Update from the HHS Office for Civil Rights

Roger Severino, Director
HHS Office for Civil Rights
2019 OCR/NIST Conference
October 16, 2019
In addition to requesting broad input on the HIPAA Rules, the RFI asked for comments on specific areas of the HIPAA Privacy Rule, including:

- Encouraging information-sharing for treatment and care coordination;
- Facilitating parental involvement in care to address the opioid crisis and serious mental illness; and
- Changing the current requirement for certain providers to make a good faith effort to obtain an acknowledgment of receipt of the Notice of Privacy Practices.
Health App FAQs

• In April 2019, OCR issued new FAQs addressing the HIPAA right of access as it relates to health apps. The FAQs clarify:
  
  • A covered entity cannot withhold sending ePHI to a health app selected by an individual because of concerns about how the health app developer will use or disclose ePHI.

  • A covered entity is not liable for the re-disclosure of ePHI by a health app if there is no business associate relationship between the health app developer and the covered entity.

  • The HIPAA Rules don’t follow health data everywhere it goes.

• https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html
WHAT’S WITH THE BOOT?!
Surprise Billing

• On June 24, 2019, President Trump issued Executive Order 13877 which directed HHS to “solicit comment on a proposal to require healthcare providers, health insurance issuers, and self-insured group health plans to provide or facilitate access to information about expected out-of-pocket costs for items or services to patients before they receive care.”

• Listening sessions with clearinghouse, business associates, health plans, healthcare providers and consumers.
## Recent Enforcement Actions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2018</td>
<td>Pagosa Springs Medical Center (calendar app and employee controls)</td>
<td>$111,400</td>
</tr>
<tr>
<td>12/2018</td>
<td>Cottage Health (unsecure servers)</td>
<td>$3,000,000</td>
</tr>
<tr>
<td>4/2019</td>
<td>Touchstone Medical Imaging (unsecure servers)</td>
<td>$3,000,000</td>
</tr>
<tr>
<td>4/2019</td>
<td>Medical Informatics Engineering (hacked user ID and password)</td>
<td>$100,000</td>
</tr>
<tr>
<td>9/2019</td>
<td>Bayfront Health St. Petersburg (Right of Access to records)</td>
<td>$85,000</td>
</tr>
<tr>
<td>9/2019</td>
<td>Elite Dental Associates (social media)</td>
<td>$10,000</td>
</tr>
</tbody>
</table>
500+ Breaches by Type of Breach

January 1, 2018 – December 31, 2018

- Theft: 11%
- Loss: 4%
- Unauthorized Access/Disclosure: 40%
- Hacking/IT: 43%
- Improper Disposal: 2%

January 1, 2019 – September 30, 2019

- Theft: 8%
- Unauthorized Access/Disclosure: 27%
- Hacking/IT: 61%
- Improper Disposal: 1%
- Loss: 2%
500+ Breaches by Location of Breach

January 1, 2018 – December 31, 2018

- Paper Records: 20%
- Desktop Computer: 8%
- Laptop: 6%
- Portable Electronic Device: 5%
- Network Server: 18%
- Email: 29%
- EMR: 7%
- Other: 7%

January 1, 2019 – September 30, 2019

- Email: 40%
- Network Server: 25%
- EMR: 4%
- Other: 6%
- Portable Electronic Device: 2%
- Paper Records: 11%
- Desktop Computer: 7%
- Laptop: 4%
Cybersecurity Concerns and Trends

- Ransomware
- Phishing attacks
- Remote Desktop Protocol Vulnerabilities
- Weak Authentication
  - Single factor
  - Poor password rules (‘password’)
- Access Controls
  - Current and former workforce members
2019 Cybersecurity Newsletters

- Current Topics:
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats

- Past Topics Include
  - Risk Analyses v. Gap Analyses
  - Workstation Security
  - Software Vulnerabilities and Patching
  - Guidance on Disposing of Electronic Devices and Media
  - Considerations for Securing Electronic Media and Devices

“Semper Paratus”
motto of the U.S. Coast Guard
For More Information

• Visit us at http://www.hhs.gov/HIPAA

• Follow us on Twitter @HHSOCR

• Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/