GLASER & WEINER, LLP

ATTORNEYS AT LAW

Ransomware

Is Your Business Protected?

When implementing and testing anti-malware security measures and security incident procedures, the Department of Health and Human Services (HHS) recently urged covered entities under HIPAA, as well as their business associates, to determine whether they have adequately addressed the rapidly growing threat of ransomware attacks. Ransomware is a type of malicious software (malware) that hacks into and encrypts a user's data so that it cannot be accessed until the user pays the hacker a ransom. Often, ransomware cannot be detected until after it has encrypted the user's data, and it can result in a serious breach of HIPAA rules.

HHS noted that HIPAA-compliant security measures and contingency planning can help prevent ransomware from infecting a covered entity or business associate's computer systems, or, if an attack does take place, recover from it. For example, adequate security measures must include a security management process that incorporates an accurate and thorough risk analysis to identify and mitigate potential threats to all electronic protected health information (ePHI) that an entity creates, receives, maintains, or transmits. The entity's security procedures must also guard against and detect malware (including ransomware), train users in detecting and reporting malware attacks, and restrict ePHI access to persons or software programs that must access it. Required contingency planning includes disaster recovery and emergency operations planning, as well as a data backup plan, for which HHS recommended conducting frequent test restorations, and possibly maintaining backups offline so that they cannot be accessed from an entity's network. Further, the entity should be able to take measures to isolate infected computer systems so that an attack does not spread.

Any ransomware attack on a covered entity or business associate constitutes a security incident under the HIPAA Security Rule. Thus, entities must have adequate security incident procedures to respond to these attacks. First, HHS said that an entity should conduct an analysis of the attack's scope, origination, how it occurred, and whether it has finished, is ongoing, or has caused other incidents. Then, the entity should take steps to contain and eradicate the ransomware, as well as fix any security vulnerabilities that allowed the attack to happen, and restore any data lost during the attack so that it can return to normal operations.

Once an attack is over, the entity should conduct a post-incident review to determine if an impermissible disclosure of ePHI and HIPAA Privacy Rule breach resulted from the attack. If ePHI is encrypted by ransomware, HHS said that this constitutes an unauthorized disclosure of ePHI and is thus presumptively a breach, unless the entity can demonstrate by conducting a

thorough risk analysis that there is a "low probability that the PHI has been compromised." The risk analysis must consider:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

If the entity determines that there has been a breach, it must then comply with any applicable breach notification requirements, such as notifying affected individuals and the Secretary of HHS, as well as the media (if the breach affects over 500 individuals).

However, if the ePHI encrypted by ransomware was already encrypted by the entity so that it is unreadable, unusable and indecipherable to any unauthorized person, than it is no longer considered to be "unsecured PHI" and the attack would not constitute a breach requiring disclosure.

Entities covered by HIPAA may wish to contact Roni Glaser or Michael Weiner to further discuss what they may do to better protect their ePHI from ransomware attacks.