HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH LAW NEWS

JULY 19, 2016

YOUR MONEY OR YOUR PHI: NEW GUIDANCE ON RANSOMWARE

Since the first large U.S. health care ransomware demand hit the news in early 2016, attacks have been increasing in visibility and frequency, reaching a claimed 4,000 attacks per day. Ransomware is a kind of malware that infects computer systems, restricting access to systems or to data until a "ransom" is paid to the criminals. There has been dispute about the appropriate way to handle a ransomware attack from both an information security and a privacy perspective. Recognizing the critical nature of this threat, the Secretary of Health and Human Services sent a letter to health care CEOs, which can be found here, and the Office for Civil Rights ("OCR") issued guidance to the industry entitled "FACT SHEET: Ransomware and HIPAA," which can be found here.

The Secretary's letter, issued on July 11, 2016, emphasized that cybersecurity, and in particular ransomware, is not merely a technology issue; it is a critical business issue that can materially impact the ability of a health care organization to provide safe and effective care. It can also lead to substantial financial losses. However, appropriate security practices can help protect against ransomware infections.

Key takeaways on ransomware prevention, detection and reporting include the following.

PREVENTION

- Conduct a risk assessment and implement a responsive security management process that mitigates identified threats and vulnerabilities.
- Implement procedures to identify and protect against malicious software.
- Train users to assist in identification and reporting of malicious software and attacks.
- Limit access to ePHI to individuals and software that require access for legitimate purposes.
- Ensure that the security management process covers all components and data of the enterprise.
- Maintain current backups of data and systems and ensure that backups can be restored.
- Maintain and test a contingency operations plan; a disaster recovery plan and continuity of operations plan should be developed and tested to ensure all critical systems and data can be accessed in the event systems are unavailable.

DETECTION

- An incident response plan should be in place that defines team members and roles to detect and respond to ransomware (and other cyber incidents).
- The goal of incident response will be to conduct an initial analysis, contain the impact and control propagation of the infection, remove all traces of the infection and mitigate or remediate vulnerabilities.
- Data will need to be evaluated to ensure its integrity has not been adversely affected.
- Forensic examination may be needed to identify the route of infection; ensure that all remnants of the malware have been removed; determine if any data was exfiltrated or changed; determine if there are any reporting obligations; and identify vulnerabilities that need to be mitigated to avoid future infections or attacks.
- Monitoring of system operations may give early warning of infection; for example, unexplained spikes in processing activity may indicate the ransomware is searching and encrypting data, and unusual communication patterns may indicate communications to the "command and control" computer. Technology staff should be encouraged to watch for and report on such anomalies.
- Users should be trained to only click on known links, not open attachments unless they are from known senders and expected and be alert to unusual activity and report anything suspicious.
- Reports to law enforcement of suspected ransomware are appropriate; however, such reports should be made through legal counsel.

TO REPORT OR NOT TO REPORT

- Ransomware infection in which the data is encrypted is presumed to be a breach under HIPAA because it is the "acquisition" of PHI in a manner not permitted under the rule.
- Whether the breach must be reported depends on whether there is a "...low probability that the PHI has been compromised..." pursuant to a risk assessment.
- Analysis of the type and variant of ransomware, communication with the command and control computer and any attempts to exfiltrate data and other information such as any known details regarding the perpetrator of the crime may help determine the risk that the PHI was compromised.
- Lack of access to data, or high risk of loss of data integrity, may also support breach reporting.
- Careful documentation of the decision process is critical.
- If the PHI was already encrypted so as to no longer be "unsecured PHI," then no risk assessment is needed to determine whether there is low probability of compromise; there is no obligation to report the incident. However, if the means of encryption left the data vulnerable in any way to the ransomware (for example, if there is a possibility that ransomware was installed on a laptop while in use, even if the laptop is encrypted, because data is typically unencrypted when in use), then the PHI was unsecured and a breach is presumed.

In addition to the Fact Sheet, OCR provided a link to ransomware guidance from the FBI, which may be found here.

One question that often arises is whether to pay the ransom to recover the files. There are risks to both paying and not paying; while most of the culprits release the encryption key upon receiving the payment, there are reports of a new variant that is not unlocked upon payment of the ransom. The decision to pay or not to pay is a complex decision that is based on the facts of the specific situation.

If you have any questions, please contact:

- Melissa L. Markey at (248) 457-7853 or mmarkey@hallrender.com;
- Elizabeth Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com;
- Stephen D. Rose at (425) 278-9337 or srose@hallrender.com; or
- Your regular Hall Render attorney.

Please visit the Hall Render Blog at http://blogs.hallrender.com/ or click here to sign up to receive Hall Render alerts on topics related to health care law.