HIPAA and Lawyers:
Your stakes have just been raised

October 16, 2013

FENTON | NELSON

Presented by:

Harry Nelson
e: hnelson@fentonnelson.com

Claire Marblestone
e: cmarblestone@fentonnelson.com

AGENDA

- Statutory & Regulatory Framework
  - Privacy/Security Obligations of Lawyers Who Are Business Associates (BA)
  - Obligations of CA Attorneys, Irrespective of HIPAA
- Protecting the Attorney/Client Privilege
- Key Terms
- Are You A BA?
- Complying with the Security and Privacy Rules
- Dealing with Breaches
- Enforcement
- Conclusion

BACKGROUND

- Growing concerns of cyber-security risks and vulnerabilities
- Demonstrated public interest in privacy and security breaches
  - Advanced persistent threats (APT's) to businesses and government (coordinated hacking)
  - Newspaper headlines re: privacy/security violations
- HIPAA Final Omnibus Rule effective September 2013 – applicability to some lawyers
- FTC – Gramm-Leach-Bliley Act – applicability to lawyers?

STATUTORY & REGULATORY FRAMEWORK

Federal Privacy and Security Laws & Regulations

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- 45 C.F.R. Parts 160, 162, 164 (HIPAA Rules)

California Privacy and Security Laws

- CA Customer Records Act (Civil Code § 1798, et seq., as amended by S.B. 1386)
- Confidentiality of Medical Information Act (Civil Code § 56, et seq.)
- The Lanterman-Petris-Short Act (Welf & Inst Code § 5000, et seq.)
- Patient Access to Health Records Act (Health & Safety Code § 123100, et seq.)

Attorney-Specific Obligations

- Duty of Confidentiality – CA Rules of Prof. Conduct 3-100
- ABA Model Rule 1.6: Duty of confidentiality extends to “information relating to the representation of a client” (including electronic data)
- Duty of Competence – CA Rules of Prof. Conduct 3-110(B)

SB 1386 (Civil Code §§ 1798.29, 1798.82, 1798.84)

- Any business that owns electronic data with "personal information" about California residents is required to disclose any breach of security to the resident
- "Personal information": first initial and last name in combination with social security #; driver's license number/ID; account number, credit or debit card number in combination with required security code; medical information; or health insurance information.

PROTECTING THE ATTORNEY CLIENT PRIVILEGE

Attorney-Specific Obligations

- Duty of Confidentiality – Cal. Rules of Prof. Conduct 3-100.
- ABA Model Rule 1.6
- Cal. Bus. & Prof. Code § 6068
- Evidentiary Privilege – Cal. Evid. Code § 952
- Duty of Competence – Cal. Rules of Prof. Conduct 3-110(B)

Cal. Ethics Opinion 2010-179

- Attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential information to an undue risk of unauthorized disclosure.

Cal. Ethics Opinion 2010-179

- Factors to consider when using technology:
  - Attorney's ability to assess the level of security afforded by technology;
  - Legal ramifications to third parties intercepting, accessing, or exceeding authorized use of information;
  - Degree of sensitivity of information;
  - Potential adverse impact on client;
  - Urgency of situation;
  - Client instructions and circumstances.

HIPAA Considerations

- Business Associate Agreements: Explicitly recognize attorney's obligations to protect client confidentiality
- Consider impact on privilege of:
  - Requests for access by patient
  - Requests for accounting of disclosures
  - Other attempts to obtain PHI in your possession


KEY TERMS

Unofficial Guide to Key HIPAA Terms

- Protected Health Information ("PHI"): Data that identifies a specific person and describes his/her demographics, medical status/history, and payment for care.
- ePHI: PHI maintained or transmitted in electronic form
- Covered Entity ("CE"): Individuals and organizations that provide or pay for health care.

45 C.F.R. § 160.103

Unofficial Guide to Key HIPAA Terms

- Business Associate ("BA"): Individual/organization that assists CEs, and use PHI to do so.
- Subcontractor: Individual/organization that assists BAs, and use PHI to do so.
- Business Associate Agreement ("BAA"): Contract between a CE and a BA (or a BA and a Subcontractor) that defines the BA's (Subcontractor's) obligations to protect PHI.

45 C.F.R. § 160.103, 164.504(e)

Unofficial Guide to Key HIPAA Terms

- Uses and Disclosures of PHI: Actions involving PHI in which a CE or BA might engage.
- Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.
- Breach: The acquisition, access, use or disclosure of PHI that is not permitted by HIPAA and that compromises the security or privacy of the PHI.

ARE YOU A BUSINESS ASSOCIATE?

FENTON NELSON

Are you a Business Associate?

- Business associate*:*
  - A business associate means, with respect to a covered entity, a person who provides, other than in the capacity of a member of the workforce of such covered entity, **legal**, actuarial, accounting, consulting, data aggregation …, management, administrative, accreditation, or financial services to or for such covered entity, … **where the provision of the service involves the disclosure of protected health information from such covered entity …, or from another business associate of such covered entity or arrangement, to the person**.

45 C.F.R. § 160.103

FENTON | NELSON

Are you a Subcontractor Business Associate?

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

45 C.F.R. § 160.103

If you are not a BA what are your obligations?

- Attorney-client obligations
  - Ethical duty to inform client of breach of confidentiality
- Customer Records Act
  - Duty to inform CA residents of breaches of personal information.
  - Duty to inform your clients that information they provided to you may have been breached.
- No duty under Gramm-Leach-Bliley Act for attorneys yet.

COMPLIANCE WITH THE SECURITY RULE

FENTON | NELSON

Business Associate Obligations

- General requirements
- Adopt administrative, physical, and technical, safeguards to protect ePHI;
- Organizational requirements; and
- Policies & procedures and documentation requirements.

45 C.F.R. § 164.306, et seq.

Administrative Safeguards

- Security Management
  - Risk analysis and management
  - Sanction policy
  - Activity review
- Designate a Security Officer
- Workforce Training
- Contingency Planning
- Evaluation

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

Technical Safeguards

- Access Controls
- Audit Controls
- Integrity
- Person/Entity Authentication
- Transmission Security

Security Rule Requirements

- Business Associate Agreements
- Policies & Procedures
- Documentation

Best Practices

- Passwords on Electronic Devices
- Lock Your Computer Screen
- Workstation Security
- Portable Device Security
- Data Management
- Anti-Virus Software
- Computer Security
- E-mail Security
- Breach Response

Cyber-Insurance

- Consider:
  - Does your Professional Liability insurance cover breaches?
  - Does your General Liability insurance cover breaches?
- Cyber-insurance is made to cover breaches.

COMPLIANCE WITH THE PRIVACY RULE

Business Associate Uses & Disclosures

- As permitted by the BAA and required by law.
- Specifically required
  - Investigation by the Secretary of HHS
  - Some individual patient requests
- Minimum necessary
- Disclosures to subcontractors
  - Requires a BAA
- Material breach/violation by subcontractors

45 C.F.R. § 164.500, et seq.

Business Associate Agreements

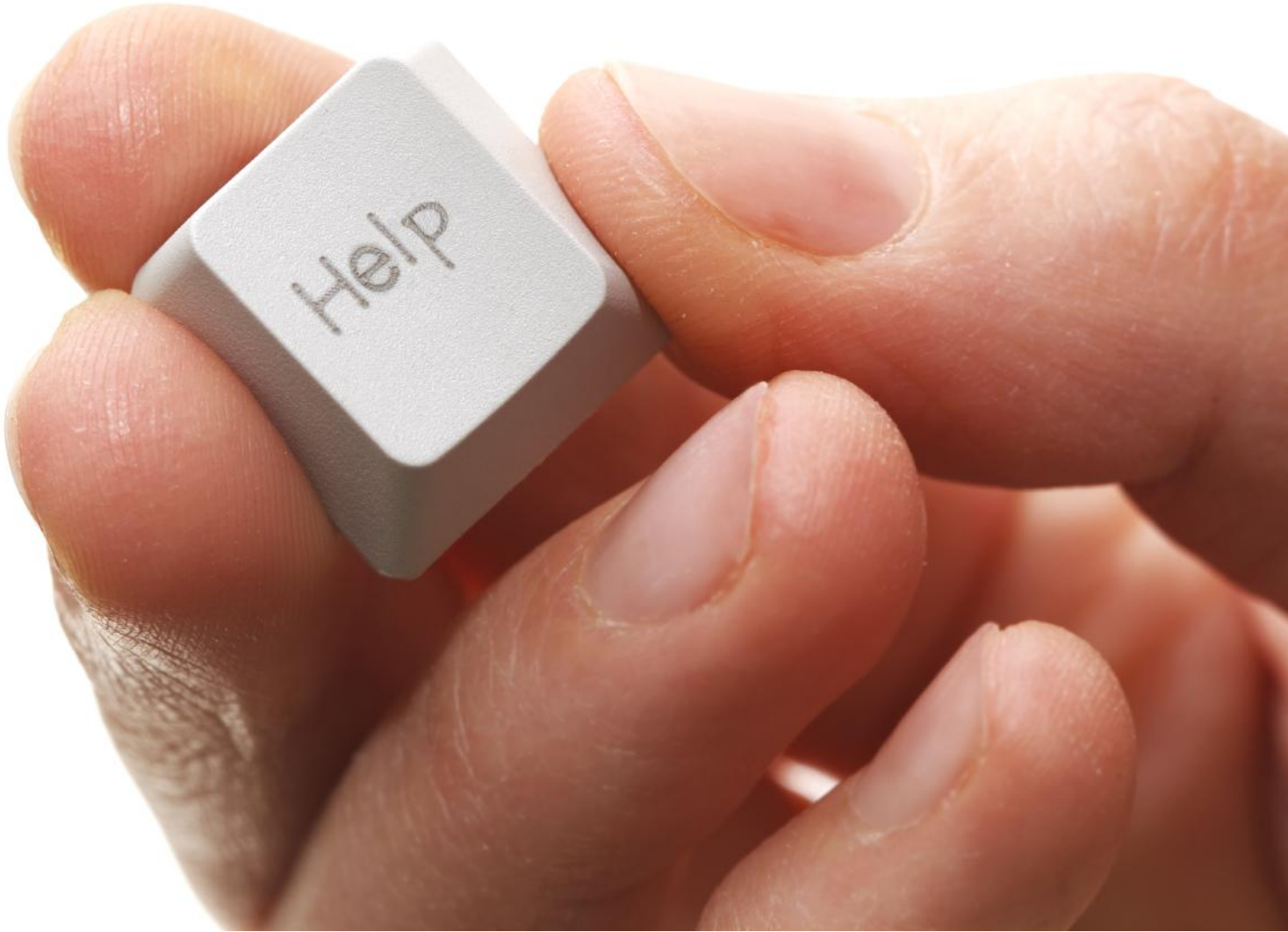
- Required Provisions
  - Appropriate safeguards, including compliance with Security Rule
  - Report non-permitted uses/disclosures to CE, including breaches of unsecured PHI
  - Subcontractor BAAs
  - Comply with Privacy Rule requests from patients, *as applicable*
  - Availability of internal records
  - Effect of termination

45 C.F.R. § 164.504(e)

Business Associate Agreements

- Other Considerations
  - Defining “minimum necessary”
  - Indemnification for breaches
  - Mitigating the effects of breaches
  - Breach notification

DEALING WITH BREACHES



Breach

- The acquisition, access, use or disclosure of PHI in a manner that:
  - Is not permitted by HIPAA; and
  - Compromises the security or privacy of PHI.
- Notification requirements for CE.
- Notification requirements for BA.

45 C.F.R. § 164.400, et seq.

Breach Notification

- Presumption: A security incident involving PHI is a breach
  - *Unless* CE/BA can demonstrate that there is a “low probability” that PHI has been compromised
  - Risk assessment factors include:
    - Nature of PHI involved, including likelihood of reidentification
    - Identity of the unauthorized user/recipient
    - Actual acquisition/viewing
    - Extent of mitigation of the risk

California Breach Notification

- Business that maintains computerized data, including personal information, that the business does not own shall notify the owner of the information of any breach of the security of the data if the information was obtained by an unauthorized person.
- Personal information includes medical information.
- Notification requirements.

Cal. Civ. Code § 1798.82

ENFORCEMENT

Enforcement

- The Office of Civil Rights ("OCR")
  - Investigates complaints
  - Conducts compliance reviews
  - Performs education and outreach
- California Office of Health Information Integrity ("CALOHII") also may impose administrative fines, civil penalties, and other disciplinary actions

Civil Penalties - HIPAA

Type of Violation	Per Violation Penalty
Did not know	$100-50,000
Reasonable Cause	$1,000-50,000
Willful Neglect, Corrected	$10,000-50,000
Willful Neglect, Not Corrected	$50,000

Maximum penalty: $1.5 million

- Criminal penalties range from $50,000 and/or imprisonment for one year, to $250,000 and/or imprisonment for up to 10 years.
- In addition, state attorneys general have authority to bring civil actions on behalf of residents of the state.

Civil Penalties - California

	Any Person or Entity (other than a licensed healthcare professional)	Any Licensed Healthcare Professional
Negligent Disclosure	Up to $2,500	Up to $2,500
Knowingly and Willfully Obtains, Discloses or Uses	Up to $25,000	1st Violation: Up to $2,500 2nd Violation: Up to $10,000 3rd Violation: Up to $25,000
Knowingly and Willfully Obtains, Discloses or uses for Financial Gain	Up to $250,000	1st Violation: Up to $5,000 2nd Violation: Up to $25,000 3rd Violation: Up to $250,000

CMIA, Civil Code § 56.36(c)

Certain licensed facilities are also subject to administrative penalties of $25,000-$250,000 for unlawful or unauthorized access to, and use or disclosure of, medical information. Health & Safety Code § 1280.15.

Civil Penalties

- HHS anticipates that it will not exact the maximum penalty in each case.
- Factors considered in assessing penalties:
  - Nature and extent of the violation
  - Nature and extent of the resulting harm
  - Number of individuals affected
  - Prior indications of noncompliance
  - Financial condition of the covered entity
  - Consideration of “other matters as justice may require”

CONCLUSION

Steps for Compliance

- Appoint Security Officer
- Perform and document risk analysis
- Create and/or revise confidentiality and security policies
- Ensure appropriate IT security safeguards are in place
  - Evaluate potential threats
  - Deploy appropriate hardware/software
- Develop, conduct and document attorney/staff training

Steps for Compliance

- Business Associate Agreements
  - Create/update your form
  - Inventory client relationships, execute or amend BAAs as needed
  - Create/update subcontractor form BAA
  - Execute or amend subcontractor BAAs

Questions?

310-444-5244

FENTON | NELSON

Harry Nelson
e: hnelson@fentonnelson.com

Claire Marblestone
e: cmarblestone@fentonnelson.com