Wrong Number Results in Security Breach

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.

Springtime in Arkansas brought pleasant temperatures as well as lots of mold and pollen, especially after the mild, wet winter. As a result, Dr. Smith*, a primary care physician, saw many patients with complaints of sneezing, congestion, coughing and sore throats. Most of the patients thought that they had a virus, but Dr. Smith often suspected allergies.

Dr. Smith had a good relationship with Dr. O'Donnell*, an allergist in the same medical office park who also treated Dr. Smith's children for their allergies. Dr. Smith referred any patients who needed allergy testing to Dr. O'Donnell.

Dr. O'Donnell's office was one of the few practices in the medical office complex whose EMR systems did not communicate with Dr. Smith's EMR system. Dr. Smith's office sent medical records including visit notes, lab and x-ray results via facsimile to Dr. O'Donnell's office for the patients who were referred. Lisa*, the Medical Referral Coordinator for Dr. Smith's practice, had Dr. O'Donnell's fax number written on a piece of paper and taped to her desk.

During one particular week, Lisa faxed records for 12 patients totaling approximately 105 pages. Unfortunately, Lisa had spilled some water on her desk and the ink on the piece of paper with Dr. O'Donnell's fax number was smeared, making it difficult to read. Lisa mistook the last digit, an "8", for a "3", and dialed the wrong number when faxing the medical records.

The incorrect fax number belonged to a distribution warehouse. Thankfully, the warehouse sent a fax to Dr. Smith's office advising that they had reached the wrong fax number. Lisa called the distribution company and the warehouse supervisor assured her that they had deleted the fax from their machine as well as shredded the paper copies that had been printed. In spite of the reassurances, there was no way of knowing how many people had seen the patients' medical records.

Fortunately, Dr. Smith had his medical malpractice insurance coverage with SVMIC and his policy included $50,000 of cybersecurity insurance coverage. Lisa reported the error to an SVMIC claims attorney, who then forwarded the information to NAS, SVMIC's partner in cybersecurity coverage. NAS was able to assist Lisa in determining how the practice should proceed in mitigating any damage caused by the faxing error.

Dr. Smith's cybersecurity coverage** not only provided assistance for a cyber-breach or

cyberattack, but it also included coverage for “a claim for an actual or alleged security and privacy wrongful act.” A “security and privacy wrongful act” as defined in the endorsement is “the failure to prevent or hinder a security breach, which in turn results in…the theft, loss or unauthorized disclosure of electronic or non-electronic confidential commercial, corporate, personally identifiable, or private information that is in an Insured’s care, custody or control.”

According to the Health and Human Services (HHS) website, the HIPAA Privacy Rule allows protected health information to be shared by covered providers for the purpose of treatment without patient authorization. There is no restriction as to how the information is to be communicated. However, the provider must have practical precautions in place.

The HHS website says the following regarding fax communications: “…when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information.” You may find more information regarding these guidelines here.

Having learned from this experience, Lisa instituted two mandatory procedures for sending faxes from Dr. Smith’s office to avoid any further mishaps. First, she programmed Dr. O’Donnell’s correct fax number, as well as any other fax numbers used by the practice, into the fax machine. Second, any time a fax containing protected health information is sent by the practice, a request for confirmation of correct recipient is faxed first and no information is sent until a response is received.

In addition to the cybersecurity coverage through NAS provided in SVMIC’s medical professional liability policy, there are other tools available to our policyholders. SVMIC has partnered with NAS to bring our policyholders access to NAS cyberNET. This site features monthly cybersecurity updates, webinars and online training and support. Access this site at https://www.svmic.com/resources/cyber-security. In addition, SVMIC’s Medical Practice Services offers consulting and training related to cybersecurity and HIPAA.

**All names have been changed.*

*** Cybersecurity coverage is subject to terms, conditions and exclusions not described in this article. The information contained in this article concerning cybersecurity insurance is intended to give you an overview of the coverage available. None of the information—including any policy or product description—constitutes an insurance policy or guarantees coverage. The policy contains the specific details of the coverages, terms, conditions and exclusions and coverage determination is made by the company at the time of a claim.*

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.