2022 Advisory Council on Employee Welfare and Pension Benefit Plans

Cybersecurity Issues Affecting Health Benefit Plans
Cybersecurity Insurance and Employee Benefit Plans

September 8, 2022  Mariah Becker, National Coordinating Committee for Multiemployer Plans
Kathryn Bakich, Diane McNally

© 2021 by The Segal Group, Inc.
About NCCMP and Multiemployer Plans

• NCCMP founded in 1974 following passage of ERISA
  – Only national organization devoted exclusively to educating and advocating on behalf of multiemployer pension and health and welfare plans

• NCCMP membership includes stakeholders from throughout multiemployer community
  – Multiemployer pension and health plans – Plan professionals
  – Unions
  – Employers and Employer Associations
About NCCMP and Multiemployer Plans

- Multiemployer plans are governed by a board of trustees with equal representation from both management and labor.
- Funded solely by contributions determined as a result of collective bargaining:
  - Made by employers, but negotiated out of wage/benefits package.
  - Made to a trust fund that is managed by the board of trustees and operates independent of either bargaining party.
  - Contributions held in trust for the exclusive purpose of providing benefit for participants.
- Size and administrative structure of funds varies greatly:
  - Approach to cybersecurity issues varies greatly as well.
HIPAA/HITECH Foundations
Background on HIPAA Privacy, Security, and HITECH

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification Provisions, and Compliance Dates:
  - Electronic Data Interchange: October 15, 2002
  - Privacy: April 14, 2003
  - Security: April 20, 2005

- The Health Information Technology for Economic and Clinical Health (HITECH) Act, was part of American Recovery and Reinvestment Act of 2009. Compliance dates are rolling:
  - Certain provisions were effective “immediately” (February 17, 2009)
  - Breach Notification was effective September 23, 2009
Latest HIPAA Security Update
New Incentive to Adopt Recognized Security Practices

- New federal law enacted January 5, 2021 (Public Law 116-321)
- Applies to covered entities (e.g., health plans and health care providers) and business associates subject to HIPAA security rule
- HHS is now required to consider entity’s adoption of “recognized security practices” in its enforcement activities under the HIPAA security rule
- Recognized security practices include standards, guidelines and best practices developed by the National Institute of Standards and Technology (NIST)
- Adoption of such standards can mitigate fines or result in early, favorable termination of HHS audit
Covered Entities

• Group health plans are “covered entities” and directly regulated by HIPAA

• Retirement plans are not “covered entities”

• Employers are not “covered entities” and are not directly regulated by HIPAA
  – Employers may not use information from health plans to make employment decisions (hiring, termination, etc.)
What is “Protected Health Information” or “PHI”?  

- Health Information that relates to:
  - Past, present or future physical or mental health or condition of an individual, or
  - The provision of health care to an individual, or
  - Past, present or future payment for the provision of health care to an individual

- Is individually identifiable

- Is created, received or maintained by a covered entity
HIPAA Privacy and Security Rules

**HIPAA Privacy Rule**

Protects all types of PHI:
- Electronic
- Written
- Oral

**HIPAA Security Rule**

- Applies to electronic PHI (ePHI) only
- ePHI = transmitted by electronic media or maintained on electronic media

**Examples:**
- Sent or received via e-mail
- Stored on computer network
- Stored on computer (including laptops, netbooks or tablets)
- Stored on electronic media such as CDs, disks, flash drives, tapes or memory cards (including those in smartphones)
HIPAA Enforcement Process

- The HHS Office for Civil Rights (OCR) enforces the Privacy and Security Rules
  - Publishes detailed guidance, FAQs
  - Investigates Complaints
  - Conducts compliance reviews to determine if covered entities are in compliance
  - Performs education and outreach to foster compliance with the Rules' requirements
  - Enters into public Resolution Agreements to resolve violations
- OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA
- Civil and criminal penalties for violations
HIPAA Complaint Process

Complaint

Intake & Review
- Possible Criminal Violation
- Possible HIPAA Rule Violation

Resolution
- Incident occurred more than 6 years ago
- Entity is not covered by the HIPAA rules
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the HIPAA Rules

DOJ
- DOJ declines case & refers back to OCR

Investigation

Resolution
- OCR finds no violation
- OCR provides technical assistance
- OCR issues formal finding of violation
- OCR makes determination not to investigate further
- OCR obtains voluntary compliance, corrective action, or other agreement

Accepted by DOJ

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html
Published Resolutions Provide Additional Guidance

OCR Settles Case Concerning Improper Disposal of Protected Health Information

OCR announced a settlement with New England Dermatology P.C., dba a New England Dermatology and Laser Center ("NDELc"), over the improper disposal of protected health information, a potential violation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. As a result, NDELc paid $300,840 to OCR and agreed to implement a corrective action plan to resolve this investigation. NDELc is located in Massachusetts and provides dermatology services.

- Read the HHS Press Release
- Read the Resolution Agreement and Corrective Action Plan
- Read OCR’s FAQs concerning HIPAA and the disposal of protected health information - PDF

Content created by Office for Civil Rights (OCR)
Content last reviewed August 23, 2022
HITECH Breaches Published

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

### Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

#### Show Advanced Options

<table>
<thead>
<tr>
<th>Expand</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Methodist McKinney Hospital</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>110244</td>
<td>08/26/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>Methodist Craig Ranch Surgical Center</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>15157</td>
<td>08/26/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>First Street Family Health</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>7310</td>
<td>08/26/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>One Medical, Inc.</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>1009</td>
<td>08/25/2022</td>
<td>Theft</td>
<td>Paper/Prints</td>
</tr>
<tr>
<td></td>
<td>USAble Mutual Insurance Company d/b/a Arkansas Blue Cross and Blue Shield</td>
<td>AR</td>
<td>Health Plan</td>
<td>6871</td>
<td>08/25/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>Health Advantage</td>
<td>AR</td>
<td>Health Plan</td>
<td>1642</td>
<td>08/25/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>EmergEOrtho</td>
<td>NC</td>
<td>Healthcare Provider</td>
<td>68861</td>
<td>08/25/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>General Health System</td>
<td>LA</td>
<td>Healthcare Provider</td>
<td>501</td>
<td>08/25/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>Prowers County Hospital District</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>1205</td>
<td>08/22/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>Cerebral Medical Group, P.A.</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>6110</td>
<td>08/19/2022</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Prints</td>
</tr>
<tr>
<td></td>
<td>Celanese Medical Plan</td>
<td>TX</td>
<td>Health Plan</td>
<td>704</td>
<td>08/19/2022</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td></td>
<td>Medical Mutual of Ohio</td>
<td>OH</td>
<td>Health Plan</td>
<td>1377</td>
<td>08/17/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>San Diego American Indian Health Center</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>27367</td>
<td>08/15/2022</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td></td>
<td>Novant Health Inc. on behalf of Novant Health ACE &amp; as contractor for NMG Services Inc.</td>
<td>NC</td>
<td>Business Associates</td>
<td>1382296</td>
<td>08/14/2022</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
</tbody>
</table>
HIPAA Privacy
Basic Regulatory Framework Since 2003

**Covered Entity: Group Health Plan**
- Multiemployer fund providing health benefits
- Health plan sponsored by single employer
- Health plan sponsored by governmental employer

**BA Agreement**

**Business Associate (“BA”)**
- Provides services to Group Health Plan
- Services require PHI
  
  **Examples:**
  - Benefit consultants
  - Actuaries
  - Attorneys
  - Auditors
  - TPAs
  - PBMs
Treatment, Payment, and Health Care Operations

- Designated health plan staff may use or disclose PHI for “payment” or “health care operations” purposes
  - Designated individuals may engage in activities that are necessary to administer the health plans

- Examples of permissible “payment” or “health care operations” activities:
  - Enrollment
  - Eligibility determinations
  - Customer service
  - Claims adjudication and payment
  - Pre-certification and referrals
  - Utilization review
  - Coordination of benefits
  - Wellness programs
Administrative Requirements - Privacy

The Privacy Rule requires health plans to (partial list):

- Appoint a Privacy Official
- Send a Privacy Notice to participants
- Develop safeguards to protect PHI
- Develop Policies and Procedures on PHI use/disclosure
- Train employees on the Privacy Rule
- Develop sanctions for Privacy Rule violations
HIPAA Security
HIPAA Security Standards

• Administrative, physical, and technical safeguards
  – Administrative safeguards: Administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and security training requirements
  – Physical safeguards: Mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion
  – Technical safeguards: Primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted

• Security rule includes required and addressable implementation specifications
Administrative Security

- Role of the HIPAA Security Official
- Granting, modifying and terminating employee access
- Asset inventory
- Activity logs reviews
- Password policies
- Security training
Physical Security

Office Controls

• Security cameras
• Alarms
• Access controls for employees and visitors

Data Centers

• Environmental monitoring systems
  – Hazardous changes in heat, humidity, airflow, smoke, and electricity
Technical Safeguards

- Access Control
- Encryption and Decryption
- Audit Controls
- Mechanism to Authenticate Electronic Protected Health Information
- Integrity Controls
The Importance of a HIPAA Security Risk Assessment

**Required element for compliance with the HIPAA Security Rule**
- It informs development and implementation of the policies and procedures required by the Security Rule
- OCR has enforced settlements based on lack of or poorly executed risk assessments

**Scope**
- Systems and media that accesses, stores, and transmits ePHI

**Risks and Vulnerabilities**
- Eliminate, mitigate or transfer

**How Often**
- From annually to up to three (3) years
- When new technologies are implemented

**Who Should Perform Assessments**
- “Do It Yourself” (DIY) approach works for covered entities with strong internal resources and time
- Advisable to perform an independent analysis
Let’s Not Forget HITECH

The HITECH (Health Information Technology for Economic and Clinical Health) Act provides guidelines for:

- Protecting ePHI at rest and in motion with encryption
- Disposal of ePHI according to NIST (National Institute of Standards and Technology) guidance
Breach Notification Requirement

- HIPAA covered entities (i.e., the health plans) must now notify individuals when there’s a breach of “unsecured PHI”
  - Applies to all PHI (e.g., oral, paper) not just ePHI
- Also requires notice to HHS and maybe the media
- Business Associate to notify Covered Entity
New Technologies that Introduce Risks and Vulnerabilities

- Workstations and laptops
- Portable media (for example external hard drives or USB drives)
- Smartphones and tablets
- Remote connections into systems
- Internet connections and wireless networks
- Multifunction machines
- Email services
- ePHI transmission channels
- Cloud-based IT environments
- Text and instant messaging
- Voicemail
- Social media presence
- Participant portals
How has COVID-19 Changed the Risk Environment?

- Remote workers
- Use of home equipment and cell phones
- Increased reliance on website communications with participants
- Lack of stable internet access
- Security of paper files and documents
- Heightened risk of cyber attacks
Cyber Insurance Briefing
Cyber Liability Insurance Coverage in Action

How the Coverage Applies

- It provides First Party Breach Response and Expense coverage for data incidents.
- It provides Third Party Liability coverage for Claims arising out of data incidents.
- Most policies provide customized loss prevention and post breach support with industry specialists and pre-screened vendors to assist in the response.
- The increase in systematic wide spread events as well as increasing cyber claims has triggered coverage restrictions, premium and deductible increases and limits reduction.
# How Does Cyber Liability Insurance Function to Cover a Data Incident?

<table>
<thead>
<tr>
<th>Incident Response</th>
<th>First-Party</th>
<th>Third-Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coach Services</td>
<td>Extortion</td>
<td>Privacy Liability</td>
</tr>
<tr>
<td>Legal Services</td>
<td>Restoration</td>
<td>Regulatory</td>
</tr>
<tr>
<td>Forensics</td>
<td></td>
<td>Payment Card</td>
</tr>
<tr>
<td>Notification</td>
<td></td>
<td>Network Liability</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td></td>
<td>Media Liability</td>
</tr>
<tr>
<td>Public Relations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interruption</td>
<td></td>
</tr>
</tbody>
</table>
### Breach Notification Expenses

**First Party Cost Coverage**

#### Notification
- Researching federal and state laws
- Crafting compliance letters
- Preparation and printing costs
- Mailing or delivery costs

#### Public Relations
- Advertising and press releases

#### Call Center Operations
- Operators, scripts, equipment
- Partners with legal counsel

#### Credit Monitoring

#### Forensics
- Legal expenses for outside attorney
- Cost of forensic examination
- Cost to remediate

#### Legal
- Response to claims including lawsuits by affected parties as well as Regulatory Actions
- Defense costs
- Penalties
- Settlements and judgements

#### Other Potential 1st/3rd Party Costs
- Extortion expenses
  - Ransom payment
  - Negotiation expenses
  - Legal expenses
- Fraud Coverages
  - Social engineering, vendor payment
  - Computer
  - Funds transfer
- Data Loss and Restoration
- Hardware replacement costs
- Business interruption/extra expense
- Media Liability: Trademark/copyright, libel/slander
Third Party Liability including Fines and Penalties

Provides protection for Third Party liability exposures

- Covers defense costs, judgments, settlements and related liabilities caused by plaintiffs who bring suit against the insured related to handling private data

- Covers various governmental fines and penalties where insurable

Experience to Date

What litigation has resulted?

Has the litigation led to successful recoveries?

How expensive have they been?

What may the future hold?
The Benefits of Cyber Liability Insurance

• Plan Sponsors should consider Cyber Liability coverage as part of their cybersecurity strategy.

• Cyber Liability provides the first party and third party coverages to protect the plan and its participants.

• Cyber Liability provides expert vendor services and advice on a 24-hour basis.

• Better training, procedures and system controls can mean broader and more affordable coverage.

• Broad coverage maybe more difficult to find at reasonable costs even with the necessary controls in place.
Key Tips for Insurance Applications

- Who is responsible for data security?
- In there an information security policy and how are violations handled?
- What protections exist for Multi Factor Authentication controls?
- Is there an incident response plan in place?
- Is there on going security training?
- Are there contracts in place for 3rd parties who process, host or store sensitive information?
- What has the breach experience been and how was it handled?

Separate questionnaires are now often required to address Ransomware and Social Engineering Fraud exposures.
Cyber Limits & Premiums

✓ Premiums follows an Insured’s cyber hygiene and controls
✓ Cyber claims can have an impact on rates and coverage
✓ Today’s cyber market amends limits as a mechanism of responding to changing risks
✓ How much in limits to carry?
  ✓ It depends on the size and scope of the business operations, type of personal information or client data handled
  ✓ Primary and excess limits vary by market appetite
Disclaimer

Segal Select Insurance Services, Inc. ("Segal Select"), a subsidiary of The Segal Group, Inc. is a specialty retail broker insurance. Any information and/or opinions herein provided by third parties have been obtained from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. The contents of this presentation and any opinions expressed herein are intended for general education purposes only and not as professional advice specific to any person, entity or circumstance. It is not intended for use as a basis for making insurance-related decisions, including determinations of appropriate types or levels of insurance coverage, nor should it be construed as advice designed to meet the needs of any particular person, entity or circumstance. Please contact Segal or another qualified insurance professional for advice regarding the evaluation of any specific information, opinion, or other content. Of course, on all matters involving legal interpretations and regulatory issues, you should consult legal counsel.
Thank You!

Mariah Becker  
mbcker@nccmp.org / 917.648.4240

Kathy Bakich  
kbakich@segalco.com / 202.833.6494

Diane McNally  
drmcnally@segalco.com / 212.251.5146