Privacy and Compliance, HIPAA State Law and GDPR

Iliana Peters, Shareholder, Polsinelli, PC
Ali Pabrai, Global Cybersecurity & Compliance Expert
CEO, ecfirst

Agenda

- Privacy: Global State
- HIPAA Settlements
- General Data Protection Regulations (GDPR)
- California Consumer Privacy Act (CCPA)
- NIST Cybersecurity Framework
State of HIPAA Compliance

Total Settlements: $31,820,400

Summary! 2019 HIPAA Fines by State Attorney Generals

Fine: $10M
Premera Blue Cross
July 11, 2019
CAP Required

Fine: $9M
Medical Informatics Engineering Inc. (MIE)
May 29, 2019
CAP Required
Premera Blue Cross, paid $10 million to 30 states following an investigation into a data breach that exposed personal information on more than 10 million people across the country.

Premera will spend $74 million to settle a federal class-action lawsuit on behalf of affected customers.

In addition to the monetary penalty, Premera is required to ensure its data security program is adequate to protect health data as required by law.

From May 5, 2014 until March 6, 2015, a hacker had unauthorized access to the Premera network containing ePHI, including private health information, Social Security numbers, bank account information, names, addresses, phone numbers, dates of birth, member identification numbers and email addresses.

The coalition of 30 state attorneys general, led by Washington State Attorney General Bob Ferguson, investigated Seattle-based Premera’s cybersecurity vulnerabilities that gave a hacker unrestricted access to ePHI for nearly a year.

MIE reached a $900,000 settlement in the country’s first federal multistate lawsuit, over a 2015 data breach that impacted 3.5 million patients.

Between May 7 and May 26, 2015, hackers gained access to a server containing data related to its NMC service. Names, addresses, usernames, passwords, and ePHI were potentially accessed and stolen.

Hackers infiltrated a MIE Web application and accessed its records on more than 3.9 million individuals. The data included sensitive medical and financial information such as Social Security numbers, lab results, medical conditions and health plan records.

Eleven of MIE’s clients and 44 radiation centers were affected, along with nearly 200 provider clients of MIE subsidiary NoMoreClipboard (NMC), which markets personal health records to health care providers, to employers and directly to consumers.

Indiana-based MIE undertook to notify all affected individuals, but some employer and health care provider clients reached out to their employees and patients as well, in part to minimize confusion.

MIE was sued by 16 states following a 2015 data breach.
Privacy and Compliance, HIPAA State Law and GDPR

General Data Protection Regulations (GDPR)

GDPR Fast Facts

GDPR Mandate
- Privacy Impact Assessment
- Personal Data
- Data Portability
- Consent
- Data Breach Notification
- Right to be Forgotten

Protect by Design

GDPR Program
1. Conduct GDPR awareness training for every workforce member
2. Appoint a Data Protection Officer (DPO)
3. Assess GDPR readiness
4. Develop policies, consent and other documents to address GDPR mandates
5. Create procedures to align with GDPR requirements
6. Update cyber incident response based on GDPR data breach specification
7. GDPR Vendor Readiness
### GDPR Settlement: Marriott

- July 9, 2019, the Information Commissioner's Office (ICO) issued a notice of its intention to fine Marriott International £99,200,396 for violating the EU’s GDPR.
- The hotel group, which suffered a breach last year, could face a fine of over £99 million ($123 million).
- The fine relates to an incident that Marriott brought to the ICO’s attention in November 2018.
- A variety of personal data containing approximately 339 million guest records were exposed by the incident.
- Approximately 30 million records were thought to relate to residents of 31 countries in the European Economic Area (EEA), with 7 million related to UK residents.
- It is believed the vulnerability began with systems of the Starwood hotel group that were compromised in 2014. Marriott acquired Starwood in 2016, but the exposure was not discovered until 2018.
- The ICO found that Marriott failed to undertake sufficient due diligence when it bought Starwood.

### GDPR Settlement: British Airways

- July 8, 2019, the ICO issued notice of its intent to fine British Airways £183.39 million for GDPR infringements.
- British Airways notified the ICO of the incident in September 2018 after suffering a cyberattack in September last year.
- Hacker had stolen payment card data associated with 380,000 transactions including bank card numbers, expiry dates and cvv codes.
- Transactions details were taken via malicious script designed to steal financial information by skimming BA's payment page before it was submitted.
- The attack, thought to be perpetrated by the same group that hit Ticketmaster, Magecart, would allow adversaries to see people’s details as they were entered on the page.
- The ICO found that the company had poor security arrangements which compromised a variety of data, including log in, payment card, and travel booking details as well name and address information.
California Consumer Privacy Act (CCPA)

Key Facts

- Enforced July 1, 2020.
- Privacy rights for California residents.
- Grants new enforcement power to the Attorney General.
CCPA Individual Rights

What personal information is being collected about them.

Whether their personal information is sold or otherwise disclosed and to whom.

To say no to the sale of their personal information.

To access their personal information and request deletion under certain circumstances.

To receive equal service and price.

CCPA Consumer Rights, A Summary

<table>
<thead>
<tr>
<th>Right to Knowledge</th>
<th>Right to be Forgotten</th>
<th>Right to Control Who has Access to their Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers have the right to request information about:</td>
<td>• Companies must delete all information they have about a consumer at the consumer’s request.</td>
<td>• Consumers must be able to opt out of the sale of their information to third parties.</td>
</tr>
<tr>
<td>• What information a company is collecting about them</td>
<td>• Exceptions include:</td>
<td></td>
</tr>
<tr>
<td>• How that information will be used</td>
<td></td>
<td>• Data being processed and retained to complete a consumer-requested transaction</td>
</tr>
<tr>
<td>• If and with whom that information will be shared</td>
<td></td>
<td>• Specific research purposes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited analytical used Other regulatory and contractual exceptions</td>
</tr>
</tbody>
</table>
CCPA Enforcement and Penalties

| CCPA Penalties | For non-compliance | Unintentional | $2,500 |
| | | Intentional | $7,500 |
| If personal information is exposed in a data breach | Per incident | $100–$750 or greater if the actual damages exceed $750 |

CCPA: Key Steps

1. Establish Responsibility
2. Perform a comprehensive and thorough risk assessment, inclusive of a technical cybersecurity assessment
3. Update policies and procedures to address CCPA
4. Remediate gaps for CCPA compliance as identified in the risk assessment
5. Review cybersecurity supply chain (e.g. business associates), including update to contracts/agreements to determine appropriate protection for all California resident data
6. Train members of the workforce to raise higher awareness of CCPA requirements
7. Monitor capabilities implemented actively to ensure appropriate management of controls
NIST Cybersecurity Framework: Foundation for Cybersecurity

<table>
<thead>
<tr>
<th>Function/Unique Identifier</th>
<th>Function</th>
<th>Category/Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GA</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk-Management</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Identify Management and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection/Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PE</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.BP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.BP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.MI</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

Cyber-attacks: Global & Sophisticated

1. Initial Recon
2. Initial Compromise
3. Establish Foothold
4. Escalate Privileges
5. Internal Recon
6. Move Laterally
7. Maintain Presence

Done

Complete Mission