Agenda

Privacy / HIPAA
  • New Omnibus Regulations
    Review of regulatory requirements
    Report of Breach statistics
    Plan to comply with requirements
  • Training and Education

Information Security
  • Risk Management
  • Security Governance
  • Security Operations
  • Training
HIPAA OVERVIEW

Health Insurance Portability and Accountability Act (HIPAA)

Administrative Simplification
[Accountability]

Transactions, Code Sets, & Identifiers
Compliance Date: 10/16/2002 and 10/16/03

Privacy
Compliance Date: 4/14/2003

Security
Compliance Date: 4/20/2005

Insurance Reform [Portability]

Insurance

Fraud and Abuse (Accountability)

HITECH
Health Information Technology for Economic and Clinical Health 9/18/2009

OMNIBUS 9/2013
Omnibus Rule 2013

Issued: January 25, 2013
Effective Date: March 26, 2013
Compliance Date: September 23, 2013
Summary of Omnibus Modifications

• Breach Notification Rule
• Business Associates
• Enforcement
• New Patient Rights
  – Electronic Access to PHI
  – Right to limit disclosure for services paid out of pocket
  – Uses & Disclosures of Protected Health Information
    - Fundraising, Marketing & Sale of PHI
• Research Authorizations
• GINA – Genetic Testing
Summary of Omnibus Modifications

• Decedent Information
  – Information is no longer PHI after 50 years.
  – NYSDOH Preemption analysis required

• Student Immunizations
  – May disclose proof of immunization of child to schools with oral agreement of parent
  – NYSDOH Preemption analysis required
HITECH Act (ARRA) Breach Notification Rule

• New Federal Breach Notification Law – Effective Sept 2009
  • Applies to all electronic “unsecured Protected Health Information” - “encryption required”
  • Requires immediate (60 days) notification to the Federal Government if more than 500 individuals effected
  • Annual notification if less that 500 individuals
  • Requires notification to patients & appropriate remediation
  • May Require notification to a major media outlet and listing on organizations website
Changes to the Breach Notification Rule

• Elimination of the *harm threshold*

• Definition of a breach modified to *low probability that PHI has 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 Highlights
September 2009 through April 15, 2013

- 571 reports involving over 500 individuals
- Over 79,000 reports involving under 500 individuals
- Top types of large breaches
  - Theft
  - Unauthorized Access/Disclosure
  - Loss
- Top locations for large breaches
  - Laptops
  - Paper records
  - Desktop Computers
  - Portable Electronic Device
Breach Notification:
500+ Breaches by Location of Breach

- Laptop: 23%
- Paper Records: 22%
- Desktop Computer: 15%
- Portable Electronic Device: 14%
- EMR: 2%
- Network Server: 11%
- Other: 10%
- E-mail: 2%
Breach Notification:
500+ Breaches by Type of Breach

- Theft: 52%
- Unauthorized Access/Disclosure: 20%
- Loss: 13%
- Improper Disposal: 5%
- Unknown: 2%
- Hacking/IT Incident: 8%
# A Decade of HIPAA Enforcement
(As of March 31, 2013)

<table>
<thead>
<tr>
<th></th>
<th>TOTAL (since 2003)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Filed</td>
<td>79,920</td>
</tr>
<tr>
<td>Cases Investigated</td>
<td>28,480</td>
</tr>
<tr>
<td>Cases with Corrective Action</td>
<td>19,306</td>
</tr>
<tr>
<td>Civil Monetary Penalties &amp; Resolution Agreements (since 2008)</td>
<td>$14.9 million</td>
</tr>
</tbody>
</table>
OCR Enforcement Results

• Order of frequency of investigations
  – Impermissible use or disclosure of PHI
  – Lack of safeguards of PHI
  – Lack of patient access to their PHI
  – Uses/disclosures of more than minimum necessary PHI
  – Lack of administrative safeguards of ePHI

• OCR referred 516 cases for criminal investigations to Department of Justice
Major Enforcement Actions 2012

• BCBS Tennessee fined $1.5M
  – *Stolen server*

• Phoenix Cardiac Surgery fined $100K
  – *EPHI disclosed via internet by a third party application hosted in the cloud*

• Alaska DHHS fined $1.7M
  – *Portable device stolen from vehicle*

• Mass Eye and Ear Institute fined $1.5M
  – *Personal device stolen from physician office*

• Hospice of Northern Idaho $50K
  – *Laptop stolen, no risk assessment*
“I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates.”
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:
  - PSOs (Patient Safety Organization’s), HIOs (HIE, RHIO)
    E-prescribing gateways, PHR vendors that provide services on behalf of a CUMC

BA is **directly liable** under the Privacy Rule for uses and disclosures of PHI that are not in accord with its business associate agreement (BAA) or the Privacy Rule
Examples of Business Associates

• Billing, collection, coding or claims processing companies

• Software Support / Data Administration (electronic applications with access to PHI)
  – examples include: CROWN, GE, Siemens & IDX

• Data analysis / processing – e.g. research

• Quality Assurance & Customer Satisfaction Services

• Medical record/information storage/destruction companies

• Consultants – business, financial, medical etc.
New Business Associate Requirements

• New Business Associate Agreement developed and posted on the HIPAA website.

• All new Business associates must sign the agreement issued April 2013

• New BAA needed for any active vendor with a BAA executed before Sept 2010

• Essential that business associates are identified and execute CUMC BAA
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.

- In general, Omnibus strengthens enforcement, especially in regards to willful neglect by adopting previously issued privacy and security rules.

- The tiered penalty structure remains in place.

- ‘Willful neglect’ determinations for enforcement purposes is founded upon evidence from OCRs investigations of the allegation(s).
# New Penalties

<table>
<thead>
<tr>
<th>Tiers</th>
<th>Description</th>
<th>Minimum per Violation</th>
<th>Maximum per Year (for identical violations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier A</td>
<td>“Did not know”</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier B</td>
<td>“Reasonable cause – not willful neglect”</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier C</td>
<td>“Willful neglect” corrected w/in 30 days</td>
<td>$10,000 - 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier D</td>
<td>“Willful neglect - uncorrected”</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

So, a breach involving PHI for 10 individuals could cost **you** anywhere from $100 to $50,000 per name.
Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

About this notice

This Notice will tell you about the ways we may use and disclose health information that identifies you (“Health Information”). We also describe your rights and certain obligations we have regarding the use and disclosure of Health Information. We are required by law to maintain the privacy of Health Information that identifies you; give you this Notice of our legal duties and privacy practices with respect to your Health Information; and follow the terms of our Notice that are currently in effect. This Notice covers the faculty practice. To the extent that we are covered by another health care provider’s Notice, that other provider’s Notice governs. Changes to our Notice of Privacy Practices will be effective for all Health Information that we create or receive on or after the effective date of the changes. We reserve the right to make changes to this Notice, but any such changes will be effective only for Health Information we collect after the notice change is made. We will abide by the Notice currently in effect.

How we may use and disclose health information about you

The following categories describe different ways that we may use and disclose Health Information.

For Treatment
We may use Health Information about you to provide you with medical treatment or services. We may disclose Health Information to doctors, nurses, technicians, medical students, or other personnel who are involved in taking care of you. We may also disclose Health Information to our staff for administrative and financial activities that are not part of direct treatment of care. For example, we may use your Health Information to bill you and to bear the costs of the services that we provide to you.

For Payment
We may use Health Information that we create or receive for billing and other payment purposes. We may provide your Health Information to your health insurance plan to obtain payment for the services that you receive from us. We may also bill you for the services that you receive from us. We may use or disclose your Health Information to another party to obtain payment from you or from your health insurance plan on your behalf. We may not sell or lease your Health Information.

For Fundraising
We may use Health Information for fundraising purposes. We may use or disclose Health Information to raise funds for our health care provider for activities that may or may not be related to health care, for example, to provide free health care services.

For Research
We may use or disclose Health Information to researchers conducting certain research. An example of research is the study for the development of new treatments. We may use Health Information to conduct research when we receive written authorization from you or your legal representative, when we are involved in a court or administrative proceeding, or when a research organization has obtained a written authorization from you or your legal representative.

How we may disclose health information

We may disclose Health Information to a third party when you give us written authorization in a form that complies with the Health Insurance Portability and Accountability Act of 1996. The person to whom we disclose Health Information has agreed to maintain the confidentiality of the Health Information.

To the extent that we are covered by another health care provider’s Notice, that other provider’s Notice governs.
New Patient Rights

• Electronic Access to medical information
  – Must provide patient with electronic copy of medical record when using electronic medical record

• Right to request restrictions
  – New right to restrict disclosures to a health plan when patient has paid in full out of pocket

• Right to control PHI use for marketing, sales and fundraising

• Right to be notified of a privacy breach
Fundraising / Development

• Adds categories of PHI used for fundraising
  – Department, physician, health insurance status

• Strengthens opt-out for fundraising
  – Statement must be clear and conspicuous, no undue burden to opt-out
  – Covered entity **MUST NOT** make fundraising communications after an individual has opted out regulation previously stated “reasonable effort”
Fundraising/Development Plan

• Modify existing HIPAA Fundraising policy

• Refine procedure to track opt outs of fundraising

• Modify language in the Notice of Privacy Practices

• Educate Development Staff

• Implementation – September 2013
Marketing

• Communication about health-related products/services to an individual require authorization if paid for by a third party
  – A device manufacturer cannot pay for marketing of that device to patients without their authorization

• Applies to receipt of financial remuneration only; does not include receipt of non-financial benefits

• There continues to be a stand-alone exception for prescription refill reminders and certain drugs and biologics.
Sale of PHI

• Entity may not receive remuneration in exchange for PHI

• Sale of PHI occurs if a covered entity “primarily is being compensated to supply data it maintains in its role as a covered entity”.

• If authorization is obtained, authorization must state that disclosure will result in remuneration

• HHS will issue additional guidance on this topic in the future
Research & GINA

• Compound Authorization
  – Single authorization form permitted for use/disclosure of PHI for conditioned and unconditioned research activities

• Future Use Authorization
  – Permitted if authorization has adequate description such that it would be reasonable for the individual to expect his/her PHI could be used for the research

• Genetic information is PHI
• Does not impact provider use of genetic information for treatment purposes
• Prohibits use or disclosure for underwriting purposes by health plans
Workforce Training & Education

- New Privacy and Information Security on-line training program developed

  - Emails will be sent out in July
    - all current staff & faculty to complete the training

- All new faculty & staff compete HIPAA training on-line
  - includes Privacy & IT modules
  - track staff completion
  - produce reminders, reports etc.
Download Materials

www.healthit.gov/mobiledevices

- Fact sheets
- Posters
- Brochures

Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT and SECURE Health Information.

Be a team player. Understand and follow your organization’s mobile device policy and procedures. It's your responsibility.
Visit HealthIT.gov/mobiledevices
Consumer Videos

Your Health Information, Your Rights
28,414 Views

Su Informacion de Salud, Sus Derechos
78,409 Views

The Right to Access Your Health Information
16,466 Views

Treatment, Payment and Health Care Operations
12,499 Views

EHRs: Privacy and Security
2,065 Views

Communicating with Friends and Family
12,905 Views

Explaining the Notice of Privacy Practices
16,414 Views

HIPAA Security Rule
80,495 Views

TOTAL VIEWS FROM FEBRUARY 16 2012 - MAY 1, 2013: 240,788

Visit us at http://www.youtube.com/USGovHHSOCR
The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.

Securing Your Mobile Device is Important!

Dr. Anderson's Office Identifies a Risk

A Mobile Device is Stolen

Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?

Worried About Using a Mobile Device for Work? Here's What To Do!
Information Security
Information Security Program at CUMC

• Significant positive progress in last 2 years
• Increased vigilance by users
• Procedures leading to robust implementations of secured data and information
• Reducing risks to patients, employees, departments and the institution
• Changing the culture towards more secure environment
Challenges, old and new

- More policing, more penalties, more regulations, OCR-style – initiated the HIPAA Audit program and Omnibus
- Increase in healthcare data breaches – fines are significant
- Tremendous use of mobile devices in healthcare – New technologies, new threats, bring new risks
- Greater patient awareness – patient engagement and satisfaction are important for tomorrow’s care
- More data, more sharing of data, more data on the cloud – changing IT management models
Security Activities

• Risk management
  – Analyze and quantify risks on information assets, risk classification and register, and non-technical mitigation strategies, threat and vulnerability analysis

• Security Governance
  – Policy development and management, security responsibilities, procedural impact evaluation, sanctions, coordination with partners (CU, NYP, etc.), legal and institutional frameworks, liability management, internal and external audits

• Security Operations
  – Safeguard data, technical threat and vulnerability monitoring, detection and prevention of malicious behavior, protect against data leakage, asset classification, identity management, authentication, authorization, audit logs, encryption, security event management, security analytics, incident handling

• Awareness
  – Training and just-in-time education, economics of identity fraud, strategies to handle spam and malware, passwords and encryption, systems and application security configuration, secure application development, communication and updates
Risk management

CUMC Risk Management Program

- Pre-implementation: Acquisition Analysis Complete
- Started: Analysis has commenced; questionnaire delivered to custodian
- To Be Issued: Report to be completed and or released by Information Security
- Issued: Report has been released
- Remediation Escalated: Remediation has been escalated to senior management
- Remediation in Progress: Risk Mitigation plan accepted and/or activities have commenced
- Passed / Remediated: Remediation was completed or was not required
- Decommissioned: Application has been removed from service (post analysis) as a risk mitigation strategy
- Dropped: Applications thought to require certification but which do not
- To Be Started: Application risk analyses have not commenced
Risk management highlights

• Risk analysis of applications and systems
  – Standards and frameworks: ISO, NIST, PCIDSS, COBIT, HiTRUST

• Pre-implementation security posture analysis
  – Ask us to take a quick look before you decide to buy the system or service

• Application-in-the-cloud (3rd party) risk analysis
  – Different set of questions

• Site certification
  – Clinical practice acquisition along with information system assets
  – 4 sites have been certified, 39 are being evaluated or triaged

• Research
  – IRB data security policy and risk analysis of sensitive systems, modified set of questions
Security governance

• Questions addressed by Security governance:
  – How do we make decisions regarding information security priorities? How do we coordinate activities?
  – How is senior management informed about risks?
  – How are authority, responsibility and accountability determined?
  – How do we ensure that security strategies are aligned with business objectives and applicable regulations?

• A critical component of OCR Audit which requires a risk governance structure
Governance groups

- CUMC Information Security Risk Management committee
  - Members include CUMC senior management and Legal
  - Quarterly meetings starting in 2012, reports from Privacy and Security
  - Enterprise view of risks (listed in a Risk Register)
  - Deliberation topics: Policies, Breaches, Endpoint and email vulnerabilities, Data Leakage Prevention, Training

- CU Information Technology Security Council
  - Representatives of security personnel of all schools in CU
  - Advisory to CU Information Technology Leadership Committee

- Information Security Policy Task Force
  - Members of CU Security, CUMC Security, Research, Legal
  - Working to reconcile info sec policies’ content, definitions, and language
  - Converting 35+ policies into about 15 policies

- Quarterly CUMC Privacy and Security Workgroup meeting
  - Members representing CUMC schools and IRB
  - Reports from Privacy and Security

- Quarterly Tri-institutional Privacy and Security meeting
  - Privacy and security officers of NYP, Cornell and Columbia
Security operations

• Layered security controls
• Monitor suspicious bot activities
• Vulnerability scan
• Managing authentication and audit log service for central clinical applications such as CROWN
• Implementing Data Leakage Prevention (DLP) solution
• Securing Email with encryption
• Desktop and mobile device encryption

Endpoint Security Campaign
Layered Security Controls

- Remote workstations
- Desktops, Laptops, Mobile
- Medical devices
- Servers

IDS/IPS – IBM ISS
Firewall - Cisco

Netflow – Arbor

AntiVirus – Symantec

Patching – Microsoft, Apple

Security Event Management – Arcsight

Email encryption – Proofpoint

Vulnerability Scanning – Nexpose, Nessus, Accunetix

Proxy Server – Bluecoat

Encryption – Symantec, Microsoft Bitlocker, Apple

Network Access Control – Aruba, Bradford, VPN

Data Loss Prevention – Symantec

New tools under implementation/evaluation

- Advanced Persistent Threat detection/prevention
- Next Generation Firewalls
- Wireless security - Aruba
- Server tampering - Tripwire
Endpoint Security Campaign

Recap of policy updates

• **Workstation Use Policy**
  – All workstations that contain PHI or PII must be encrypted

• **Backup/Mobile storage devices**
  – All removable media that contain PHI or PII must be encrypted

• **HIPAA Sanctions policy**
  – Departments may be fined for any loss of PHI or PII

• **Email policy**
  – All CUMC email services will be consolidated into the centrally managed CUMC Exchange email system
Endpoint Security Campaign

- Over 1,900 encrypted USB drives have been distributed as part of the USB Swap program
- USB swap program is still on-going
- Over 2,500 laptops and mobile devices were brought to the CUMC IT service desk for encryption
- Working with departments to certify their endpoint environment for encryption
Endpoint Security Campaign

• We are on the right track!

• 5+ endpoint devices were lost in past year, and in every case, the device was found to be encrypted, requiring no breach notification

• The program has already saved CUMC’s bacon, as stated by Dr. Goldman in P&S State of the School address yesterday!
Endpoint Security Campaign

- Email encryption is now available for all CUMC IT email users!
  - *As easy as putting #encrypt in subject header*
Endpoint Security Campaign

• Emails which are identified as containing sensitive data and do not have #encrypt in Subject header – are blocked
New program: monitor vulnerabilities

- Vulnerability scanner scans all systems (112) that have been opened in the Firewall
Security Training

• Recently concluded a System administrator training
  – “All about hacking”
  – Over 50 departmental system administrators
  – Professional, hands-on training for 2 days
  – Well liked and appreciated!

• The course will be repeated in September

• Training on new security topics will be made available
Security Training

• New Privacy and Information Security on-line training starts in July
• All current staff and faculty to complete the training courses
• Security material are primarily general security material
• Non-completion may mean loss of access to clinical and research PHI systems in CUMC and NYP
Mobile Devices: Tips to Protect and Secure Health Information

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate wiping and/or remote disabling.
- Disable and do not install file-sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of your mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.
Encryption of endpoint devices

• Laptops
  – Microsoft bitlocker
  – Apple filevault
  – Truecrypt
  – Regardless of PHI

• Desktops
  – If it stores PHI, must be encrypted

• Mobile Phones
  – Password protected
  – Encrypted
  – Remote wipe capable

• Flash drives
  – Purchase a flash drive that is already encrypted

➤ Strong passwords
➤ Appropriate timeout
Encryption

• Kingston hardware encrypted USB drives cost $12.  
 http://www.cumc.columbia.edu/it/howto/encrypt/swap.html

• Encrypted USB drives are safer than data on unencrypted desktops

• **There should be NO excuse for unencrypted storage of PHI**

• Information on encryption appears in  
 http://secure.cumc.columbia.edu/cumcit/secure/policy/encrypt.html
# CUMC Information Security Office

**Erik Decker**  
Assistant Director - CISSP, ENCE, GSEC, GPEN  
(212) 342-0268  
ed2513@columbia.edu

<table>
<thead>
<tr>
<th>Lisa Mui</th>
<th>Rajneel Dhotre</th>
<th>Miguel Delgado</th>
<th>Michael Jemmott</th>
</tr>
</thead>
</table>
| InfoSec Risk Manager  
(212) 305-5056  
lm2906@columbia.edu | InfoSec Manager  
(212) 305-5705  
rd2612@columbia.edu | InfoSec Analyst  
(212) 305-3734  
mad2223@columbia.edu | InfoSec Analyst  
(212) 305-0006  
mj2573@columbia.edu |

| William Li  
IT Risk Analyst  
(212) 305-2665  
william.li@columbia.edu | Achebe Sam  
IT Risk Analyst  
(212) 305-1924  
as4281@columbia.edu | Michael Meyer  
IT Risk Analyst  
(212) 305-6397  
mm4319@columbia.edu | Intern |

security@mail.cumc.columbia.edu
Soumitra Sengupta, PhD
Information Security Officer
sen@columbia.edu
security@mail.cumc.columbia.edu
(212) 305-7035

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