ManageEngine
DataSecurity Plus

HIPAA GUIDELINES ON RANSOMWARE ATTACKS

Ransomware

Malicious software designed to capture, encrypt, and hold data hostage until victims pay a ransom.

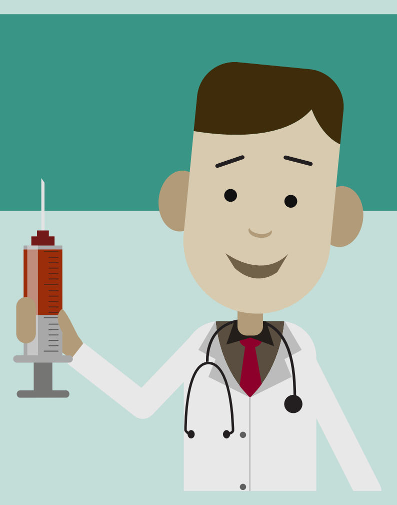
HIPAA

Standards health care companies need to follow to protect and maintain the confidentiality of personally identifiable health care information.

How can HIPAA compliance help prevent malware infections, including ransomware attacks?

HIPAA's security rule mandates enterprises adopt security measures that prevent ransomware, such as:

- Conducting risk analysis to identify threats and vulnerabilities to PHI.*
- Educating end users about malicious software protection.
- Detecting malicious software.
- Implementing the principle of least privilege to limit access to PHI.



How can HIPAA compliance help enterprises recover from ransomware infections?

HIPAA mandates organizations follow a few key procedures to respond to and recover from a ransomware attack, including:

- Detecting and conducting initial analysis on the ransomware attack.
- Conducting post-incident activities that include in-depth forensic analysis.
- Restoring data lost during a ransomware attack.
- Containing the impact and propagation of ransomware.
- Remediating the vulnerabilities that permitted ransomware propagation.

Post-breach analysis should include an assessment of whether there was a breach of PHI as a result of the ransomware security incident.

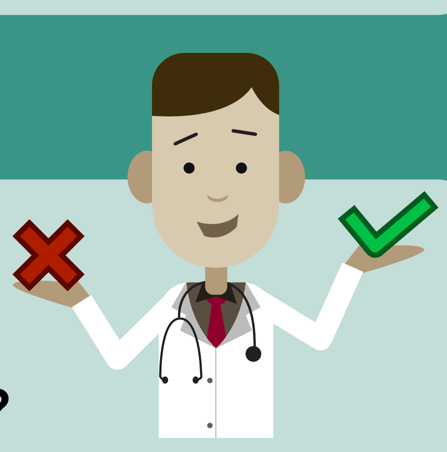
Is it a HIPAA breach if ransomware infects a covered entity's system?

- If ePHI** is encrypted as a result of a ransomware attack, then a HIPAA breach has occurred.
- If the organization can prove that there is a "...low probability that the PHI has been compromised," then the ransomware attack has not resulted in a HIPAA breach.

How can businesses prove that a ransomware attack hasn't compromised their customers' PHI?

If an organization faces a ransomware attack, HIPAA mandates that they report the breach if any PHI has been compromised. However if an organization can prove PHI wasn't exfiltrated or compromised during the attack, they can avoid the breach notification process. Organizations should ask themselves the following questions when investigating whether PHI was compromised:

- What type and amount of PHI was involved in the attack?
- To what extent has the risk to the PHI been mitigated?
- Was the PHI actually acquired or viewed?
- Who used the PHI and who was it disclosed to?



Is it a reportable breach if the compromised ePHI was already encrypted to comply with HIPAA?

- No, since ePHI encrypted to comply with HIPAA is no longer considered "unsecured PHI."

* PHI - Protected health information

** ePHI - Electronic protected health information

Source: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

ManageEngine
DataSecurity Plus

www.datasecurityplus.com
support@datasecurityplus.com