Privacy Officer Roundtable - Best Practices and Lessons Learned from the Front Line

HIPAA Summit
March 27, 2018
Agenda

I. Introductions

II. Trends in HIT and Health Privacy & Security

III. Privacy Officer Roundtable – Lessons Learned from the Front Line

IV. Questions
I. Panel Introductions
## I. Panel Introductions

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Title &amp; Institution</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Column</td>
<td>Jana Aagaard, MA, JD</td>
<td>Senior Counsel, Privacy/Health IT, Dignity Health, Sacramento, CA</td>
<td>Sacramento, CA</td>
</tr>
<tr>
<td>2nd Column</td>
<td>Shauna Van Dongen, JD, CIPP</td>
<td>Chief Privacy Officer, Providence/ St. Joseph Health, Seattle, WA</td>
<td>Seattle, WA</td>
</tr>
<tr>
<td>3rd Column</td>
<td>Joyce Musante</td>
<td>Head of Privacy Officers, Legal Business Groups, Phillips, Murrysville, PA</td>
<td>PA</td>
</tr>
<tr>
<td>5th Column</td>
<td>Kimarie R. Stratos, JD</td>
<td>Senior Vice President and General Counsel/Chief Privacy Officer, Memorial Healthcare System, Hollywood, FL</td>
<td>Hollywood, FL</td>
</tr>
<tr>
<td>6th Column</td>
<td>Jim Koenig, JD CIPP/US</td>
<td>Partner and Co-Chair, Privacy &amp; Cybersecurity Practice, Fenwick &amp; West LLP</td>
<td></td>
</tr>
</tbody>
</table>
II. Trends in HIT and Health Privacy & Security
Trend 1 - Revolution in HIT and Healthcare Delivery Models

- **Health Information, IT and Sharing Revolutions.** Healthcare being conducted globally. Stimulus Bill provided funds driving HIT and analytics, but organizations went from 0 to 11 in IT maturity.

- **Care without Walls.** Healthcare using new channels and technologies to deliver treatments – i.e. specialty pharma, telemedicine, Internet of Things/addressable medical devices, social media, care without walls.

- **New, but Vulnerable, Healthcare Ecosystem.** All the new data sharing and movement of data creates new capabilities and new data vulnerabilities.

- **More Third Parties Needed to Enable/Support.** New business partners, business associates and independent contractors needed to deliver and host new healthcare delivery methods/technology.

- **New Cyber Threats Attacking Healthcare.** Many pharma, medical device, providers, payers, and BAs have been the target of cyber-attacks.

*Privacy and security are prerequisites for new, health analytics and HIT models.*

- 75% of Healthcare organizations indicate they have or plan to use data for secondary and new uses
- 48% have implemented privacy and security safeguards
Trends 2 – New Global Laws/Enforcements Impacting Health

Global Changes to Accommodate New Business Models

- Business operations and IT increasingly being consolidated and/or conducted globally.

Growing Web of Laws Increasing and Creating Complexity

- 250+ privacy/security laws in 150+ countries impacting marketing, health, HR, breaches.
- New laws in US, Japan, Singapore, Malaysia, South Africa, Mexico, Venezuela.
- Privacy Shield and other EU/global data transfer solutions used following Safe Harbor.
- Dramatic privacy, data handling and retention requirements under upcoming EU GDPR.
- New Types - Breach Notification, ID Theft Prevention, Required Security Controls Laws.

Heightened Regulatory and Class Action Scrutiny Raises Stakes

- Regulator aggressively inspecting and pursuing breaches and failure of safeguards.
- HIPAA audits and enforcements in the US, and health-related inspections in EU.
- Over $450 million paid in fines, penalties and class-actions for breaches/non-compliance.
- Under EU GDPR, fines can be levied up to 4% of annual revenue for non-compliance.
**Trend 3 – Rise of Cyber and Vendor Breaches in Healthcare**

**Threat actors are more diverse and capable, increasing the frequency and magnitude of cyber-attacks and compromise of healthcare IP and crown-jewels**

- **More Diverse**
  - The Threats have become more diverse and distributed...
  - Foreign Intelligence Services
  - Cyber Criminals
  - Terrorists
  - Hactivists
  - Hate

- **More Capable**
  - ... while growing in sophistication with lower barriers to entry
  - The sophistication of available tools is growing
  - While the sophistication required of actors is declining

- **Greater Impact**
  - ...increasing both the frequency and impact of attacks
  - 1,023,108,267 Records Compromised
  - 2,122 Confirmed Data Breaches
  - 79,790 Security Incidents
  - 90%+ Stem from Common Techniques, although risks vary by industry, including:
    - Compromised Credentials
    - RAM Scraper
    - Phishing
    - Spyware/Keylogger
  - 70%+ Alerted by Third Party

**55%** of individuals who had their information compromised were from vendor/ BA breaches.

**Economic impact from cyber attacks estimated $400M-$1 Bil.**
III. Privacy Officer Roundtable – Lessons Learned from the Front Line
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

1. Big Picture – What Is the Biggest Change Occurring and Coming in Healthcare
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

2. Risk Assessment – Given the OCR Focus on Risk Assessment – How Has that Impacted What You Do as an Organization?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

**Cyber Risk –**

3. **Risk or Hype.** How Is This Risk Different than Traditional Old Security (what are you seeing – cyber attacks, ransomware, medical ID theft, phishing, other)?

4. **Preparedness.** What Have You Done as An Organization to Mature Cybersecurity Preparedness (i.e., enhanced controls, incident response plans, table top exercises, other)?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

**Business Associates –**

5. **New Technology.** What rights have you entrusted to third parties for new technology and machine learning (or other innovation)?

6. **Controls.** Given all of the new vendors and third parties involved in the delivery of healthcare, how are you enhancing third party controls (i.e., pre-contract assessment, enhanced BAAs, and post-contract monitoring/auditing)?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

7. **International** – How Do You Integrate HIPAA with GDPR and other global requirements?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

8. Workforce Training – How Do You Keep It Real . . . Real Fun?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

9. Workforce Monitoring – Hard to Do – What Is Working (e.g., Fair Warning, manual, other approach)?
III. Privacy Officer Roundtable – Lessons Learned from the Front Line

10. Remarks – What Advice Do You Give to New Privacy Professionals on How to Prepare to Succeed?
IV. Questions