Privacy & Information Security Annual Update

June 30, 2014
Agenda

Privacy

• Regulatory update
• Training and education

Information Security

• Resolution Agreement and Corrective Action Plan (CAP)
• Information Security program report
HIPAA Privacy and Information Security Program

YESTERDAY
- 2003 Privacy Rule
- 2005 Security Rule
- 2009 HITECH
- 2013 Omnibus

TODAY
- HIPAA audits
- Resolution Agreement
- Breach Notification
- Heightened security awareness

TOMORROW
- Increased enforcement
- More security
- More regulations
- More HIPAA audits
Basic Elements of a Privacy Program

- Controls
- Evaluate
- Monitor
- Enforce
- Consistent Corrective Action

Areas of Risk
- Policies
- Sanctions

Effective Communicated Enforced

Policies

Training
- Areas of Risk
- Policies
- Sanctions

Sanctions
- Enforce
- Consistent
- Corrective Action

Audit
- Controls
- Evaluate
- Monitor

Privacy and Information Security Briefing 2014
Health and Human Services
Office for Civil Rights (OCR)
Enforcement and Regulatory Update

In the News
Enforcement Highlights 2013

Continued focus on HIPAA Security Rule compliance

- Affinity Health Plan – over $1.2 million
  - ePHI left on photocopier drives
- Wellpoint - $1.7 million
  - Information accessible on web portal
- Idaho State University – $400,000
  - Disabled firewall exposed ePHI to breach
- Adult & Pediatric Dermatology – $150,000
  - Stolen unencrypted thumb drive; lacked risk analysis, and policies

Privacy

- Shasta Regional Medical Center – $275,000
  - Patient medical records shared with media

Total Settlements 2013
$3.725 million
Enforcement Highlights 2014

- **Parkview Health System, Inc. – June 23**
  - $800,000 and CAP for dumping boxes of medical records on a lawn

- **NewYork-Presbyterian Hospital and Columbia University – May 7**
  - NYP $3.3 million; CU $1.5 million monetary settlements and CAPs
  - More on this later

- **QCA – April 22**
  - $250,000 monetary settlement and CAP
  - Did not implement policies and procedures to prevent, detect, contain, and correct security violations of computer systems containing ePHI

- **Concentra – April 22**
  - $1.725 million monetary settlement and CAP
  - Failed to manage its laptops, identified lack of encryption of ePHI

- **Skagit County – March 7**
  - $215,000 monetary settlement and CAP
  - Provided access to ePHI on its public web server. No HIPAA Policies

Total Settlements
January – June 2014
$7.790 million
Enforcement

- Requires the OCR to formally investigate a complaint if a preliminary investigation of the facts of the complaint indicates a possible, not probable, violation due to willful neglect and to impose a civil money penalty for a violation due to willful neglect.

- Willful neglect determinations for enforcement purposes is founded upon evidence from OCRs investigations.
Definition of Willful Neglect

“The conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated”

i.e., failure to comply with the HIPAA/HITECH rules can be classified as willful neglect
## HIPAA Compliance / Enforcement

(as of December 31, 2013)

<table>
<thead>
<tr>
<th>Category</th>
<th>TOTAL (since 2003)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Filed</td>
<td>90,000</td>
</tr>
<tr>
<td>Cases Investigated</td>
<td>31,925</td>
</tr>
<tr>
<td>Cases with Corrective Action</td>
<td>22,026</td>
</tr>
<tr>
<td>Civil Monetary Penalties &amp; Resolution Agreements</td>
<td>$18.6 Million</td>
</tr>
</tbody>
</table>

The **single** NYP & CU Joint Resolution Agreement accounts for 25% of settlements since 2008
Compliance and Enforcement Audit – Lessons Learned

**Privacy**
- Notice of Privacy Practices
- Access of Individuals
- Minimum Necessary
- Authorizations

**Security**
- Risk Analysis
- Media Movement and Disposal
- Audit Controls and Monitoring
Issued: January 25, 2013
Effective Date: March 26, 2013
Compliance Date: September 23, 2013

HIPAA Omnibus Rule 2013
Omnibus Final Rule
HITECH/GINA/HIPAA

• HITECH Provisions:
  – Modified Breach Notification Rule
  – Business Associates
  – Marketing and sale of protected health information
  – Fundraising
  – Electronic Access
  – Right to request restrictions
  – Enforcement

• GINA Provisions:
  – Genetic information as PHI
  – No use for underwriting

• Other HIPAA Provisions:
  – Notice of Privacy Practices
  – Research authorizations
  – Student immunization records
  – Decedent information
Changes to the Breach Notification Rule

• Elimination of the harm threshold

• Definition of a breach modified to low probability that PHI has not been compromised

• Unauthorized acquisition, access, use or disclosure is presumed to be a reportable breach unless a risk assessment demonstrates a low probability that the PHI was compromised
Breach Notification

500+ Breaches by Type of Breach

- Theft: 48%
- Unauthorized Access/ Disclosure: 18%
- Loss: 11%
- Other: 10%
- Hacking/IT Incident: 7%
- Unknown: 1%
- Improper Disposal: 5%

Data as of February 2014
Breach Notification

500+ Breaches by Location of Breach

- Paper Records: 22%
- Desktop Computer: 14%
- Laptop: 23%
- Other: 10%
- Portable Electronic Device: 12%
- Network Server: 11%
- E-mail: 4%
- EMR: 4%

Data as of February 2014
Business Associates

• New definition of business associate
  – Creates, receives, maintains or transmits protected health information on behalf of a covered entity

• Business Associates now include:
  – Patient Safety Organizations (PSOs) and Health Information Exchanges (HIEs), E-prescribing gateways, Personal Health Records (PHRs) if the vendor provides services on behalf of CUMC

• Important for all departments/programs to identify/assess all disclosures of PHI to consider if it is a business associate.

• Guidance on the HIPAA webpage
HIPAA Privacy Program
What’s new?

- New Notice of Privacy Practices
- New policies and procedures
- New Business Associate Agreement
- New online training
- New/updated forms
- #encrypt for email
- Personal Health Record (PHR) - FollowMyHealth
  – All information available on the HIPAA website
Privacy & Security Training

• ~15,000 faculty, staff and students completed training in 2013

• Process in place to enroll new faculty, staff and students when UNI is created and affiliated with the medical center

• Will not get access to Library and RASCAL until complete
Privacy & Security Training

• FY 2013 - Online training and data attestation completed by faculty, staff and students
• FY 2014 - New / updated training will be released in August 2014
• All faculty, staff and students must complete training to meet CAP requirements
• [https://columbia.sighttraining.com/](https://columbia.sighttraining.com/)
Privacy & Security Training
(Sanctions)

For those individuals who fail to complete training in the time allotted:

- Access removed from RASCAL, Library resources, CROWN, AXIUM and IDX
- Progressive enforcement will occur
  - Letters to DA and HR placed in employee file
  - Notices to employee chair and dean
  - Suspension (staff) / non-renewal (faculty) / conduct process (students)
OCR YouTube Videos

http://www.youtube.com/user/USGovHHSOCR
HealthIT.gov Downloadable Materials

- Fact sheets
- Posters
- Brochures

http://www.healthit.gov/mobiledevices
We are here to help
INFORMATION SECURITY
New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million

$4.8M HIPAA Fine Part Of Wider HHS Crackdown

Server mishap results in largest HIPAA fine to date

Largest HIPAA Settlement for Breach of Information

New York Hospitals to Pay Record $4.8 Million for HIPAA Data Breach

In addition to the impermissible disclosure of ePHI on the internet, OCR’s investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.
Excerpt of news release from HHS issued on May 7, 2014

• “When entities participate in joint compliance arrangements, they share the burden of addressing the risks to protected health information,” said Christina Heide, Acting Deputy Director of Health Information Privacy for OCR. “Our cases against NYP and CU should remind health care organizations of the need to make data security central to how they manage their information systems.”

• The NewYork-Presbyterian Hospital resolution agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf

• The Columbia University resolution agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/columbia-university-resolution-agreement.pdf

• http://www.hhs.gov/news/press/2014pres/05/20140507b.html
Columbia University
Resolution Agreement

• CU Settlement Agreement of $1.5 Mil
• NYP Settlement Agreement of $3.3 Mil
• Findings
  – CU failed to conduct a thorough risk analysis
  – CU failed to implement security measures to reduce risk of inappropriate disclosure
• Agree to a Corrective Action Plan (CAP)
• Monitoring in place for 3 years
• Failure to abide could result in Civil Monetary Penalties (CMP)
Corrective Action Plan (CAP)

Columbia is required to improve in the following areas:

1. Risk analysis of all patient information
2. Access management to patient information
3. Management of patient information on computers and mobile devices
4. Controlling changes to systems with patient information
5. Training
6. Reporting policy violations to HHS
CAP (1)
Risk Analysis / Management

**HHS expectations:** “A complete and thorough risk analysis of ... all electronic equipment, data systems, and applications ...”

**CUMC expected deliverables:**

- **A full inventory of all workstations, servers, mobile devices, etc**
  - *We need your participation*
- **A strategic plan** that aligns risks of patient information to the obligations under the CAP
  - Plan to be implemented over the next year
- **New policies and procedures for the medical center**
- **A new breed of IT**
HHS expectations: “process ... for requesting authorization to access CU ePHI, obtaining approval of such request, documenting such request, and conducting periodic monitoring of ePHI usage”

CUMC expected deliverables:

• Updated policies and procedures
• Tighter controls, updated processes and more thorough tracking of all ePHI access for all workforce members
• Improved central monitoring of ePHI usage
CAP (3)  
Endpoint and Media Management

HHS expectations: “revise ... procedures related to the use of hardware and electronic media including [laptops, tablets, etc] [used for] CU ePHI. [Policies and procedures will include methods for] obtaining authorization for the use of personal devices”

CUMC expected deliverables:

• Better management of workstations, laptops, mobile devices, tablet, etc
• Approvals required for use of personal devices
• More approvals and tracking of the use of flash drives, dvd/cds, and external hard drives
CAP (4)
Change Management

HHS expectations: “CU shall develop a process to evaluate any environmental or operational changes that affect the security of CU ePHI.”

CUMC expected deliverables:

- New governance process for overseeing changes to production systems
- Oversight and approvals from ‘board of peers’ to make changes to ePHI technologies
  - This means changing configuration on your servers or server based applications requires approval by a ‘Change Advisory Board’
CAP (5)
Reportable Events

HHS expectations: “CU shall, upon receiving information that a workforce member may have failed to comply with ... policies ... investigate the matter. If ... workforce [member] has failed to comply with its... policies ... CU shall notify HHS in writing within 30 days.”

CUMC expected deliverables:
• Investigations of policy and procedure violations of ePHI
• Evaluation to compliance of CAP
• Report confirmed violations to HHS within 30 days
Status Report

- Governance and committee structures developed and/or updated
- KPMG (big 4 auditing firm) is conducting the risk analysis, penetration study and security program review
- Experis (consulting firm) hired to conduct backlog of systems assessments
  - Please work with Information Security to expedite this process
- Policy revisions completed
- Procedures drafted and under final evaluation by committees.
- Change management process developed
- Updated risk analysis strategies
- New privacy and security training modules in August 2014
Governance Updates

The following committees were charged with governing CAP strategy development:

- **Executive HIPAA Risk Committee**
  - Overall strategic direction and approval
  - Senior leadership of CUMC

- **Dean’s HIPAA Breach Committee**
  - Providing feasibility input from schools and research
  - Chairs selected by Dr. Goldman

- **NYP / CUMC Joint Workgroup**
  - Cross-institutional strategic alignment
  - IT Leadership of CUMC and NYP

- **Privacy & Security Workgroup**
  - Administrative feasibility of implementation
  - Admin and IT of 4 schools
CAP – Timelines

Effective May 2\textsuperscript{nd}

- 90 Days: Policies & Procedures
- 120 Days: Change Management
- 180 Days: Risk Analysis
- 270 Days: Risk Management
- 480 Days: Finish Implementation
- \sim 3 Years: Monitoring and Reporting
CAP – Final thoughts

• Under review for next 3 years
• Significant changes will occur
• Unplanned spending will occur

We will be a better place because of it!
Some good news

Significant improvements in the last year

• ~15,000 completed privacy and security training
• Thousands of people inventoried and encrypted their endpoints
  – Dozens of thefts/losses did not result in a breach
• New security protections implemented
  – Secure email - ~3,000 emails per month
  – Automated blocking of ePHI via email – prevents breaches

More automated and consistent security controls coming, making your life easier
Closing relevant thoughts

• Do not ever use personal email
• Do not use Cloud storage that has not been approved by Security or Privacy
  – Dropbox, Google, Skydrive, etc
• Use #encrypt on the subject line of a message to send sensitive data
• Only share ePHI with people who have a “need to know”
• encrypt Encrypt ENCRYPT!
• Register all information systems with the Information Security Office, regardless of whether they contain ePHI
  – https://rsam.cumc.columbia.edu
• Report any suspicious privacy or security incidents to hipaa@cumc.columbia.edu or security@cumc.columbia.edu
Erik Decker
Information Security
ed2513@cumc.columbia.edu
security@cumc.columbia.edu
(212) 305-4357

Karen Pagliaro-Meyer
Privacy Officer
kp155@cumc.columbia.edu
HIPAA@cumc.columbia.edu
(212) 305-7315

http://www.cumc.columbia.edu/hipaa/index.html
Health Insurance Portability & Accountability Act (HIPAA) Information

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") provides comprehensive guidance for patients including their privacy rights concerning the use or disclosure of their medical information. These rights are described in detail in the Notice of Privacy Practices.

Notice of Privacy Practices

- Notice of Privacy Practices (NPP)
  - Notice of Privacy Practices (Spanish)
- Patient Acknowledgement Form
  - Patient Acknowledgement Form (Spanish)

HIPAA Forms

- Authorization to Release Medical Information (Legal)
- Authorization to Release Medical Information (Legal) (Spanish)
- Business Associate Agreement
- Confidentiality Agreement
- HIPAA Fax cover sheet
- Important Information About Patient Email
- Patient Request for Email Communications

Patients - HIPAA Rights

- Request a Copy of your Medical Record
  - Request a Copy of your Medical Record (Spanish)
- Request an Accounting of Disclosures
- Request an Amendment to Health Information

Training

All CUMC faculty, staff and students must complete mandatory HIPAA training.

- On-line HIPAA Training
  - For any questions regarding training, please email HIPAA@columbia.edu.

- Researchers
  - Researchers must complete an additional HIPAA training course on RASCAL under the Testing Center.

HIPAA Education Material

- HIPAA &HITECH Briefing - Privacy and Information Security 2013
- HIPAA &HITECH Briefing Information Security and Privacy 2013 - Video (UNI required)
- Welcome Program 2013
- HIPAA and Electronic Medical Record Access - Students
- HITECH Email Breach Notification Requirement
- Social Security Number Protection Act
- Privacy Walk Through
- Student Health Services 2012