What does the latest flurry of HIPAA settlements mean to you?
Are you ready for some HIPAA!

Donna Grindle

30 years in Healthcare IT
Programmer, Tech nerd, Teacher, Podcaster, Blogger, Speaker, and Consultant

Kardon Compliance
Plan: Learn from others mistakes

▷ 2016 OCR settlement headlines
▷ A few case examples
▷ Violations listed in settlements
▷ Corrective Action Plans
▷ What does all this tell you?
2016 settlement headlines

OCR has been busy
<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
<th>2013</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settlements</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>$6,193,400</td>
<td>$6,215,000</td>
<td>$3,740,780</td>
<td>$4,800,000</td>
</tr>
</tbody>
</table>
February 2016

- **February 3** - Administrative Law Judge rules in favor of OCR enforcement, requiring **Lincare, Inc.** to pay **$239,800**
- **February 16** - Physical therapy provider, **Complete P.T., Pool & Land Physical Therapy, Inc.**, settles violations that it impermissibly disclosed patient information to pay **$25,000**
- **Total** **$264,800**
March 2016

▷ March 16, 2016 - North Memorial Health Care $1.55 million settlement underscores the importance of executing HIPAA business associate agreements

▷ March 17, 2016 - Improper disclosure of research participants’ protected health information results in $3.9 million HIPAA settlement with Feinstein Institute for Medical Research

▷ 2016 Total = $5,714,800
April 2016

▷ April 14 - $750,000 settlement highlights the need for HIPAA business associate agreements (Raleigh Orthopaedic Clinic, P.A.)
▷ April 21 - Unauthorized Filming for “NY Med” Results in $2.2 Million Settlement with New York Presbyterian Hospital
▷ 2016 Total = $8,664,800
June 2016

▷ **June 29** - Business Associate’s Failure to Safeguard Nursing Home Residents’ PHI Leads to $650,000 HIPAA Settlement with Catholic Health Care Services of the Archdiocese of Philadelphia

▷ **2016 Total = $9,314,800**
July 2016

▷ **July 18** - Widespread HIPAA vulnerabilities result in **$2.7 million** settlement with Oregon Health & Science University

▷ **July 21** - Multiple alleged HIPAA violations result in **$2.75 million** settlement with the University of Mississippi Medical Center

▷ **2016 Total** = **$14,764,800**
August 2016

- August 4 - Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million
$20,314,800

2016 year-to-date OCR settlements
OCR Enforcement Growth

OCR Settlement Amounts

- 2012: $6,000,000
- 2013: $2,000,000
- 2014: $6,000,000
- 2015: $6,000,000
- 2016: $24,000,000
2. A few case examples

What really happened
A manager left behind documents containing the PHI of 278 patients after moving out of her home she shared with her husband.
Pool & Land Physical Therapy

Posted pictures and full names of patients for testimonials on their website without approval.
BA laptop stolen

North Memorial
Raleigh Orthopaedic

Released x-ray films and related PHI of 17,300 patients to an entity to transfer the images to electronic media in exchange for harvesting the silver without a BAA.
Laptop stolen from ICU
UMMC visitor asked to use it and left.
3 Breaches in 3 months
Advocate Health

**Four desktop computers**
3,994,175 patients involved when they were stolen from the administrative office building

**Billing service breach**
2,027 patients involved when BA network hacked

**Stolen laptop**
2,237 patients involved when workforce member’s unlocked car had a laptop taken
3. Violations

What did OCR find missing in compliance
Violation - Lack of Risk Analysis

___________ failed to conduct an accurate and thorough risk analysis that incorporates all of its facilities, information technology equipment, applications and data systems utilizing ePHI.

(Or not Security policies at all)
We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI is secure.
Violation - No BAA = 2 violations

Lack of Business Associate Agreements as required by law.

Unauthorized disclosures to billing services, IT vendors, internet-based applications, online storage, etc because no Business Associate Agreement in place.
HIPAA’s obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise. It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.
Violation - Documentation

▷ No written policies and procedures.
▷ No written plans to address the *addressable* standards like encryption
▷ No written risk analysis and risk management plans
In addition to identifying risks and vulnerabilities to their ePHI, entities must also implement reasonable and appropriate safeguards to address them within an appropriate time frame.
4. Corrective Action Plans

This is the part no one talks about
What is a CAP?

1. Corrective Action Plans are part of settlements.
2. Specific provisions each entity must meet on a limited timeline.
3. OCR approves and monitors plans for the specified time frame.
2 year CAP - 5
North Memorial, ROC, NYPH, CHCS, Advocate

3 year CAP - 4
Pool, Feinstein, OHSU, UMMC

1 with no CAP
Lincare didn’t settle
We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI.
Examples of CAP provisions

**Conduct HIPAA Risk Analysis**

...submit the Risk Analysis to HHS – within ninety (90) days of the Effective Date – for HHS’ review, and either approval or disapproval.

**RA Approval Process**

HHS will respond within 60 days with a detailed, written explanation of its disapproval or approval of the Risk Analysis. Within 60-days make updates and re-submit.

**Implementation**

initiate implementation of security risk management activities under the plan no later than thirty (30) days following receipt of HHS's approval of the plan.

**Business Associates**

Within 120 days provide list of all BAs, copies of BAAs.
Within 60 days revise all policies to include responsibility for BA management and send to OCR for approval.

**Written Policies and Procedures**

Send to HHS for approval within 90 days of approval of risk management plan.

**Training**

Within 120 days of HHS approval provide security awareness and training program materials for HHS approval.
## Reporting requirements

### Implementation Reports
Progress reports on specific violation corrections.

### Reportable Events
Workforce member may have failed to comply if it is an event.

### Annual Reports
A summary of corrective actions taken and progress.
A summary of reportable events and their status.

---

### All Reports Include
An attestation signed by an owner or officer attesting that he or she has reviewed the Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.
Process continues for years

Year 1
Crunch time

Year 2
Review

Year 3
Proof
5. What does all this tell you?

Your take-aways for the day
From well-publicized large scale breaches and findings in their own risk analyses, OHSU had every opportunity to address security management processes that were insufficient.
This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously.
HIPAA is enforced

There are substantially more cases where OCR did not require entities to settle. But, they will apply the law when they don’t see effort.
Do a risk analysis

Do a real one, not a checklist or simple spreadsheet. Where is PHI, what are threats, risk levels, plans for dealing with risk, etc.
Write it down

You can’t just say you did things, you need to show you did things. Write everything down.
Manage your BAs

Get the BAAs signed and up to date. Don’t just let them “check the box” by signing it. Ask them about their compliance program.
Leadership

They have made it clear that the leadership should be paying attention. If you decide not to do this then write down your explanation.
Don’t let Plucky Muck You Up
Thanks!

Any questions?

You can find me at:
@KardonHIPAA or @HelpMeWithHIPAA
Donna@KardonCompliance

KardonCompliance.com
HelpMeWithHIPAA.com - new episodes every Friday
Credits

Special thanks to all the people who made and released these awesome resources for free:
▷ Presentation template by SlidesCarnival
▷ Photographs by Unsplash