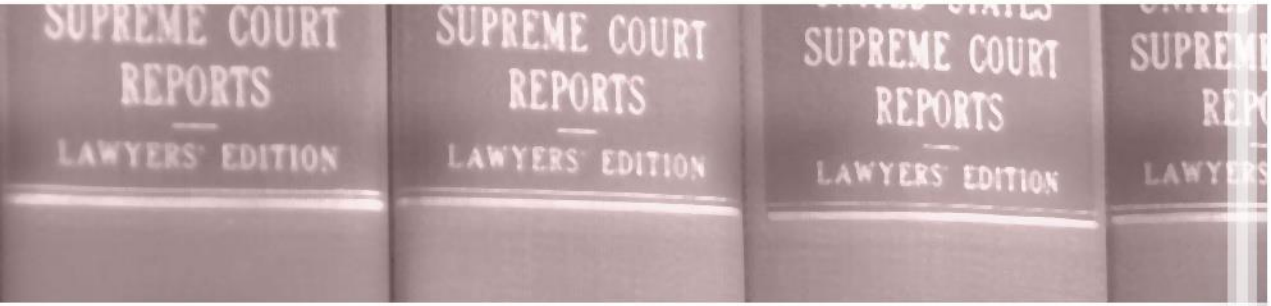

LOWE & EVANDER, P.A.

707 Monroe Road
Sanford, FL 32771
Phone: 407.332.6353
Fax: 407.332.7450
E-mail: mlowe@lowehealthlaw.com
www.lowehealthlaw.com

Medical Records- Practical Practices for Practice Managers

Presented by
Mike Lowe, Esquire
Brian C. Evander, Esquire

VGMA
CENTRAL FLORIDA, FLA.

CFMGMA
January 16, 2019

LOWE & EVANDER, P.A.

707 Monroe Road
Sanford, FL 32771
Phone: 407.332.6353
Fax: 407.332.7450
E-mail: mlowe@lowehealthlaw.com
www.lowehealthlaw.com

This presentation provides education on record management and related legal ***principles***, not specific legal advice

The presenters advise vetting of all your Legal Health Record activities with your legal counsel

HIPAA Megarules, Avoiding Violations

Top 4 Changes for Physicians Under Final Rule

- New responsibilities and liabilities for Business Associates and Subcontractors
- Definition of breach and changes to the Breach Notification Rule
- New and/or expanded patient rights (including access to and restrictions on disclosures of PHI) including New Rights for Patients to Restrict Access to/Disclosure of PHI
- Social Media management

HIPAA Enforcement

With this year's resolution agreements we see many of the same enforcement themes we have seen in previous years, including:

- the importance of conducting an accurate and thorough risk assessment;
- the necessity of business associate agreements; and
- the need to be good at the "basics" of HIPAA compliance.

For instance, a Florida physician group shared protected health information (PHI) with a medical billing services vendor without first entering into a business associate agreement (BAA). The issue of not having a BAA in place with vendors has been a costly oversight for many providers over the past few years. Similarly, disclosing PHI to news media is also a recurring issue and one that appeared again in 2018, this time implicating a physician practice. In that case, one of the practice's physicians disclosed PHI to a reporter at a local television station in response to a public patient complaint. The disclosure led to a $125,000 penalty.

OCR Announcements

OCR continued its regular monthly newsletter and often promoted back-to-basics principles. OCR reminded health care providers about the importance of using simple measures to ensure HIPAA compliance, including:

- Using simple, physical safeguards to protect PHI, like locked cabinets and privacy screens;
- Assessing and mitigating information security risks; and
- Securely disposing and destroying electronic devices and media after they are no longer needed.

Recent HHS/OCR Settlements

- Phoenix Cardiac Surgery (April 2012) - $100,000 settlement and corrective action plan with a small cardiothoracic surgery physician practice, over its failures to comply with the HIPAA Security Rule. The practice's alleged actions included the posting of electronic protected health information ("ePHI") on "a publicly accessible, Internet-based calendar" and transmission of ePHI to employees' personal, Internet-based e-mail accounts. OCR also alleged failures to have adequate policies, train the medical group workforce on HIPAA, assign a security officer, conduct an accurate and thorough risk assessment, and obtain a business associate contract from the Internet-based calendar and e-mail providers that allegedly maintained ePHI on the medical group's behalf.

- Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (September 2012) - $1.5 million settlement which also required a three-year corrective action plan with external monitoring.

- Hospice of Northern Idaho (December 2012) - $50,000 settlement involving stolen laptop computer with failure to encrypt PHI and also to take corrective action. Self-reported case through breach notification process (June 2010).

- Massachusetts and New Hampshire dermatology practice, Adult & Pediatric Dermatology PC (December 2013) – failure to perform risk analysis as required under the HIPAA Security Rule, implement written breach notification policies and procedures, and provide breach notification training- $150,000 settlement which also requires a corrective action plan. The investigation resulted from a report of the theft of an unencrypted thumb drive from a vehicle.

Top Cybersecurity Risks for Healthcare Industry

- Clearwater Compliance's newest CyberIntelligence Insight Bulletin concludes that the top three cybersecurity risks for the healthcare industry, which accounts for 36.8% of reported critical risk incidents include:

  1) user authentication deficiencies, including placing passwords in obvious places where others can find them like on the computer monitor or under the keyboard, using generic user IDs and passwords that can be compromised and emailing user credentials unencrypted;

  2) endpoint leakage; and

  3) excessive user permissions.

Consequences of Non-Compliance

- HIPAA/OCR Investigations and penalties
- Civil lawsuits for breach of or failure to maintain a patient's confidentiality
- Complaints to state licensing boards (Board of Medicine, Board of Osteopathic Medicine, Board of Podiatric Medicine) and possible disciplinary action
- Patient dissatisfaction and bad publicity/public relations

HIPAA Security Basics: Keeping your Medical Web-Based Business Complaint

If you are handling any PHI on or through your website, you must ensure that your website is HIPAA complaint. Here are some recommendations to address the security and privacy of PHI that your website may manage (please note that this is not a comprehensive list):

- **Unique User Identification**: each user should have a unique User ID so that use can be tracked.
- **Automatic Logoff**: implement electronic safeguards that terminate an online session after a period of inactivity.
- **Authorization:** the PHI should only be accessible by authorized personnel.
- **Storage:** PHI must be encrypted when it is stored or archived.
- **Fire Transfer Protocol:** don't Use File Transfer Protocol (FTP) to transfer patient data.
- **Remote access:** When accessing data from remote locations for telecommuting, use a Virtual Private Network because it creates a temporary encrypted connection that only exists during the period of use.

HIPAA Security Basics: Keeping your Medical Web-Based Business Complaint

- **SSL encryption:** In order to safely transmit information online, a SSL (Secure Sockets Layer) certification provides the encryption of sensitive data, including financial and healthcare.
- **Data must be sent through a secure network:** HIPAA-protected information should never be sent through an unencrypted network to an insecure email account. If you want to receive this data by email, it should be encrypted from sender to recipient. Another option would be to store the information on your HIPAA-compliant server, and set up email alerts any time new data is submitted by a user on your website. Users would instead log into your server account to retrieve the information.
- **Privacy Policy:** Your privacy policy must be regularly updated to keep up with any changes in the law or your practice's privacy policy to stay HIPAA-complaint.

Overview

- Section 456.057, Florida Statutes
  - Medical record ownership statute for licensed health care practitioners

- Sections 395.3015 and 395.3025, Florida Statutes
  - Patient medical record requirements for licensed facilities (primarily hospitals and ambulatory surgical centers ("ASCs"))

(Brief Reference/Reminder)

Florida Law – Superconfidential Information

- Categories
  - HIV/AIDS
  - Mental Health
  - Substance Abuse
  - Reportable STDs/Communicable Transmissible Diseases
  - Pregnant Minors
- Must have <u>specific</u> authorization from the patient to release this type of information. General consent (i.e., patient consents to release of all of the patient's information in medical records) <u>not</u> sufficient

Aetna $17.2 Million Breach Settlement Brings Lessons for Handling Health Data

- Aetna will pay almost $17.2 million to settle a federal class action lawsuit stemming from a 2017 mailing that disclosed the HIV status of health plan members. Aetna also agreed in January 2018, to pay a $1.15 million fine to the state of New York after the Attorney General Eric Schneiderman's (NY AG) investigation into Aetna's alleged violations of federal and state privacy laws. Both settlements require compliance monitoring and record keeping obligations.

- Ironically, the mailings at issue were a required part of a settlement agreement from other lawsuits against Aetna first brought in 2014 and 2015. As part of those settlements, Aetna was required to mail notice to certain customers of the various options for obtaining HIV medications. Thousands of patients received the mailing from Aetna—names and addresses, and also HIV status, were visible through the clear window of the envelopes. Family, friends, roommates, landlords, neighbors, co-workers, mail carriers, or even complete strangers could see the individuals HIV status through the address window. In addition to the class action lawsuit, the NY AG launched an investigation.

- Adding a HIPAA twist, the lawsuit and NY AG alleged that although Aetna sent protected health information to its outside counsel handling the matter under a HIPAA business associate agreement, neither Aetna nor its outside counsel executed a business associate agreement with the third party settlement administrator engaged to mail the notices. The settlements highlight the importance of maintaining and implementing comprehensive policies and procedures, and related trainings and audits, to prevent unauthorized disclosures of protected health information (PHI).

- Covered entities' responsibilities to safeguard PHI extend beyond technical controls. "Low-tech" breaches, including mis-directed faxes and mailing errors, continue to be a focus for privacy regulator scrutiny. Even outside the context of litigation, covered entities often use a vendor, or multiple vendors, for mailing services. Aetna's settlements serve as reminders that organizations should have in place and continue to maintain and monitor compliance with policies and procedures to safeguard against unauthorized disclosures of PHI. With regard to vendors, covered entities should review agreements with service providers to ensure they are executing business associate agreements where required and that flow-down provisions are included.

Business Associate Agreements

- A. Patient Rights
- B. Subcontractors
- C. Reporting/Handling Breach
- D. Termination of BAA- What do I do now?

Business Associates

- What is a “business associate”?
  - Person or company which performs an activity or service for a Covered Entity that involves the use or disclosure of individually identifiable health information or any other function regulated by the Privacy Standards

Business Associates

- What is a “business associate”?
  - Examples of business associates are firms conducting claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or legal, actuarial, accounting, consulting, management, accreditation, administrative, or financial services (Refer to BA Matrix Spreadsheet in Downloadable Tools)
  - HHS does not have the statutory authority to regulate business associates

Implications of the HIPAA Final Rule for Business Associates

- The final rule added the following to the definition of business associate

1. A health information organization, e-prescribing gateway, or other entity that provides data transmission services to a covered entity and requires access on a routine basis to protected health information (PHI). The preamble to the final rule clarifies that an entity that is a mere conduit (such as a courier service) does not require access to PHI, and therefore is not included.

2. An entity that offers a personal health record (PHR) on behalf of a covered entity. However, if the PHR is not offered on behalf of a covered entity, the PHR vendor is not a business associate.

3. A subcontractor. The regulations provide that if a business associate subcontracts part of its function requiring access or use of PHI to another organization, that subcontractor is also subject to HIPAA. There must be an agreement between the business associate and its subcontractor that contains the elements required to be included in business associate agreements and describes the subcontractor's permitted uses and disclosures of PHI (which may not include uses and disclosures not permitted to the business associate).

Implications of the HIPAA Final Rule for Business Associates

- New responsibilities and liabilities under HIPAA for Business Associates

1. To keep records and submit compliance reports to HHS, when HHS requires such disclosure in order to investigate the business associate's compliance with HIPAA, and to cooperate with complaint investigations and compliance reviews.

2. To disclose PHI as needed by a covered entity to respond to an individual's request for an electronic copy of his/her PHI

3. To notify the covered entity of a breach of unsecured PHI

4. To make reasonable efforts to limit use and disclosure of PHI, and requests for PHI, to the minimum necessary

5. To provide an accounting of disclosures

6. To enter into agreements with subcontractors that comply with the Privacy and Security Rules.

BAAs & Breach Notification under the New HIPAA/HITECH Omnibus Final Rule

- The timeframe within which the business associate ("BA") must notify the covered entity ("CE") of a breach
- Indemnification for breach expenses
- Cooperation in breach risk assessment
- Cooperation in HIPAA investigations
- Reporting of unsuccessful Security Incidents
- The extent to which the CE may direct the patient rights duties of the BA
- The right of the BA to operate outside the U.S., including storing data offshore
- Audit rights
- BA's right to de-identify protected health information ("PHI")
- BA's right to use PHI for management and administration and data aggregation purposes
- Defining when return or destruction of PHI upon termination of BAA is infeasible
- The extent to which the provisions in the BAA between the BA and its subcontractor shall be identical to the BAA between such BA and the CE.

New Patient Rights

- Right to Request Restrictions on Disclosures
- Expanded Patient Rights to Request Electronic Copies
- NPP's Heads up!

Patients' Right to Request Restrictions on Release of Records – Key Provisions in the Final Rule

- **Medical Records**. Providers do not need to create separate medical records or segregate PHI subject to a Required Restriction. However, they will need to flag or use some other method to identify portions of the record that contain PHI subject to a Required Restriction to ensure it is not inadvertently sent or made accessible to the health plan for payment or healthcare operations purposes (for example, PHI subject to a Required Restriction must be excluded from records made available to a health plan during performance of an audit).

- **Bundled Services**. To the extent a patient requests a restriction with respect to one of several items or services provided in a single patient encounter, the provider should counsel the patient on the ability or inability of the provider to unbundle the services and the consequences of doing so (i.e., the health plan may still be able to identify the services performed based on the context). If the provider cannot unbundle the items or services, the provider should inform the patient and give the patient the option to restrict and pay out of pocket for the entire bundle of items or services.

Patients' Right to Request Restrictions on Release of Records – Key Provisions in the Final Rule

- **Dishonored Payments**. Providers need not abide by a restriction if a patient's payment is dishonored. However, HHS expects providers to make reasonable attempts to resolve payment issues with the patient prior to disclosing PHI to the health plan. Further, a provider may choose to require payment in full at the time the restriction is requested to completely avoid payment issues.

- **Downstream Providers**. Providers are not required to notify downstream providers of Required Restrictions. This remains the patient's responsibility. Providers are encouraged to counsel patients that for the restriction to apply to other providers, the patient must request a restriction and pay out of pocket for care rendered by other providers.

- **Follow-up Care**. If the patient does not request a restriction and pay out of pocket for follow-up treatment, the provider may include previously restricted PHI when billing the health plan for the follow-up treatment, if necessary to have such service deemed medically necessary. No patient authorization is required to disclose the previously restricted PHI.

Patients' Right to Request Restrictions on Release of Records – Key Provisions in the Final Rule

- **Health Maintenance Organizations (HMOs)**. Contractual requirements for a provider to submit claims to an HMO do not exempt the provider from his or her obligations with respect to Required Restrictions. Provider contracts may need to be updated to be consistent with these new requirements.

- **Mandatory Billing Rules**. Generally, a provider may submit PHI to a government health plan as required by law (e.g., mandatory claim submission laws). However, there are various mechanisms that may allow a provider to avoid such legal mandates (e.g., if the patient refuses to authorize submission of a bill to Medicare). Providers must utilize such mechanisms in order to comply with the request for a Required Restriction.

Patients' Right to Request Restrictions on Release of Records – Key Provisions in the Final Rule

- In response to the Final Rule, covered entities may wish to consider the following actions:
  - Identify personnel whose job functions will be affected by the Final Rule and ensure that they are properly trained in implementing Required Restrictions and protecting restricted PHI.
  - Review and alter policies and procedures to comply with the Final Rule.
  - Consider whether electronic systems need to be updated to allow them to communicate with each other to ensure that information is not disclosed to, and health plans are not billed for, items or services subject to a Required Restriction.

Patients' Right to Electronic Access and Copies of Their Records

- In the Final Rule HHS has clarified the following:
  - The electronic copy provided must include all of the electronic PHI held by the covered entity in a designated record set, or appropriate subset if only specific information is requested, at the time the request is fulfilled.
  - If the electronic PHI contains a link to images or data, the images or other data must be included in the electronic copy provided.
  - If a medical record is in mixed media (e.g., some paper and some electronic PHI), the covered entity is not required to scan the paper documents to provide a single electronic copy. Although a covered entity would have this option, a combination of electronic and hard copies may be provided.
  - A covered entity is not required to use an individual's flash drive or other device to transfer the electronic PHI if the covered entity has security concerns regarding the external portable media.
  - If secure email is not available and an individual requests to receive the electronic copy via unencrypted email, the covered entity may send the electronic copy in this fashion, but only if the covered entity has advised the individual of the risk that the information could be read by a third party.

Patients' Right to Electronic Access and Copies of Their Records

- Transmitting to Third Parties

  –The final rule adopts the proposed rule's requirement that, if requested by an individual, a covered entity must transmit the electronic copy directly to another person designated by the individual. HHS clarified that covered entities may rely on information provided by the individual regarding the third-party recipient, but they must implement policies and procedures to verify the identity of any person requesting PHI and implement reasonable safeguards to protect the information disclosed.

Patients' Right to Electronic Access and Copies of Their Records

- Fees/Costs
  - The final rule adopts proposed amendments to include labor costs for copying PHI, whether in paper or electronic form, as one factor that may be included in the reasonable, cost-based fees that may be charged to individuals. HHS clarified that labor costs could include the technical staff time spent creating or copying electronic files, such as compiling, extracting, scanning, and burning PHI to media. Reasonable, cost-based fees also may include: (1) the costs of supplies for creating electronic media (e.g., discs, flash drives) if the individual requests the copy on portable media; and (2) postage if the individual requests mailing or delivery of electronic media. However, under the final rule, covered entities may not: (1) include costs of new technology, maintaining systems for electronic PHI, data access, and storage infrastructure; or (2) charge a retrieval fee (whether a standard fee or actual costs) for electronic copies. Finally, under the state law preemption provisions of HIPAA, a state law imposing lower costs limits would apply. Thus, if costs permitted under HIPAA exceed the state law limits, the covered entity may not charge more than the state law allows.

Patients' Right to Electronic Access and Copies of Their Records

- Timeliness
  - The final rule decreases the time within which covered entities must respond to requests for access from 90 to 60 days by removing the provision allowing an additional 30 days to respond if PHI is not maintained onsite. Covered entities now have 30 days to respond, but they may have a one-time extension of up to 30 days upon provision of written notice to the individual, including the reason for the delay and the expected date of completion. HHS considered, but declined to adopt, different timelines for electronic versus paper copies, opting instead for a single standard.

Required Changes to Notice of Privacy Practices Under the New Final Rule

- The eight changes to the NPP requirements for healthcare providers are the following:

1. The NPP must include a description of the types of uses and disclosures which require an authorization in the following three areas: 1) disclosure of psychotherapy notes; 2) disclosures for marketing purposes; and 3) disclosures that constitute a sale of protected health information. The NPP also must state that other uses and disclosures not described in the NPP will not be made unless an individual provides an authorization and that authorizations may be revoked prospectively at any time by written revocation.

2. The NPP must explain the right of an individual to restrict disclosures of Protected Health Information (PHI) to a health plan for payment or health care operation purposes (but not for treatment purposes) for items or services which an individual has paid for in full and out-of-pocket. Providers will also need to adopt some method to flag in the record any such mandatory restrictions.

3. If a provider intends to use PHI for fund-raising purposes, it must inform the individual of such intent and of the individual's right to opt out of receiving fundraising communications.

4. The NPP must inform the individual of the right to be notified following a breach of the individual's unsecured PHI.

Required Changes to Notice of Privacy Practices Under the New Final Rule

5. The NPP must advise the individual that PHI may not be sold without the individual's express written authorization.

6. One prior requirement for NPPs has been removed: NPPs should no longer include a statement that the provider may send communications regarding treatment alternatives or health-related products or services if the provider is paid by a third party to make the communication. This change is due to the fact that the Omnibus Rule treats subsidized treatment communications as marketing and requires an individual's authorization before such communications can be made.

7. A health care provider that maintains a physical service delivery site must make the NPP available at the site for individuals to take with them, and also must post the NPP in a "clear and prominent" location where individuals will be able to read it.

8. When an NPP is revised, as it must be by September 23, 2013, a health care provider is not required to mail out the new NPP, but rather to make the new NPP available to individuals upon request on or after the effective date of the revision, and to follow Step 7 above, if applicable. Of course, any new patient encounter after revision will require delivery of the NPP and an attempt to have the patient acknowledge receipt of the NPP.

Social Media Marketing/
Patient Communication Pitfalls
(to text or not to text? Or email …)

Intersection of Law and Social Media

- **Professional Liability/Risk Management**
  - Highly recommend not giving medical advice, consultation, care, treatment, etc. via social media
  - Try to document all social media correspondence and communications that may involve medical advice, consultation, care, treatment, etc. in the patient's record
  - Check with your professional liability insurance carrier to determine if such communications or correspondence are covered or excluded from your policy
  - Develop a written policy and procedure for your practice and physicians on the use of social media and communication with patients

Intersection of Law and Social Media

- **HIPAA/Florida Medical Record Confidentiality Law Considerations (§ 456.057, F.S.)**
  - Use written consent/authorization forms that clearly identify the use of social media for patient communication purposes and the patient's authorization to do so
  - Use HIPAA compliant procedures for secure transmissions and/or encryption for e-mails, Facebook or Twitter
  - Try to avoid posting any patient information in social medias if at all possible
  - Never put superconfidential information (HIV/AIDS, STDs, substance abuse, mental health, etc.) in social media, even if the patient requests it (highly recommend declining such requests)

“Cybersituations”

Practical Advise for Conducting a HIPAA Security Assessment

Security Assessment

- Examples of Administrative Safeguards
  - Continual risk assessment of your health IT environment.
  - Continual assessment of the effectiveness of safeguards for electronic health information.
  - Detailed processes for viewing and administering electronic health information.
  - Employee Training on the use of health IT to appropriately protect electronic health information.
  - Appropriately reporting security breaches (e.g., to those entities required by law or contract) and ensuring continued health IT operations.
  - Securely configured computing equipment (e.g., virus checking firewalls).

- Examples of Physical Safeguards
  - Office alarm systems.
  - Locked offices containing computing equipment that store electronic health information.
  - Security guards.

- Examples of Technical Safeguards
  - Securely configured computing equipment (e.g., virus checking firewalls).
  - Certified applications and technologies that store or exchange electronic health information.
  - Access controls to health IT and electronic health information (e.g., authorized computer accounts).
  - Encryption of electronic health information.
  - Auditing of health IT operations.
  - Health IT backup capabilities (e.g., regular backups of electronic health information to another computer file server).

Let’s Get Real: What to do Next

- Risk Assessment
  - Evaluating what you have and what the risk is of a problem
  - Planning on how to reduce/limit the risk
  - Implementing the Plan
  - Documenting it
  - Conducting it under attorney-client privilege
- Policies and Procedures
  - Matching them to your Plan
  - Telling and working with your team on expectations
  - Documenting your internal/external rules
- Inside and Outside Technical and Policy Writing Help

Covered Entities: Assemble the Team

- Identify Individuals to Address HIPAA Privacy Changes
  - Privacy and security officer
  - Health information management/medical records
  - Information technology
  - Legal
  - Risk management
  - Policies administration/management
  - Contracts administration/management
  - Human resources/training
  - Marketing/fundraising

Covered Entities: Assess Current Compliance

- Review Policies and Procedures
  - Complete? Accessible? Followed?
- Business Associate and Data Use Agreements
  - In place? Current? Gathered together?
- Other Requirements:
  - NPP, access, accounting, amendment, restrictions on use/disclosure, confidential communication arrangements, personnel, training, documentation
- Address Gaps

Covered Entities: Business Associates

- Policies and Procedures
  - Types of business associates
  - Agreement content
    - Compliance with updated privacy and security requirements
    - Breach notification
    - Accountings of disclosures

- Contract Management

Top 8 Ways You’re Violating HIPAA Article

Are You Financially Prepared for a Data Breach? Article

Breach Notification – OMG- I have a Breach!!! Now What?

Prior Notification Obligations in Case of Breach of PHI or PHR

Effective by August 16, 2009 (interim final regulations due)

- Covered Entities – Upon discovering a breach of unsecured personal health information ("PHI"), a CE will be required to notify the affected individual(s) and, if more than 500 individuals are affected, HHS and prominent media outlets serving the area. CEs will be required to maintain and submit annually to HHS a log of all breaches.

- Business Associates – Upon discovering a breach of unsecured PHI, a BA will be required to notify the CE.

- PHR Vendors and Entities – Upon discovering a breach of security of personal health records ("PHR"), a PHR vendor or entity will be required to notify the affected individual(s) and the Federal Trade Commission ("FTC").

- Third-Party Service Providers – Upon discovering a breach of security of PHR health information, third-party service providers that provide services to PHR vendors or entities that offer products and services through a website will be required to notify the PHR vendor or entity.

Changes to Breach Notification in Final Rule

- The Final Rule retains many requirements from the interim final breach notification rule. However, it removes the "risk of harm" standard in exchange for a more objective standard for determining whether a "breach" has occurred. (Thus, inquiry into whether there is a significant risk of harm to privacy and security is no longer appropriate.)

- The Final Rule establishes a presumption that impermissible uses and disclosures of PHI are breaches, unless an exception applies. Covered entities can rebut that presumption (removing the notification requirement) by engaging in a risk assessment to determine whether there is a low probability that PHI has been compromised. However, because of the presumption, covered entities may avoid the risk assessment and provide notification.

Changes to Breach Notification in Final Rule

- A risk assessment would examine at least the following four factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - 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.
- If no exception applies and, after reviewing all of these factors, the covered entity cannot demonstrate that there is a low probability of compromise to the PHI, notification is required.
- The OCR cautioned that, when working through these factors, many forms of health information can be sensitive, not just information about sexually transmitted diseases, mental health diseases or substance abuse. In addition, the OCR confirmed that violations of the minimum necessary rules also could result in breaches requiring notification.

Changes to Breach Notification in Final Rule

- **OCR clarified other aspects of the breach notification rule:**
  - The time for notification begins to run when the incident is known to have occurred, not when it has been determined to be a breach. However, a covered entity is expected to make notifications after a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual(s).
  - The obligation to determine whether a breach has occurred and to notify individuals remains with the covered entity. However, covered entities can delegate these functions to third parties or BAs.
  - Written notification by first-class mail is the general, default rule. However, individuals who affirmatively agree to receive notice by e-mail may be notified accordingly. In limited cases, individuals who affirmatively agree to be notified orally or by telephone may be contacted though those means with instructions on how to pick up the written notice.
  - Notices of Privacy Practices must include a statement that covered entities must notify affected individual following a breach

Privacy Violations and Breaches

- HITECH is definitely pushing for all PHI to be secured, methods of disclosing that are unsecured (i.e. paper & faxes) are not encouraged

- 'Breach' defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the Privacy & Security of unsecured PHI and is going to be very strictly enforced

- Cases of PHI Breach will cause the CE, Data Exchange or PHR (Personal Health Record) to notify the Individual of all breaches of their unsecured PHI that were determined to have the potential for harm.
  - If HHS Secretary (OCR) must be notified as well
  - Media must also be notified if over 500 names and posted on your website

- 'Secured 'vs. 'unsecured' PHI is a very complex set of concepts, thorough understanding of these terms and which of your data falls into which category is mandatory.

Privacy Violations and Breaches

- Snooping into electronic records, unauthorized access, is definitely a privacy violation, but if the records are ‘secured’ according to definition the violation need not be reported to Individuals or OCR

- Inadvertent access by employees, as long as they immediately close the records they accessed without reading is not a privacy breach

- Misdirected faxes are a privacy violation as are lost, mailed paper record copies are too, may also be technically a ‘breach’

- CE must make ‘harm’ determination, whether there is a potential for reputational or financial harm resulting from the violation . If there is the potential for harm to the Individual (and the PHI is unsecured according to definition) then the violation is a breach and both the Individual and OCR must be notified.

- Get ready! HHS has just stated that not knowing is no excuse, in fact beware of Willful Neglect!

- Notification methods listed, in HITECH could be burdensome for CE

Privacy Violations and Breaches

- Set-up your Policies, Procedures and forms now.
- I like to use the term ‘Privacy Events’, they are not Breaches until that is determined by defined procedure
- Very complex set of Policies and Procedures to structure, must be aware of all the rules and apply them to areas like Harm Threshold Analysis, how to determine unsecured vs. secured PHI and who needs to be notified when
- Remember BAs have to report Privacy Events to CEs asap, make sure that the CEs and BAs coordinate
- Breach reporting:
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Privacy Event, Breach, Harm Threshold Analysis and Notification

- Purpose
  - To provide foundational elements for the determination and response to Privacy Violations, Breaches (wrongful acquisition, access or disclosure) of PHI (Protected Health Information), the resultant Harm Threshold Analysis and Breach Notification responsibilities, policies and procedures that may occur from both HIPAA and State perspectives.

- Policy
  - Create your policy to cover appropriate areas of the overall policy scope.
  - Let’s review the Policy example

Privacy Event, Breach, Harm Threshold Analysis and Notification

Key Steps in Breach Procedure

1. Investigation and documentation by CE (or BA) of a Privacy Event.
2. Final determination of whether a Privacy Violation has occurred.
3. Determine if a Breach of *unsecured* PHI has probably occurred;
4. If unsecured PHI has been breached perform a Harm Threshold Analysis.
    a) If a HIPAA Privacy violation of unsecured PHI has occurred notify OCR either immediately (if over 500 individuals per event) or annually (if under 500 individuals per event).
    b) If less than 500 individuals per Breach were involved notify OCR annually.
5. If required, notify individuals(s) of a breach of their PHI.
6. Feedback, mitigation, sanctions and corrective actions developed and recorded.

Steps for Privacy Breaches

- **<u>What is Secured PHI?</u>**
- On April 27, 2009, HHS issued the HITECH Breach Notification Guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

- *Encryption*. Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The Rule identifies the various encryption processes which are judged to meet this standard. Further, such confidential process or key that might enable decryption must not have been Breached. To avoid a Breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

- *Destruction*. Hard copy PHI, such as paper or film media, is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Steps for Privacy Breaches

- **Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule.** For an acquisition, access, use, or disclosure of PHI to constitute a Breach, it must constitute a violation of the HIPAA Privacy Rule.

- **Analyze whether there is a use or disclosure that compromises the security and privacy of PHI (Harm Threshold Analysis).** See Use case and Q&A Tools

- **Assess Whether any Exceptions to the Breach Definition Apply.** The Rule discusses a number of exceptions to the definition of Breach. The following three situations are excluded from the definition of "Breach" under the Act:
  - The unintentional acquisition, access, or use of PHI by any 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
  - The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a CE or BA to another person at the same CE or BA, or at a organized health care arrangement in which the CE participates
  - An unauthorized disclosure where a CE or BA has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Notification Requirements

- **<u>Notification Requirements to Individuals and /or Media in the Event of a Breach of Unsecured PHI</u>**

- The Breach notifications required by the Act and the Rule are significant and are triggered by the "discovery" of the Breach of unsecured PHI. A Breach is treated as "discovered" by a CE as of the first day the Breach is known, or reasonably should have been known, to the CE.

- **Notification to Individuals.** A CE must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach, without unreasonable delay and in no case later than 60 calendar days after the date the Breach was first discovered by the CE. Or sooner if state law is more stringent (i.e. Florida is 45 days).

- **Notification to Media.** If a CE discovers a Breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction

Notification Requirements

- **Notification to HHS (OCR).** If more than 500 individuals (are involved in the Breach, regardless of whether the Breach involved more than 500 residents of a particular State or Jurisdiction, then the CE must notify HHS concurrently with the individual notifications.

- For Breaches involving fewer than 500 individuals, the CE must maintain an internal log or other documentation of such Breaches and annually submit such log to HHS.

- **Notification by a Business Associate.** Following the discovery of a Breach of unsecured PHI, a BA is required to notify the CE of the Breach so that the CE can, in turn, notify the affected individuals. To the extent possible, the BA should identity each individual whose unsecured PHI has been, or is reasonably believed to have been, Breached. CE should notify CE of suspected privacy violation or breach within 1 business day

Methods and Contents of Notice

- **Methods of notification include:**
  - First class mail to last known address
  - Or e-mail if preferred by patient
  - Provide for substitute notice if insufficient or unknown contact information
  - In the case of a Breach with 10 or more patients with unknown contact info post general info in media, site website and have a toll free number to call

- **Contents of Breach Notification:**
  - Dates of Breach and Discovery
  - Brief description of what happened
  - Description of types of information involved
  - Steps individuals should take to protect themselves
  - Brief description of CE (or BA) remediation actions
  - Contact information for individuals to learn more

- **Timing of notification:** Without unreasonable delay, not longer than 60 days after discovery

LOWE & EVANDER, P.A.

707 Monroe Road
Sanford, FL 32771
Phone: 407.332.6353
Fax: 407.332.7450
E-mail: mlowe@lowehealthlaw.com
www.lowehealthlaw.com

Copies and contact information

Request copies of this presentation
and more information from

Michael R. Lowe, Esquire

www.lowehealthlaw.com

407-332-6353