"HIPAA FOR LAW FIRMS"
WHAT EVERY LAW FIRM NEEDS TO KNOW ABOUT HIPAA

NEXT CHALLENGE. NEXT LEVEL.

NEXSEN | PRUET

SOUTH CAROLINA ASSOCIATION OF LEGAL ADMINISTRATORS

THURSDAY, APRIL 14, 2016

Jeanne M. Born, RN, JD
Jborn@nexsenpruet.com

What Every Law Firm Needs to Know About HIPAA

- On August 21, 1996 President Clinton signed HIPAA into law
- 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

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

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

Game Changer: To Whom does HIPAA Apply?

- Prior to HITECH HIPAA applied only 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.
- First: A little “HIPAA 101”

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 Standards primarily cover:

- 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 do the Security Standards 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

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

How does HIPAA/HITECH affect your law firm?

- HIPAA/HITECH affects how your Firm deals 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

CE Adversaries and Nonparty CEs your Firm needs PHI from

- Changed the way law firms obtain PHI:
  - Authorization ("HIPAA Compliant")
  - Discovery processes must include "satisfactory assurances":
    - 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 Standards.

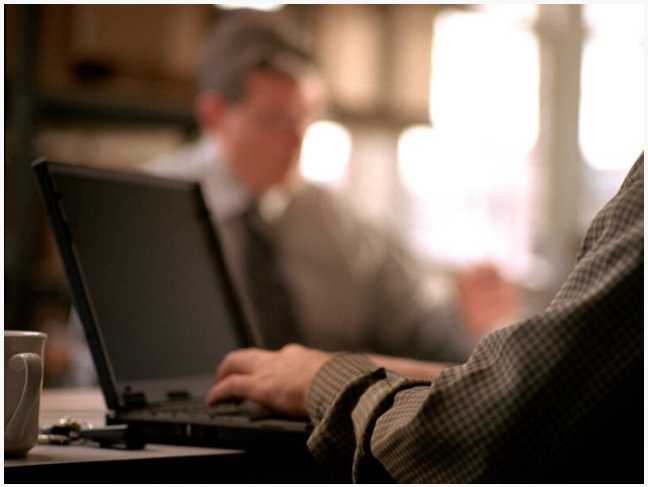
How your Firm deals with clients who are CEs or BAs

- And now for the BIG game changer for business associates:
- If you provide legal services to a client and your receive PHI from the client in the process of providing legal services, you are a business associate of your client (or a subcontractor of a BA) and your Firm is subject to HIPAA.
- Congratulations!

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)

Is the Law Firm a BA?

- After the HITECH update it is clear:
  - Even more entities are considered BAs;
  - Many of the HIPAA provisions apply directly to BAs;
  - The enforcement provisions apply to BAs.
- If the Firm contracts with CEs, the Firm needs to review its contractual relationships with CEs to determine if a BA relationship exists.
- If a BA relationship exists . . . .

What if the Law Firm is a BA?

- Comply with applicable Privacy and Security Standards:
  - Must enter into a Business Associate Agreement (BAA) and pass on your BA obligations to Subcontractors
  - Develop and implement policies and procedures to comply with Privacy Standards:
    - Identify when an engagement of a CE creates a BA relationship
    - Identify when to pass on BA obligations to subcontractors
    - Establish workforce members' responsibilities with the use and disclosure of PHI
    - Establish the minimum necessary PHI to request/access
    - Provide for the rights of the subject of the PHI:
      - Access
      - Amendment
      - Accounting

What if the Law Firm is a BA?

- Develop and implement policies and procedures to comply with Privacy Standards (cont'd):
  - Provide safeguards (administrative; physical and technical) to protect PHI
  - Sanctions for violations by workforce members and subcontractors
  - Non-retaliation
  - Mitigation of breaches/unauthorized uses or disclosures
  - Breach notification
  - Training

What if the Law Firm is a BA?

- Develop and implement policies and procedures to comply with Security Standards.
  - Risk Analysis
  - Risk Management
  - Sanctions
  - Information System Review Activity
  - Security Official
  - Information Access Policy
  - Security Awareness Training
  - How to Identify and Respond to Security Incidents
  - Development of a Contingency Plan

What if the Law Firm is a BA?

- Develop and implement policies and procedures to comply with Security Standards (continued):
  - Evaluation of Security Policies
  - Facility Access Controls
  - Workstation Use & Security
  - Device & Media Controls
  - Technical Access Controls
  - Audit Controls
  - Integrity
  - Person or Entity Authentication
  - Transmission Security

What if the Law Firm is a BA?

- Develop and implement policies and procedures to comply with Security Standards (continued):
  - Implementation of the Security Standards allows:
    - Scalable/flexible implementation that takes into account:
      - Size, complexity and capabilities of your Firm;
      - Technical infrastructure, hardware, and software capabilities;
      - Probability and criticality of potential risks to PHI.
    - Addressable/Required components.

Business Associate Agreement:

- The Privacy and Security Standards both require that the CE and BA enter into a BAA.
  - Recommend having the BAA as an amendment/addendum to your engagement letter.
- The Privacy and Security Standards have both:
  - Permissive provisions
  - Required provisions

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 (management/administration/carry out legal responsibilities) 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 Standards.

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.

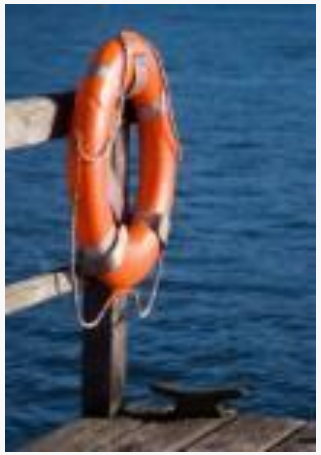
Business Associate Agreement: Required Provisions

- 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 ("DRS") (Practice Tip: Don't maintain a DRS).
- 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 DRS (Practice Tip: Don't maintain a DRS).

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 CE's or BA'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

- After HITECH, 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, after HITECH, visa versa

*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 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).

What (Else) Law Firms May Not Know

- Law Firms providing health insurance for the first time.
- What the Law Firm's health plan HIPAA obligations entail:
  - Fully-insured and fully administered plans.
  - Self-insured plans that are either self-administered or administered by a third party administrator (TPA).

HIPAA Requirements: Fully Insured and Administered Plans

- Fully-insured and fully administered plans:
  - Amend plan documents to allow sharing of information if necessary.
  - Provide the Health Plan's Notice of Privacy Practices (NPP)upon request.
  - Refrain from retaliatory or intimidating acts for making HIPAA complaints.

HIPAA Requirements: Self Insured and Either Self-Administered or Administered by TPA

- Enter into appropriate BAAs;
- Amend the plan documents to allow sharing of information;
- Institute procedures to comply with plan amendments;
- Use and disclose PHI only as allowed under the Privacy Standards;
- Have all policies and procedures required under the Privacy/Security Standards;
- Provide plan participants with the NPP.

Privacy & Security Policies and Procedures

- Designate a privacy official
- Train your employees
- Safeguard the PHI
- Handle Complaints
- Sanction violations
- Refrain from retaliation for making complaints about your privacy practices

Privacy & Security Policies and Procedures

- Provide for participants' rights:
  - Access
  - Amendment
  - Accounting
  - Restrict uses and disclosures
  - Confidential communication
  - Receive notice of the Company's privacy practices
  - Receive notice of breaches of unsecured PHI

Privacy & Security Policies and Procedures

- Especially be sure that no health plan information is disclosed to or used by the employer to make employment decisions.

HITECH/HIPAA Update: 9/23/2013
What Law Firms that already provide Health Insurance for their employees need to know

- All CEs are required to update all policies and procedures and forms with the updates in HITECH. Changes include:
  - Modification to and addition of certain definitions;
  - Changes in BAAs (final transition 9/23/2014);
  - Requirement for BAs to pass on BA obligations to Subcontractors;
  - Changes in permitting individual access to PHI;
  - Changes in permitting requests for restriction of PHI;
  - Changes in permitting CE to disclose PHI to those involved in an individual's care;
  - Changes in permitting a CE to use or disclose PHI for marketing;
  - Changes in permitting a CE to use or disclose PHI for fundraising;
  - Changes in the concept of requesting/providing the minimum necessary PHI to accomplish the purpose of the request, use or disclosure;
  - Changes in circumstances in which an authorization is required; and
  - Changes in the identification of breaches of unsecured PHI.

WHY DO CEs and BAs COMPLY?

- Potential for Criminal Penalties:
  - HITECH amended the HIPAA 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 civil money penalties for 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

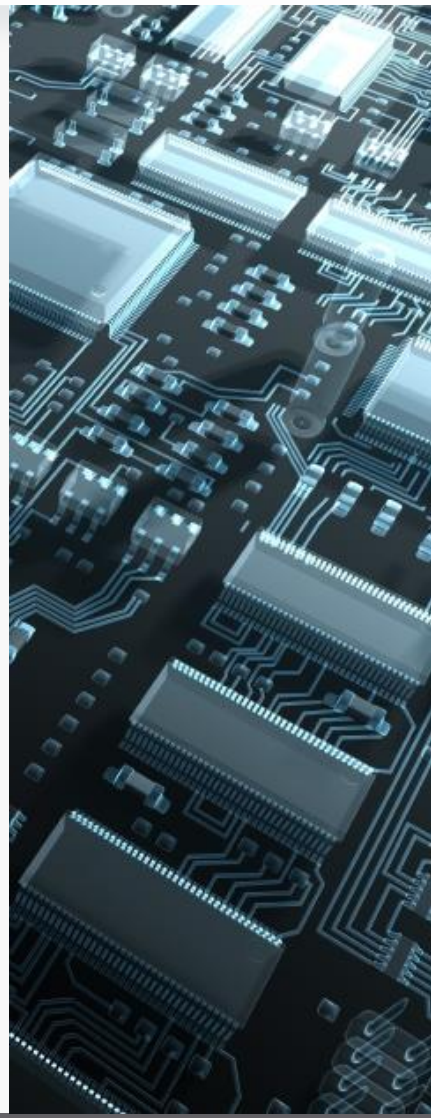
- Phoenix Cardiac Surgery (5 physician practice)
- Complaint: posting surgery and appointment schedules on a publically accessible internet-based calendar
- OCR found a “multiyear, continuing failure” to
  - Implement policies and procedures
  - Document training of employees
  - Identify a security 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 – 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 Corrective Action Plan
  - CMP of $50,000
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf

BA ENFORCEMENT ACTIONS (3/2016)

- "Pharmacy Chain Enters into Business Associate Agreement with Law Firm
- Covered Entity: Pharmacy Chain
- Issue: Impermissible Uses and Disclosures; Business Associates
- A complaint alleged that a law firm working on behalf of a pharmacy chain in an administrative proceeding impermissibly disclosed the PHI of a customer of the pharmacy chain. OCR investigated the allegation and found no evidence that the law firm had impermissibly disclosed the customer's PHI. However, the investigation revealed that the pharmacy chain and the law firm had not entered into a Business Associate Agreement, as required by the Privacy Rule to ensure that PHI is appropriately safeguarded. Without a properly executed agreement, a covered entity may not disclose PHI to its law firm. To resolve the matter, OCR required the pharmacy chain and the law firm to enter into a business associate agreement."*
- * Source OCR website: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html.

What Next?

- Critical: Determine whether your firm is or is not a BA.
- If your firm is a BA, then:
  - Enter into a BAA with each CE client;
  - Arrange for a Security Risk Assessment (if you haven't had one already or recently) by a reputable, experienced provider with appropriate IT credentials;
  - Implement the recommendations of the Risk Assessment;
  - Develop and implement Privacy and Security Policies and Procedures;
  - Train your workforce;
  - Evaluate your compliance program and update as necessary.
- Be sure your Health Plan meets all of the applicable HIPAA and HITECH requirements.

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