Ransomware Cost This Practice $240,000 in Government Penalties: How Phishing Set Off a Chain Reaction

By Rana McSpadden, FACMPE

On October 3, 2024, the Office for Civil Rights (OCR) announced Providence Medical Institute (PMI) in Southern California was ordered to pay $240,000 because of a ransomware breach investigation. What makes this announcement unique compared to other OCR investigations is that, in a rare move, the payment was the result of a Civil Monetary Penalty rather than a settlement.

Why was a penalty imposed?

After receiving the results of the OCR's investigation in September 2023, PMI was offered the opportunity to settle the investigation but failed to do so. In January 2024, the OCR then sent PMI a Letter of Opportunity informing them that they had failed to comply with certain provisions of the HIPAA Privacy and Security Rules and failed to resolve these matters through informal means. As a result, PMI was provided with an opportunity to submit evidence of any mitigating factors or defenses against the allegations to support a waiver of Civil Monetary Penalties. While they provided arguments in February 2024, the OCR determined this information did not support an affirmative defense or waiver of Civil Monetary Penalties, and thus, after obtaining authorization from the Attorney General of the US, a Notice of Proposed Determination to impose a Civil Monetary Penalty (CMP) was issued. PMI chose to waive their right to a hearing and not contest the OCR's proposed determination. On July 1, 2024, the OCR published a Notice of Final Determination. As a result, PMI was required to pay $240,000, in full, upon receipt of the notice.

How did we get here?

Before discussing what violations led to the CMP, let's first discuss what happened to trigger an investigation. In July 2016, Providence Medical Institute acquired Center for Orthopaedic Specialists with an end goal to transition them into PMI's IT environment over the next two years. During the transition period, Center for Orthopaedic Specialists (COS) was allowed to maintain their relationship with their current IT vendor. Before the transition into the PMI IT environment was completed, an employee of COS clicked on a phishing email that resulted in a ransomware attack on February 18, 2018. Systems were quickly restored using system backups; however, the same ransomware attacker was able to ransom the systems two additional times on February 25, 2018 and March 4, 2018. A breach report was submitted to the OCR on April 18, 2018 reporting that 85,000 individuals' data, including names, had been compromised in the ransomware attacks. As a result of the report, the OCR opened an investigation into the incident in May 2018.

What did the investigation find?

During the OCR's investigation, PMI also conducted a post-incident investigation in June 2018. That investigation found that COS:

- utilized outdated and unsupported operating systems on computers that housed ePHI,
- failed to separate their private network from the public internet,
- had a misconfigured firewall that did not properly track network access,
- allowed insecure remote access to workstations, and
- workforce members shared administrative login credentials, allowing unrestricted administrator access.

The OCR found additional evidence during their investigation that COS had not deployed encryption on their workstations or servers, allowing ePHI to be visible and accessible during the ransomware attacks. They also found that PMI, being the owner of COS, did not have a signed Business Associate Agreement with the IT vendor providing services to

COS during the transition to PMI's systems until June 2018.

The final ruling from the OCR found PMI failed to uphold the HIPAA Security Rule by:

- failing to implement various required technological policies and procedures to prevent unauthorized access to ePHI, and
- failing to have a signed Business Associate Agreement with the IT vendor providing services to COS during the transition period.

Takeaways

Regardless of the size of the practice, many things can be learned from this case. Here are a few helpful points:

- All workforce members, including all staff, physicians, advanced practice practitioners, volunteers, and students, must have proper cybersecurity education to include how to spot phishing emails and what to do if one is received.
- Ensure Business Associate Agreements (BAA) are signed and maintained with any business associate who has access to systems containing ePHI. Anytime there is a change in ownership of either the covered entity or business associate, a new BAA must be signed.
- Utilize systems with current and up-to-date operating systems. Install all system security updates to keep devices containing and accessing ePHI secure, including all workstations and servers.
- All employees must have their own login credentials that should not be shared with anyone. Only select users should have administrative access.
- Conduct routine Security Risk Analyses, especially when there are significant changes within the practice, including changes in ownership/administration, changes in hardware/software, changes in location, or any other event that could change the security risk of ePHI.
- Change any compromised user credentials or passwords whenever a security incident occurs involving the improper acquisition of a user's login credentials. However, select circumstances may require all user credentials to be reset. Conduct an incident assessment to determine the level of credential reset necessary to ensure all unauthorized access to systems has been eliminated.

In conclusion, the case of Providence Medical Institute underscores the critical importance of robust cybersecurity measures and compliance with HIPAA regulations. The significant financial penalty imposed by the OCR serves as a stark reminder that healthcare organizations must prioritize the security of ePHI. By implementing comprehensive security protocols, ensuring all workforce members are educated on cybersecurity best practices and maintaining up-to-date systems and agreements, healthcare practices can better protect themselves against cyber threats and avoid costly penalties. This case highlights that proactive measures and timely responses to security incidents are essential in safeguarding patient data and maintaining regulatory compliance.

If you have questions about HIPAA, cybersecurity, or access to SVMIC resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity or other HIPAA related incident, contact SVMIC as soon as possible by calling the Claims department at 800-342-2239.

Other individuals in your organization who may benefit from these articles and resources include your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

References:

1. (2024, October 3). *HHS Office for Civil Rights Imposes a $240,000 Civil Monetary Penalty Against Providence Medical Institute in HIPAA Ransomware Cybersecurity Investigation*. U.S. Department of Health and Human Services. https://www.hhs.gov/about/news/2024/10/03/hhs-ocr-imposes-civil-monetary-penalty-against-providence-medical-institute-hipaa-ransomware-cybersecurity-investigation.html
2. (2024, March 29). *Providence Medical Institute Notice of Proposed Determination*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/pmi-npd/index.html
3. (2024, July 1). *Providence Medical Institute Notice of Final Determination*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/pmi-nfd/index.html