The One Thousand Dollar Ransom Request

The following article is based upon an actual claim situation experienced by an SVMIC policyholder. The details have been altered to protect our policyholder's privacy.

When Mandy*, the receptionist at the small rural medical practice of Dr. Smith, saw that the message light on the phone was blinking, it was not unusual. The practice voicemail was set up with instructions for an emergency, but provided an option to leave a message for routine calls, such as an appointment or prescription refills. However, what Mandy heard on the recording that morning was not a patient, as she anticipated. The electronically disguised voice on the other end of the line informed her the practice's server had been encrypted, the records were being held for ransom and provided instructions to pay the $1,000.00 to unencrypt the records. Mandy saved the message and immediately notified the practice administrator.

Unfortunately, this scenario has become all too common in medical practices. NAS Insurance, our partner in cybersecurity insurance, reported in their June 2017 edition of the Cyber Claims Digest that the company experienced a significant increase in claims activity related to ransomware events during 2016. NAS reported that in 2016, the number of "healthcare-related ransomware events doubled over 2015 activity." You can find this report here.

Fortunately, for this practice, Dr. Smith's professional liability insurance policy with SVMIC includes $50,000 of cybersecurity insurance. The practice administrator called SVMIC claims department, and the report was forwarded to NAS.

A forensic investigator determined that the breach involved only the server that held the images of the old paper files that were scanned when the practice transitioned to electronic health records (EHR), and not their main EHR system. The files on this server were not used very often by the practice and is the reason that they were unaware of the breach until the message was retrieved from their voicemail system. Thankfully, this server, along with all of their other records, was backed up regularly and the practice was able to restore the records without paying the ransom.

However, restoring data is only part of the necessary process after a ransomware attack. A ransomware fact sheet issued by The Department of Health and Human Services (HHS) requires the following regarding a ransomware event: "Unless the covered entity or business associate can demonstrate that there is a '…low probability that the PHI has been compromised,' …a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected

individuals without unreasonable delay, to the Secretary of HHS, and to the media …in accordance with HIPAA breach notification requirements." You can find the fact sheet here .

This HHS fact sheet further describes what steps a covered entity should take in order "to demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach." HHS says that "a risk assessment considering at least the following four factors …must be conducted: 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."

The good news for Dr. Smith was that the IT forensic expert was able to meet the requirements set forth by HHS to show that it was unlikely that the PHI had been compromised. This story has a successful conclusion because he had been backing up his data nightly, and he had SVMIC's included cybersecurity protection. However, if it had been discovered that Dr. Smith's patients' data had been accessed and compromised, the notification and monitoring costs along with the potential fines and penalties may have exceeded the limits included within his SVMIC policy.

SVMIC has partnered with NAS to bring our policyholders access to NAS cyberNET, a new extensive online resource. This portal offers tools, resources, videos, policies and access to cybersecurity experts. This portal is available here on our cybersecurity resources page. In addition, SVMIC's Medical Practice Services offers consulting and training related to cybersecurity and HIPAA.

* All names have been changed
