Katherine Downing, MA, RHIA, CHPS, PMP
Vice President AHIMA Information Governance and IGAdvisors™ Consulting

One in Two Out:
Impact of Trump Administration on HIPAA Privacy and Security
Introductions and Welcome!

KATHERINE DOWNING is the Vice President for IGAdvisors® focused on Information Governance, Privacy, Security, Compliance, and the Electronic Health Record. She has over 20 years of experience in healthcare leadership and consulting, and an extensive background in planning and directing cross-functional business operations and technology projects. She is an analytical, fast-thinker who effectively partners with organizations to assess opportunities, facilitate strategic decisions, and lead successful implementations.

Business development and strategic consultancy: Ms. Downing’s project management experience plus her ability to assess complex situations and identify appropriate solutions give her a unique ability to gain meaningful insights into an organization’s information governance needs. She is particularly skilled at group facilitation and enjoys forging consensus among people with diverging ideas and opinions.

Katherine Downing, MA, RHIA, CHP, PMP
Vice President IGAdvisors®
E-mail: kathy.downing@ahima.org
Phone: (312) 233-1900
## Agenda

<table>
<thead>
<tr>
<th>Part</th>
<th>IG Topic Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part I</td>
<td>Current state of Privacy and Security</td>
</tr>
<tr>
<td>Part II</td>
<td>21\textsuperscript{st} Century Cures Act Impacts on Health IT</td>
</tr>
<tr>
<td>Part III</td>
<td>NPRM’s forthcoming</td>
</tr>
<tr>
<td>Part IV</td>
<td>Summary / Open Discussion</td>
</tr>
</tbody>
</table>
Aetna Agrees To Pay $17 Million In HIV Privacy Breach

Aetna settled a lawsuit for $17 million Wednesday over a data breach that happened in the summer of 2017. The privacy of as many as 12,000 people insured by Aetna was compromised in a very low-tech way: the fact that they had been taking HIV drugs was revealed through the clear window of the envelope.
News

Nuance says NotPetya attack led to $92 million in lost revenue

Recent SEC filings disclose losses, and predicts additional spend in 2018 for security enhancements and upgrades

Nuance Communications, a software company that offers speech and imaging technology to a number of markets, including healthcare and finance, said the 2017 NotPetya malware attacks caused the company to lose $92 million in revenue, and that number is expected to grow as they push forward into 2018.
One Year of OCR Enforcement

HIPAA Enforcement since April 2017

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/12/2017</td>
<td>Metro Community Provider Network</td>
<td>$400,000</td>
</tr>
<tr>
<td>4/21/2017</td>
<td>Center for Children's Digestive Health</td>
<td>$31,000</td>
</tr>
<tr>
<td>4/21/2017</td>
<td>CardioNet</td>
<td>$2,500,000</td>
</tr>
<tr>
<td>5/10/2017</td>
<td>Memorial Hermann Health System</td>
<td>$2,400,000</td>
</tr>
<tr>
<td>5/23/2017</td>
<td>St. Luke's-Roosevelt Hospital Center</td>
<td>$387,200</td>
</tr>
<tr>
<td>12/28/2017</td>
<td>21st Century Oncology</td>
<td>$2,300,000</td>
</tr>
<tr>
<td>2/1/2018</td>
<td>Fresenius Medical Care North America</td>
<td>$3,500,000</td>
</tr>
<tr>
<td>2/13/2018</td>
<td>FileFax</td>
<td>$100,000</td>
</tr>
</tbody>
</table>

Total $11,618,200
CMP’s through 2017

HIPAA Resolution Agreements and Civil Monetary Penalties

50 settlement agreements and 3 civil money penalties through 2017
OCR Enforcement Efforts

HIPAA Enforcement Highlights
April 14, 2003 – January 31, 2018

• Over 173,426 HIPAA complaints received to date
• Over 25,695 HIPAA cases resolved with corrective action and/or technical assistance
• Expect to receive over 24,000 HIPAA complaints this year
OCR Enforcement Efforts

HIPAA Enforcement Highlights
April 14, 2003 – January 31, 2018

- Over 173,426 HIPAA complaints received to date
- Over 25,695 HIPAA cases resolved with corrective action and/or technical assistance
- Expect to receive over 24,000 HIPAA complaints this year
HIPAA Breach Summary

Latest Breach Reporting Highlights

September 2009 through January 31, 2018

- Over 2,200 reports involving a breach of PHI affecting 500 or more individuals
- Type:
  - Theft makes up 38% of large breaches
  - Hacking/IT now accounts for 19% of incidents
- Location:
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
- Individuals affected are approximately 177,065,101
- Over 316,000 reports of breaches of PHI affecting fewer than 500 individuals
HIPAA Breach Summary

500+ Breaches by Type of Breach from September 2009 through January 31, 2018

- Theft: 38%
- Unauthorized Access/Disclosure: 27%
- Loss: 8%
- Hacking/IT: 19%
- Other: 4%
- Improper Disposal: 3%
- Unknown: 1%
HIPAA Breach Summary

500+ Breaches by Location of Breach from September 2009 through January 31, 2018

- EMR: 6%
- Email: 11%
- Network Server: 17%
- Laptop: 16%
- Portable Electronic Device: 9%
- Desktop Computer: 10%
- Paper Records: 21%
- Other: 10%
Consumer Effects of Breach

Healthcare Data Breaches Among U.S. Consumers

1 in 4
Consumers had their healthcare data stolen

1 in 2
Breaches resulted in identity theft

FROM THESE LOCATIONS:

Hospitals
Pharmacy
Urgent Clinic

Highest percentage of breaches occurred

OUTCOME FOR VICTIMS:

$2.5K
in average out-of-pocket costs per incident

STOLEN DATA USED TO:

37%
Purchase items

35%
Fraudulently bill for care

26%
Fraudulently receive care

26%
Fraudulently fill prescriptions

12%
Access/modify health records

Source: Accenture Survey, 2017
21st Century Cures Act
Audience Poll – How familiar are you with the 21st Century Cures Act

1. Very familiar. Our organization is working toward understanding and compliance.
2. Somewhat familiar, realize there are impacts forthcoming.
3. Never heard of it!
21st Century Cures Act

- Signed into law December 13, 2016 under Obama administration
- Authorizes 6.3 billion package

- Significant Health IT provisions
21st Century Cures Act

- Key HIT provisions of the Cures legislation:
  1. Require the Secretary to establish a strategy to reduce administrative and regulatory burdens associated with providers’ use of electronic health records (EHRs).
    - Must include MU, MIPS, APMs, certification, standards.
  2. Seek to advance interoperability and curb information blocking.
    - By promoting new reporting measures on usability, security, and functionality for EHRs and other HIT and require adherence for certification.
    - By establishing a new HIT Advisory Committee with broad duties and responsibilities.
    - By supporting a development of a new trust framework and agreement for networks.
    - By seeking to improve patient care and access to health information in EHRs.
    - By requiring the establishment of a new digital contact index, e.g. a directory, for health care professionals, practices, and facilities.
    - By ensuring adequate patient matching to protect privacy and security.
21st Century Cures Act (Section 3010)

- Ensuring interoperability of HIT
- Criteria
  - Secure transfer
  - Complete Access to health information
  - No information blocking
- Categories for interoperability standards
  - Vocabulary
  - Content
  - Transfer
  - Security
  - Services
Information Blocking Defined in Cures

• A practice, except as required by law, that:
  – Is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information
  – If conducted by an HIT developer, exchange or network, such entity knows or should know that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of health information.
  – If conducted by a healthcare provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of eHI
Information Blocking Penalties

- New CMP’s of up to 1 million per information blocking violation...
Reducing HIPAA Burdens
The Answer is YES!
Possible HIPAA Reductions

Proposed Changes to HIPAA Privacy and Enforcement Rules

• NPRM on Presumption of Good Faith of Health Care Providers

• NPRM on Changing Requirement to Obtain Acknowledgment of Receipt of Notice of Privacy Practices

• Request for Information on Distribution of a Percentage of Civil Monetary Penalties or Monetary Settlements to Harmed Individuals
Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encryption
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
OCR Guidance Efforts

New OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions
- New Materials for Professionals and Consumers
  - Fact Sheets for patients, families, and health care providers
  - Information-sharing Decision Charts
OCR Guidance Efforts

- Disclosures are permitted without the patient’s authorization or permission to law enforcement, family, friends or others who are in a position to lessen the threatened harm—when disclosure “is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others.”

- Disclosures must be consistent with applicable law.
OCR Efforts

Future HIPAA Guidance

- Texting
- Social Media
- Encryption
Information Governance – Beyond PHI

• IG is an enterprise wide effort to protect ALL information and access points, not just clinical information.

• Getting Started with IG Practical Examples:

  1. Information Asset Inventory
     • Enterprise wide understanding of access
     • Data and Information Stewards
     • Data Owners

  2. Information Classification

  3. Data and Information Inventory
AHIMA’s Information Governance Adoption Model Competencies (IGAM)™
IG Executive Training Video
IG BRAND SPONSOR AND SUPPORTER PROGRAM

Thank you to our IG Brand Partner and Supporters. With your help we will be able to increase the implementation of IGHealthRate™ in an effort to grow the adoption of IG across the healthcare ecosystem.

BRAND PARTNER

SUPPORTERS

Interested in learning more about becoming a Supporter or Brand Sponsor? Contact us at IGAdvisors@ahima.org for details.
You don’t need a crystal ball to see where the healthcare industry is going. What you need is the

**Privacy, Cybersecurity, and Information Governance Institute**

**SEPTEMBER 22-23, 2018 | MIAMI, FL**

AHIMA celebrates the Privacy and Security Institute’s 12th anniversary with a name change to match the evolutionary changes in the industry. In 2018, this meeting will be called the Privacy, Cybersecurity, and Information Governance Institute. Watch ahima.org for more details!

Mark Your Calendars.
REGISTRATION OPENS MAY 2018!
IGIQ.com is your ONE STOP for all Tools and Resources for Information Governance
2018 Privacy and Security Meetings

MARK YOUR CALENDARS

**Webinars**

- **Apr. 17** Compliance in a Connected World: A Guide to Engaging with Patients Online
- **June 19** How to Avoid Unwanted Hackers and Ramp Up System Security
- **July 24** Cybersecurity, Cyber-Insurance, and Human Resources Issues in Cyberspace
- **Aug. 21** I Want PHI and I Want it Now! Patient Access Versus Authorization
- **Nov. 27** Cybersecurity for Executives, Directors, Privacy Officers, and Senior Managers—What They Didn’t Teach You in the MBA Program
- **Dec. 11** Identity and Cloud Computing Security—The Azure Cloud Example

**SAVE THE DATE**

Privacy, Cybersecurity, and Information Governance Institute
September 22–23 | Las Vegas, NV
REGISTRATION OPENS IN MAY

Watch your e-mail and ahima.org/events for updates.

**Live Meeting**

Privacy and Security Training with CHPS Exam Prep Workshop
December 6–7 | Las Vegas, NV

Register for meetings at ahimastore.org.

* On-demand option is available for all webinars.
The First Step on Your Path to Information Governance.

Request a demo at IGHealthRate.com.
What’s Next? Move Your Organization’s IG Forward.

- IG consulting and implementation services (project management)
- Analysis and assessment
- On-site or virtual organization-specific training
- Score validation from the IGHealthRate™ system for IGAM Level 4 or 5 sites
- Identify your organization’s true level of IG maturity
- Differentiate your organization from its competition and other organizations
- Validate your organization’s maturity level
- Receive extensive reporting, guidance, and comparison to other entities of your size and specialty

For more information contact us at (844) 554-4447 or visit IGIQ.org.