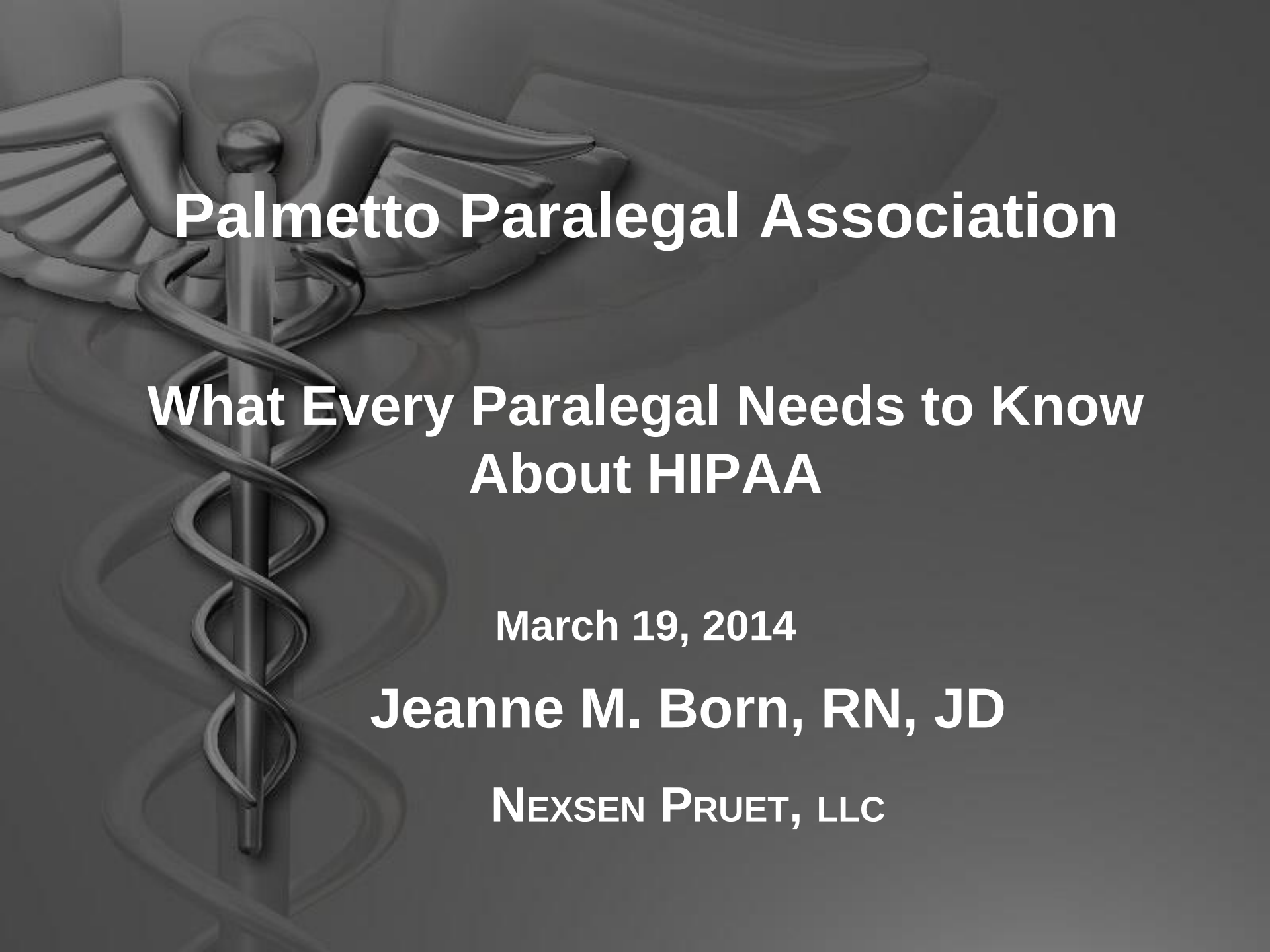


# Palmetto Paralegal Association

## What Every Paralegal Needs to Know About HIPAA

March 19, 2014


**Jeanne M. Born, RN, JD**

Nexsen Pruet, LLC

# What Every Paralegal Needs to Know About HIPAA

- In August of 1996 Congress passed HIPAA
- Little did we know how much of an impact HIPAA would have on the practice of law.
- Not just health care practices, but all practices.

# What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Administrative Simplification; 42 U.S.C. § 1320d-1320d-8

# What is HIPAA's purpose?

- To improve the efficiency and effectiveness of the health care system by simplifying the electronic transmission of health information in specific statutory transactions
- To provide for, among other things, the promulgation of federal standards regarding health information privacy, confidentiality and security

# The Regulatory Scheme

- Eight regulations effect HIPAA's purposes by:
  - Standardizing code sets and transactions formats
  - Standardizing identifiers
  - Protecting the privacy and security of health information

# Then on 2/17/ 2009 . . . Congress passed a game changer

- Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”)
  - Subtitle D – Privacy
- HITECH Implementing Regulations: 78 F.R. 5566 (“HITECH Final Rule”) published January 25, 2013 – effective March 26, 2013 – enforcement began September 23, 2013

# Abbreviations: KEY

- Covered Entity: CE
- Business Associate: BA
- Business Associate Agreement: BAA
- Individually Identifiable Health Information: IIHI
- Protected Health Information: PHI
- Civil Money Penalty: CMP

# To Whom does HIPAA Apply?

- HIPAA applies to
  - Health Plans
  - Health Care Clearinghouses
  - Health Care Providers who transmit any health information in electronic form in connection with any transaction covered by HIPAA.
- After HITECH, also to BAs . . . Later.

# What Information Does HIPAA Cover? Health Information:

- Any information whether oral or recorded in any form or medium that:
  - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and
  - Relates to the past, present, or future physical or mental health, condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

# Is HIPAA Concerned with All Health Information?

- **Individually Identifiable Health Information ("IIHI"): IIHI is health information**
  - **created or received by a health care provider, health plan, employer or health care clearinghouse; and**
  - **relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provisions of health care to an individual; and**
  - **that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.**

# What Information Does the Privacy Standard Cover?

The Privacy Standard primarily covers:

- Protected Health Information ("PHI"). PHI is IIHI that is transmitted by electronic media, maintained in any medium described in the definition of electronic media or transmitted or maintained in any other form or medium except:
  - Employment records held by a CE in its role as an employer;
  - Certain education records;
  - Records of a person deceased more than 50 years.

# What does the Security Standard Cover?

- Electronic Protected Health Information ("E-PHI"): IIHI that is transmitted by electronic media, maintained in any medium described in the definition of electronic media:
  - Electronic storage material on which data is or may be recorded electronically
  - Transmission media used to exchange information already in electronic storage media

# Privacy and Security Standards Pre/Post HITECH

- Require that CEs comply with a complex set of regulations to protect the privacy and security of protected health information
- Many (not all) of the Privacy and Security Standards are now directly applicable to BAs and enforcable as of September 23, 2013.

# How does HIPAA/HITECH affect your law firm?

- HIPAA/HITECH affects how you deal with
  - CEs with which your client has an adversarial relationship.
  - CEs who are not parties to your case and from whom you desire to obtain PHI
  - Your clients who are CEs
  - Your clients who are Bas of CEs

# You had to learn a new vocabulary

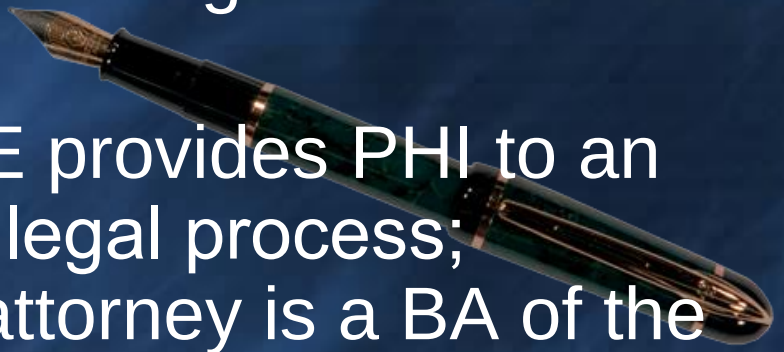
- Consent v. Authorization

# CONSENT

Consent:  Permitted under the Privacy Standard to be used by a health care provider to use or disclose protected health information for treatment, payment, or healthcare operations purposes.

# AUTHORIZATION

- An “authorization” must be obtained by a CE before the CE uses or discloses PHI for reasons other than to carry out treatment, payment or health care operations (not disclosures required by law/subject to legal process).
- Must be used when requesting psychotherapy notes and when using or disclosing protected health information for marketing or for the sale of PHI.
- Must be used when a CE provides PHI to an attorney’s office (absent legal process; applicable law; or if the attorney is a BA of the CE).



# A valid authorization must contain the following elements:

- describe the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- specify the name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure;
- specify the name or other specific identification of the persons(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

# A valid authorization must contain the following:

- describe each purpose of the requested use or disclosure;
- provide an expiration date or an expiration event that related to the individual or the purposes of the use of disclosure;
- provide a statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

# A valid authorization must contain the following:

- Include a statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Standard;
- Include a statement regarding whether treatment, payment or enrollment or eligibility for benefits is conditioned on whether the individual signs the authorization (may do so only under very limited circumstances);
- The signature of the individual and date;
- if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and
- Must be written in plain language.

# Disclosures for Judicial and Administrative Proceedings

- Disclosures of PHI for judicial and administrative proceedings do not require consent or an authorization, but have many technical requirements . . .

# Disclosures for judicial and administrative proceedings

- A CE may disclose PHI pursuant to and to the extent required by a court order.

# Disclosures for judicial and administrative proceedings

- Disclosures pursuant to a subpoena, discovery request or other lawful process not accompanied by a court order may be made IF the CE receives satisfactory assurances that:
  - Reasonable efforts have been made by the party seeking the PHI to ensure that the individual who is the subject of the PHI has been given notice of the request; OR
  - Reasonable efforts have been made by the party seeking the PHI to secure a qualified protective order that meets the requirements of the Privacy Standard.

# Disclosures for judicial and administrative proceedings

- Satisfactory assurance by notice
  - Good faith attempt to provide written notice to the individual or the personal representative
  - Personal representative
    - the person who is legally authorized by state law to make healthcare decisions for the individual
  - If the subject of the PHI is a party to the action notice to the individual's attorney is sufficient notice to provide satisfactory assurance

# Disclosures for judicial and administrative proceedings

**Before a CE can disclose PHI requested in a discovery request, the CE must (unless the subject of the PHI is a party to the law suit) receive a letter from the requesting attorney containing the following:**

- Good faith attempt to provide written notice to the individual;
- The notice includes sufficient information about the litigation or proceeding to permit the individual to raise an objection;
- The time for the individual to raise the objection has elapsed;
- No objections were filed or all objections have been resolved; and
- Disclosures requested are consistent with the resolution.

# Disclosures for judicial and administrative proceedings

or the CE must receive the following with the discovery request:

- Satisfactory assurances by receiving a qualified protective order ("QPO")
  - The parties have agreed to a QPO and have filed a motion requesting a consent order with the court or administrative tribunal; or
  - The party requesting the PHI has requested a QPO from the court or administrative tribunal.

# Disclosures for judicial and administrative proceedings

- Qualified Protective Order ("QPO")
  - An order of the court or a stipulation by the parties that
    - prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such PHI was requested; and
    - requires the return to the CE or the destruction of the PHI at the end of the litigation or proceeding.

# Special Issues: Workers'Compensation

- The Privacy Standards permit covered entities to use or disclose PHI as required by State Workers Compensation ("WC") laws.
- 42-15-95 requires providers to disclose written PHI to the WC carrier, employer, attorney or the WC Comm'n that *pertains directly to a WC claim*.
- 25A SC Code Regs. 67-1301 requires providers to disclose all medical information *relevant to the employee's complaint of injury* to the claimant, the employer, the employer's representative or to the WC Comm'n.
- WC subpoenas are <u>likely</u> subject to the requirement that disclosures may be made only with "satisfactory assurances."

# Workers'Compensation

- Providers may discuss/communicate about an employee's medical history, diagnosis, causation, course of treatment, prognosis, work restrictions, and impairments if the employee is:
  - Timely notified of the request (prior to the discussion/communication);
  - Advised of the nature of the discussion/communication (prior to the discussion/communication); and
  - Provided with a copy of written questions at the same time the questions are provided to the Provider and a copy of any response.
- Must not conflict or interfere with the employee's examination or treatment.
- Discussion/communication does not breach any duty of confidentiality.

# Business Associate

- How you deal with clients who are CEs or BAs:
  - Congratulations! You are a business associate of your client.

# Business Associate Definition

- "Business associate" generally means, with respect to a covered entity, a person who on behalf of a covered entity, but other than as a member of the workforce
  - creates, receives, maintains or transmits PHI for a function regulated under HIPAA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefits management, practice management, and repricing; or . . .

# Business Associate Definition

- a person who provides ***legal***, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity where the provision of such services involves the disclosure of PHI.

# Business Associate Definition

- Business Associate:  HITECH update includes:
  - Patient Safety Organizations (“PSOs”);
  - Subcontractors (A person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA);
  - Health Information Organizations (“HIOs”);
  - E-Prescribing Gateways;
  - Vendors of PHRs; and
  - Other persons that facilitate data transmissions; (conduits limited to courier services (ex: USPS; UPS) & their electronic equivalents (ex: ISPs));
  - Exceptions moved from 164.308(b)(2) & 164.502(e)(1)(ii)

# How will HIPAA affect my practice?

- The CE must obtain “satisfactory assurances” that the BA will safeguard the PHI.
- You must enter into a Business Associate Agreement (“BAA”) with your CE client:
- If you are a subcontractor of a BA, you must enter into an agreement with the BA assuming the same obligations as the BA.
- After HITECH, the Privacy Standards and Security Standards have specific requirements for the BA.

# Business Associate Agreement: Permissive Provisions

- The BAA MAY PERMIT the BA to use PHI in its capacity as a BA to the CE, if necessary:
  - For the proper management and administration of the BA; and
  - To carry out the legal responsibilities of the BA.

# Business Associate Agreement Permitted Provisions

- The BAA MAY PERMIT the BA to disclose PHI in its capacity as a BA for the foregoing purposes if:
  - the BA is required to do so by law; or
  - if the BA obtains reasonable assurances from the person(s) who will receive the PHI that it will be held confidentially and used or disclosed only as required by law or for the purpose for which it was disclosed and agrees to report any breach.
  - For example:  Disclosure to an expert.

# Business Associate Agreement: Required Provisions

- The BAA must establish the permitted and required uses and disclosures of PHI by the BA –
- The BAA may not authorize the BA to disclose or use the PHI in violation of the Privacy Standard.

# Business Associate Agreement: Required Provisions

- The BAA must require that the BA not use or further disclose the PHI other than as permitted or required by the BAA or as required by law;
- The BA may not use or disclose the PHI in a way that the CE may not.

# Business Associate Agreement: Required Provisions

- The BAA must require that the BA use appropriate safeguards to prevent the use or disclosure of the PHI other than as required by the contract.

- The CE & BA must
- have administrative, technical, and physical safeguards in place to protect the privacy of PHI;
  - Have policies and procedures in place/meet documentation requirements;
  - reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements; and

# Business Associate Agreement: Required Provisions

- reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

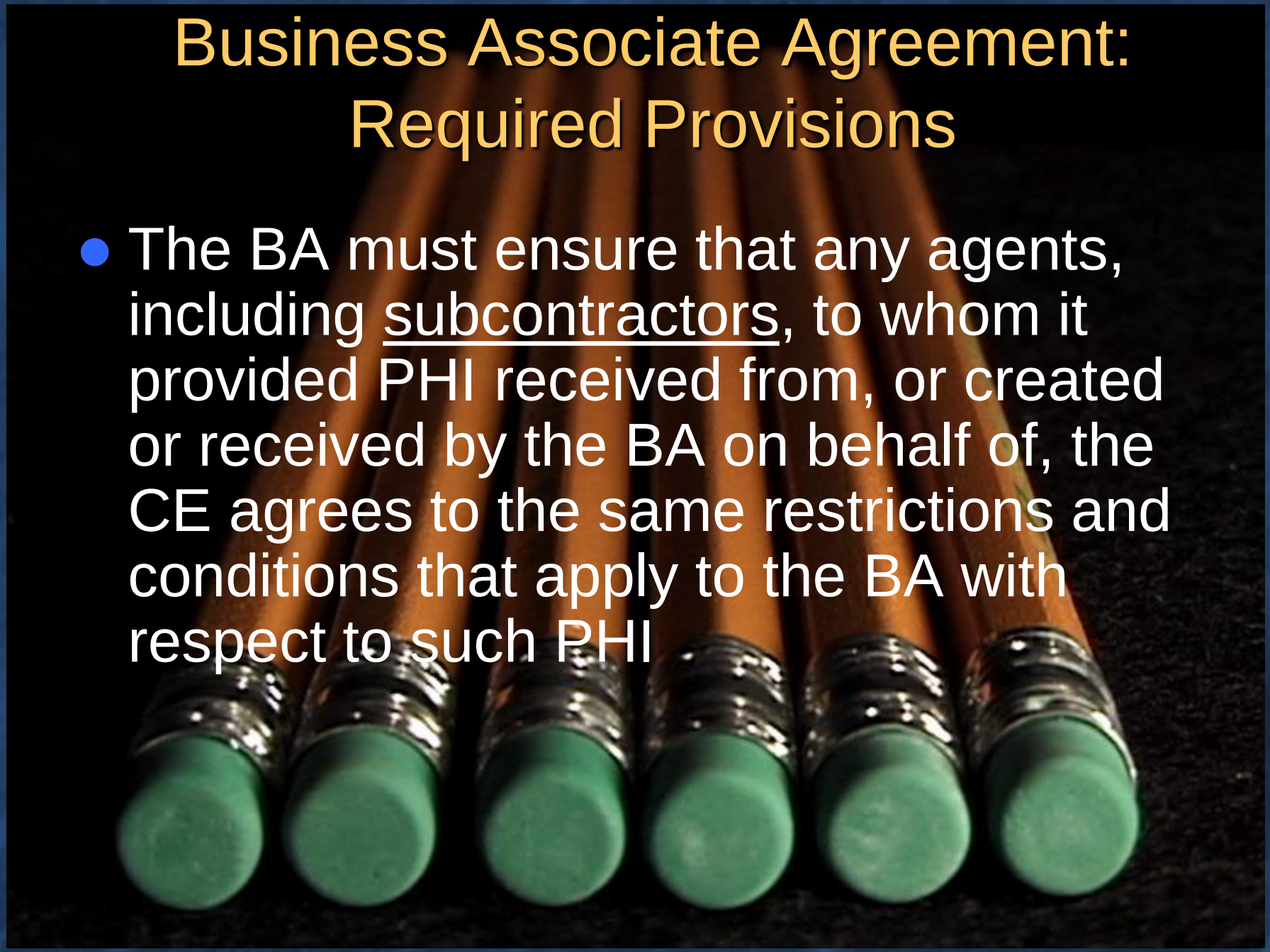
# Business Associate Agreement: Required Provisions

- The BA must report to the CE
  - Any use or disclosure of the PHI not provided for in the contract of which it becomes aware;
  - Any Security Incident;
  - Any Breach of Unsecured PHI . . .
    - Later

- BA must require subcontractors to report the same to the CE.

# Business Associate Agreement: Required Provisions

- The BA must ensure that any agents, including subcontractors, to whom it provided PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such PHI



# Business Associate Agreement: Required Provisions

- The BA must make the PHI available in accordance with access requirements of the Privacy Standard.
- This obligation is limited to when the BA maintains the PHI in a designated record set; and
- The individual does not have access to PHI complied in a reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

# Business Associate Agreement: Required Provisions

- The BA must make the PHI available in accordance with the requirements for amendment and incorporate any amendments to PHI.
- This obligation is similarly limited because the requirements for amendment apply only if the BA maintains the PHI in a designated record set.

# Business Associate Agreement: Required Provisions

- The BA must make the PHI available in accordance with accounting requirements of the Privacy Standard.
- Requires that the BA track and report its uses and disclosures to the client or, if requested to the individual.

# Business Associate Agreement: Required Provisions

- The accounting requirements do not apply to the following uses or disclosures:
  - Uses and disclosures to carry out treatment, payment or health care operations;
  - Disclosures to the individual;
  - Disclosures pursuant to an authorization
  - Disclosures pursuant to a facility's directory (Hospital) or to persons involved in the individual's care or other notification purposes;

# Business Associate Agreement: Required Provisions

- Disclosures for national security and intelligence purposes
- Disclosures to correctional institutions or law enforcement officials (in custodial situations only)
- As part of a limited data set; and
- Uses and disclosures incidental to the above.

# Business Associate Agreement: Required Provisions

- The BA must provide an accounting of disclosures from the earlier of the previous six (6) years.
- The CE must be provided with the following information related to each applicable disclosure:
  - The date of the disclosure
  - The name of the entity or person who received the PHI and, if known, the address of such entity or person
  - A brief description of the PHI disclosed
  - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) (when required by the Secretary of DHHS) or 164.512 (required by regulation or statute)

# Business Associate Agreement: Required Provisions

- The BA must make the BA's internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of DHHS for the purpose of determining the covered entity's compliance with the Privacy Standard.

# Potential Waiver of the Attorney Client Privilege and Work Product Doctrine

- May operate as a waiver of the attorney client privilege and work product doctrine.
- Any disclosure to a third party operates as a waiver.
- The waiver may extend to all communications related to the subject.
- Recommend modifying the BAA to require the Covered Entity's consent prior to disclosing PHI to the Secretary.
- Helps to satisfy the confidentiality requirements of S.C.R.P.C. 1-6

# Business Associate Agreement: Required Provisions

- The BAA must require at the termination of the contract, if feasible, the return or destruction of all PHI received from, or created or received by the BA on behalf of the CE that the BA still maintains in any form and retain no copies of such information or, if such return is not feasible, extend the protections of the contract to the information.

# Business Associate Agreement: Required Provisions

- The BAA must authorize termination of the contract by the CE, if the CE determines that the BA has violated a material term of the contract; and
- Visa versa.

# Business Associate Agreement: Required Provisions

- A CE is not in compliance with the business associate requirements if the CE knew of a pattern of activity or practice of the BA that constituted a material breach or violation of the BA's obligation under the contract or other arrangement, unless the CE took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful either:
  - Terminate the BAA or, if termination is not feasible;
  - Report the violation to the Secretary of DHHS
- And visa versa

# Transition Provisions to Update BAAs

- A CE or a BA of the CE with respect to a Subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e) and 164.504(e) with respect to a particular BA relationship for the time period set forth below if:
  - Prior to January 25, 2013, CE s or BAs with respect to a Subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the BA that complies with the applicable provisions of §§ 164.314(a) or 164.502(e) that were in effect on such date; and
  - The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013 or September 23, 2104.
- If neither Section above apply, then the CE or the BA with respect to a Subcontractor, must enter into a BAA that complies with the HITECH Final Rule.
- On September 23, 2014, all BAAs must comply with all provisions of the HITECH Final Rule.

# Notification of Breaches of Unsecured PHI

- A BA is required to report Breaches of Unsecured PHI to the CE.
- Breach means: the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Standards which *compromises the security or privacy of such information* . . .

# Exceptions to the Meaning of Breach

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under Privacy Standards;
- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at same CE or BA or OHCA in which the CE participates, and the PHI received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Standards; and
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

# Unsecured PHI

- Unsecured Protected Health Information ("Unsecured PHI"): PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized ~~individuals~~ persons and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.
- Guidance published April 17, 2009.

# Whether a Breach is Reportable

- A breach is reportable if the breach is of Unsecured PHI; AND if
- There is has not been a finding that there is a low probability that the privacy or security of the PHI has been compromised based on a risk assessment of the following 4 factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

# Discovery of the Breach and Reporting to the CE

- Timing of the report is determined in the BAA;
- A breach is discovered on the first day the breach is known or by exercising reasonable diligence, would have been known by the CE;
- A breach is discovered by a BA on the first day the breach is known or by exercising reasonable diligence, would have been known by the BA;
- A BA or Subcontractor is required to report the breach to the CE in accordance with the terms of the BA;
- Clarified in the HITECH Final Rule: A CE will be deemed to have discovered a breach on the first day the breach was discovered by a BA only if the BA is acting as an **agent** of the CE.
- Determined by the federal common law of agency.

# Content of the Notice of the Breach to the CE

- A brief description of what happened (include date of breach and date of discovery)
- A description of the types of Unsecured PHI involved in the breach
- The steps that individuals should take to protect themselves from potential harm
- A brief description of what the CE is doing to investigate, mitigate losses and protect against further breaches
- Any other information required by the CE in the BAA

# Regarding Any Disclosures of PHI

- Generally, the “Minimum Necessary” PHI must be used or disclosed to effect the intended purpose.
- The CE/BA may not use or disclose the entire medical record unless it is specifically justified.

# Regarding Any Disclosure of PHI

- A CE may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when the information is requested by a professional who is a member of its workforce or is a BA of the CE for the purpose of providing professional services to the CE, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).

# WHY DO CEs and BAs COMPLY?

- Potential for Criminal Penalties:
  - HITECH amended the statute that sets forth the criminal penalties to make it clear that criminal penalties apply to employees and other individuals, including BAs.
- A person who knowingly and in violation of the criminal statute (42 U.S.C. §1320d-6)
  - (1) uses or causes to be used a unique health identifier;
  - (2) obtains IIHI relating to an individual; or
  - (3) discloses IIHI to another person, shall be punished as provided in subsection (b) of this section.

# Why Do Covered Entities Comply?

- Criminal Penalties: 42 U.S.C. §1320d-6(b)
  - Wrongful use or disclosure: $50,000 fine and imprisonment for one year.
  - Use or disclosure under false pretenses: $100,000 fine and imprisonment for five years.
  - Use or disclosure with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm: $250,000 fine and imprisonment for ten years.

# Physician Criminal Conviction Upheld: 5/10/2012

- A visiting cardiothoracic surgeon from China (working as a research assistant) was convicted of misdemeanor violation of the HIPAA criminal statute
- After his termination from UCLA, on at least four occasions, he accessed four patient records (co-workers and celebrity)
- The 9th Circuit upheld the district court's finding that he knowingly and in violation of HIPAA obtained IIHI relating to individuals
- Sentence:
- Four months in prison, then a year of supervised release;
- $2000 fine

# Increased Enforcement of Civil Penalties

- HITECH significantly revised 42 U.S.C. §1320d-5 to include non-compliance due to willful neglect and requires DHHS to investigate if a complaint indicates a violation due to willful neglect.

# HITECH: Civil Money Penalty Tiers

- (a) $100/violation, the total not to exceed $25,000 for identical violations / calendar year;
- (b) $ 1,000/violation, the total not to exceed $100,000 for identical violations/calendar year;
- (c) $ 10,000/violation, the total not to exceed $250,000 for identical violations/calendar year;
- (d) $ 50,000/violation, the total not to exceed $1,500,000 for identical violations/calendar year.

- A violation where the person did not know and by exercising due reasonable diligence would not have known, the penalty will be not less than (a) but not more than (d).
- A violation due to reasonable cause, but not willful neglect, the penalty will be not less than (b) but not more than (d).
- A violation due to willful neglect:
- If corrected, the penalty will be not less than (c) but not more than (d);
- If not corrected, the penalty will be not less than (d).

# HITECH Final Rule Defined:

- **Reasonable Cause**: An act or omission in which a CE or BA knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the CE or BA did not act with willful neglect.
- **Reasonable Diligence**:  The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- **Willful Neglect**: Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

# Violations Attributable to CE or BA

- Violations of a BA can be attributed to a CE if the BA is an agent of the CE:
  - Federal Common Law of Agency when acting within the scope of the agency.
- Violation of a Subcontractor can be attributed to a BA if the Subcontractor is an agent of the BA.
  - Federal Common Law of Agency when acting within the scope of the agency.

# Four Factors DHHS Considers in determining the CMP

- The nature and extent of the violation, consideration may include:
  - The number of individuals affected; and
  - The time period during which the violation occurred.
- The nature and extent of harm resulting from the violation, consideration may include whether the violation:
  - Caused physical harm;
  - Resulted in financial harm;
  - Resulted in harm to an individual's reputation; or
  - Hindered an individual's ability to obtain health care.

# Four Factors DHHS Considers in determining the CMP

- The history of noncompliance by the CE or BA, consideration may include:
  - Whether the violation is the same or similar to previous noncompliance;
  - Whether and to what extent the CE or BA has attempted to correct previous noncompliance;
  - How the CE or BA has responded to technical assistance from the Secretary in the context of the compliance effort; and
  - How the CE or BA has responded to prior complaints.

# Four Factors DHHS Considers in determining the CMP

- The financial condition of the CE or BA, consideration may include:
  - Whether the CE or BA had financial difficulties that affected its ability to comply;
  - Whether the imposition of a CMP would jeopardize the ability of the CE or BA to continue to provide or pay for health care; and
  - The size of the CE or BA.

- Such other matters as justice may require.

# Affirmative Defenses:

- Violation punishable under HIPAA criminal provisions;
- Violation penalized under HIPAA criminal provisions;
- Violation is:
  - Not due to willful neglect; and
  - Is corrected either during:
    - 30 day period during which the CE or BA knew or by exercising reasonable diligence should have known of the violation;
    - Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

# First CMP:  2/4/2011

- Cignet Health:  Large multi-healthcare provider group
- Failed to provide 41 patients access to their PHI (were 41 complaints – all individually filed with the OCR)
- Initial fine:  $1.3 Million for failure to provide access
- Subsequent fine:  $3.0 Million for failure to cooperate with the OCR's investigation (3/17/2009 – 4/7/2010)
- Total fine:  $4.3 Million
- Upshot – cooperate with the OCR investigation!

# OCR sends a message to small physician practices: 4/17/2012

- Phoenix Cardiac Surgery (5 physician practice)
- Complaint:  posting surgery and appointment schedules on a publically accessible internet-based calendar
- OCR found a “multiyear, continuing failure” to
  - Implement policies and procedures
  - Document training of employees
  - Identify a security official at the practice
  - Conduct a security analysis
  - Obtain business associate agreements with its internet-based email and scheduling services

# Phoenix Cardiac Surgery Penalties

- Resolution Agreement:
- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf
  - $100,000 CMP
  - Comply with a Corrective Action Plan (one year)
    - Develop and implement Privacy and Security policies/procedures and provide to the OCR for approval
    - Implement the policies/procedures within 30 days of approval
    - Distribute the policies/procedures to its workforce and require written certifications of initial compliance from each
    - Assess and update the policies and procedures annually
    - Make reports to the OCR

# High Risks – Computers and Portable Devices

- Take great care:
  - Risks are high with EHR
    - Greater access/speed/availability means an even greater risk of potential breaches/liabilities
  - Use of portable devices:
    - Be mindful of where you are using portable devices and whether you have appropriate security (technical and physical)
    - Use only those portable devices that are approved by your practice

# CMP for Stolen Mobile Device

- Massachusetts Eye and Ear Infirmary and its associated physician practice
- Self-reported the theft of an unencrypted laptop containing PHI of > 500 patients from an employed physician while on vacation
- No finding of financial or reputational harm to the patients
- Findings: Failure to . . .
  - Restrict access to ePHI from unauthorized users/portable devices and be able to track access
  - Track movement of both Hospital/personal portable devices on and off premises
  - Implement encryption or appropriate alternatives to encryption
- 9/17/2012 – Agreement (3 years)
  - $1.5 Million CMP
  - A Corrective Action Plan (includes a framework for updating policies/procedures and compliance plans for mobile devices)
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf

# First HIPAA Settlement for Breach of < 500 patients' PHI (01/02/2013)

- Hospice of North Idaho ("HONI") reported the theft of an unencrypted laptop containing the PHI of 441 patients
- OCR found:
  - HONI failed to conduct risk analysis;
  - HONI failed to implement security measures;
  - HONI failed to have policies and procedures for mobile devices
- Settlement Agreement:
  - Enter into a CAP
  - CMP of $50,000
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf

# Improved Enforcement: AGs

- Enforcement by Attorneys General: In any case in which the AG has reason to believe that an interest of one or more of the residents of the State has been threatened or adversely affected by any person who violates a provision of HIPAA, the AG may bring a civil action on behalf of such residents to:
  - Enjoin further such violations; or
  - To obtain damages on behalf of such residents calculated by multiplying the number of violations by $100, the total not to exceed $25,000 for identical violations during a calendar year.
- The court may award attorney fees.

# Improved Enforcement: AGs

- The AG must serve notice on DHHS and provide DHHS a copy of the complaint
- DHHS has the right to:
  - Intervene in the action;
  - To be heard on all matters; and
  - File petitions for appeal.
- Effective: The date of HITECH publication (NOW).

# HITECH Act: Improved Enforcement

Distribution of Civil Money Penalties ("CMPs"):

- $$ go to the Office for Civil Rights to be used for enforcement purposes
- The Government Accounting Office is to issue a report 18 months after HITECH is published concerning whether the individual who is harmed by the violation may receive a percentage of the CMP.
- Cannot locate such a GAO report.

# NEXSEN PRUET, LLC

**ATTORNEYS & COUNSELORS AT LAW**

*With Offices In:*

*Columbia, South Carolina*
*Charleston, South Carolina*
*Greenville, South Carolina*
*Myrtle Beach, South Carolina*
*Hilton Head, South Carolina*
*Charlotte, North Carolina*
*Greensboro, North Carolina*
*Raleigh, North Carolina*

WWW.NEXSENPRUET.COM