Health Information Compliance Alert

Ransomware 101: A Quick-Start Guide

So there's new guidance from **HHS's Office of Civil Rights** about how to fight ransomware, and you've certainly read about ransomware attacks on health care providers, but what is ransomware exactly?

Data-for-ransom is the latest fad in the hacking world. Ransomware hackers breach servers and encrypt files containing documents and PHI, then demand a ransom in exchange for the remedy needed to decrypt the files.

Sometimes these hackers pose as the FBI or other law enforcement officials and claim that the ransom is a fine for failure to pass some kind of regulation and that failure to pay will result in prosecution.

New forms of ransomware encrypt files of website operators, threatening not only their files containing stored data, but the very files needed to operate their web sites. Other ransomware variants now target files on mobile devices.

The highly sensitive nature of PHI has led to health care providers being primary targets. Consider just three of many recent examples:

1. In February 2016, **Hollywood Presbyterian Medical Center** computer systems were held for ransom and were not released until the hospital paid 40 bitcoins, about $17,000.
2. In May 2016, **Kansas Heart Hospital** EHR systems were attacked and locked by hackers. When the hospital paid the hackers' requested ransom, the hackers demanded a second ransom in order to regain access to their system. Fortunately, patient data was not compromised.

Note: Read the OCR guidance here: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.