“ONCE MORE UNTO THE BREACH, DEAR FRIENDS, ONCE MORE…”

Revisiting the PHI Breach
Under HIPAA and HITECH and
Considerations for Ophthalmologists

Neil H. Ekblom, Esq.
885 Third Avenue, 16th Floor, New York, NY 10022
212.430.8031 | neil.ekblom@leclairryan.com

AAO Meeting New Orleans, November 16, 2013
To follow along on your laptop or tablet:

http://www.leclairryan.com/aaoc-conference/
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Privacy Rule – applies to all Protected Health Information (PHI) (including EPHI and oral and paper forms).

- Security Rule – applies to EPHI. Now Business Associates (BAs) as well as covered entities (CEs) must comply with entire HIPAA security rule. (Omnibus Rule, Jan. 25, 2013)
Health Information Technology for Economic and Clinical Health Act (HITECH)

- **Breach Notification Rule**: Requires HIPAA CEs and BAs to provide notification following a breach of unsecured PHI where there is a significant risk of harm to the subject person. (Dec. 2009)

- **Omnibus Rule**: Implements provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA. (Jan. 25, 2013)
Omnibus Rule Changes for BAs

PHYSICIAN PRACTICE

CONTRACTOR

SUBCONTRACTOR

NOTIFICATION

NOTIFICATION
Definitions

- What is Protected Health Information?
  - Individually identifiable health information held or transmitted by a CE or its BA in any form or media, whether electronic, paper or oral.

- What is Unsecured Protected Health Information?
  - PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons.

- What is De-Identified Health Information?
  - Does not identify or provide a reasonable basis to identify the individual.
It’s a breach (triggering notification requirements) if the following applies:

1. It involves use or disclosure of unsecured PHI, and
2. It is a use or disclosure of PHI not permitted by the HIPAA privacy rule, and
3. It does not fit within three exceptions in the HITECH rule, and
4. It compromises the security or privacy of PHI.
It’s a breach: (cont.)

1. If it involves use or disclosure of unsecured PHI.
   - PHI is unsecured if not encrypted, destroyed or de-identified and individually identifiable health information remains.
2. If it is a use or disclosure of PHI not permitted by the HIPAA privacy rule. (treatment, payment, operations permitted)
It’s a breach: (cont.)

3. If use or disclosure does not fit within three exceptions in the HITECH rule.

   **Exception 1:**
   - A. Unintentional access/acquisition/use of PHI by workforce member of CE or BA,
   - B. in good faith,
   - C. in scope of work, and
   - D. no further HIPAAA prohibited disclosure.
HITECH

Exception 2:
Inadvertent disclosure of PHI by:
A. one workforce member to another at same CE or BA,
B. both authorized to access information, and
C. no further HIPAA prohibited disclosure.
HITECH

Exception 3:
Unauthorized disclosure of PHI to an unauthorized person where:
A. there is good faith reason to believe
B. recipient would not retain information.
It’s a breach: (cont.)

4. If it compromises the security or privacy of PHI, meaning:

- **Old Standard** ➢ Use or disclosure that poses a **significant risk** of financial, reputational, or other harm to the person whose rights were violated.

- **New Standard** ➢ Determining whether compromise exists requires a good faith **risk assessment** by the CE which documents consideration of relevant factors in determination. Notification required unless CE can demonstrate low probability that PHI is compromised based on risk assessment.
## Risk Assessment

<table>
<thead>
<tr>
<th>FACTORS</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nature &amp; extent of PHI involved, including types of identifiers and</td>
<td>SSN, STD, mental health</td>
</tr>
<tr>
<td>likelihood of re-identification;</td>
<td></td>
</tr>
<tr>
<td>The unauthorized person(s) who used PHI or to whom PHI disclosures were</td>
<td>Hacker, layperson, another CE/BA</td>
</tr>
<tr>
<td>made;</td>
<td></td>
</tr>
<tr>
<td>Whether PHI actually acquired or viewed; and</td>
<td>Verbal, paper, electronic, stolen, lost</td>
</tr>
<tr>
<td>Extent to which risk to PHI mitigated.</td>
<td>Investigation, quick response, recovery</td>
</tr>
</tbody>
</table>
Risk Assessment

- CE should provide notice without delay for risk assessment when obvious breach.
- If low probability, presumption overcome and notification not required.
- Documentation of analysis important.
- Meaning of “compromised”:
  - Does it require the potential for harm to persons, or just “use and disclosure” alone?
Not a Breach, Review

- PHI de-identified or destroyed.
- Use or disclosure permitted by HIPAA.
- Where HITECH exception.
- Where risk assessment overcomes presumption.
Breach Notification

- If, under either standard, a breach occurs, then CE (or BA to CE) must:
  1. Give written notice (email if consent) to persons affected within 60 days of discovery (actual knowledge/reasonable diligence).
  2. Notice contains:
     - What occurred/when occurred.
     - PHI content description.
     - Steps people can take to protect themselves.
     - What mitigation commenced.
     - CE or BA contact information.
4. Law enforcement requests notification delay, 30 day extension, or more if in writing.
5. Substitute notice and alternate forms of notice depending on number of persons affected.
6. More than 500 persons requires media notice:
   A. 500 or more, file electronic notice with HHS via website.
   B. Less than 500, notice to HHS within 60 days of calendar year end.
Breach Enforcement

- Investigation by Office for Civil Rights (OCR).
- OCR must investigate “willful neglect” complaints.
- Breach penalties vary depending on culpability:
  - Did not know / with reasonable diligence would not have known.
  - Reasonable cause.
  - Willful neglect.
- Prompt action equals no willful neglect.
Breach Enforcement (cont.)

- State AGs permitted to sue on behalf of residents to obtain damages/injunctive relief + costs and attorneys’ fees.
- HHS Audits.
- Private Right of Action.
State Rules

HITECH rules comparison with state laws required.

- Apply state law first if patients all residents of same state.
- HIPAA privacy rule provides federal baseline.
- If no conflict or state law provides greater protections, both sets of rules must be followed.
- Contrary state law may not be preempted if HHS gives exemption.

Example:
- California and Connecticut - 5 day breach notices to state agencies.
- Florida – 45 days to person.
- Idaho – 24 hours to state AG for certain breaches.
Business Associates

- Contractual obligations.
- Legal obligations and enforcement risk.
- Legal obligations to follow many of the privacy provisions of BAA and HITECH provisions.
- Must now follow HIPAA security rule, as well as downstream contractors.
- Marketing, sales, and research issues, BA can’t sell PHI without authorization, exceptions.
Physician Office Strategy

- Get working knowledge of state law.
- Inventory employees and vendors who handle your office PHI.
- Employees sign off on written PHI office policies + seminar.
- Catalog BAAs for vendors/contractors, subcontractors.
- Revise BAAs to address:
  1. Indemnification, legal costs to defend CE, penalties.
  2. Agency.
  3. Breach notification costs, mitigation and remedy costs.
- Set up an incident response plan in advance, line up outside resources.
- Quick response, decisive corrective action = possibility of no HHS fine.
Thank You

Neil H. Ekblom
neil.ekblom@leclairryan.com
Disclaimer

- This slide show provides general information and is not legal advice and should not be used or taken as legal advice for specific situations. You should consult legal counsel before taking any action or making any decisions concerning the matters in this show. This communication does not create an attorney-client relationship between LeClairRyan, A Professional Corporation, and the recipient.
- Copyright 2013, LeClairRyan, A Professional Corporation. All rights reserved.