Phishing by Fax: Do Not Become a Victim

By Rana McSpadden, FACMPE

Scenario: It is Friday afternoon, and the physician is working on a stack of documents requesting his signature. Most are routine requests, but one in particular draws his attention. It is seemingly from a national pharmacy requesting the practice confirm an active patient and indicates it is pursuant to 45 CFR 164.508. His initial thought is “great; something else to sign.” Not having received a form like this before, he continues to review it with more scrutiny. The document has all the patient’s correct information as well as all the information for the practice. It then goes on to ask the physician to confirm the patient is/was under their care and to indicate if the patient “changed or switched to another provider”. There are additional grammatical and formatting errors on the form. At the bottom of the form, a request is made for the physician’s confirmation signature and additionally asks for the “clinical/office stamp” and notes this is mandatory. At this point, the physician reaches out to the claims attorneys at SVMIC for guidance.

Was the form legitimate? After the SVMIC claims attorney reviewed the document, the

answer was NO. In addition to the other red flags, a Google search of the fax and phone number did not relate to that pharmacy chain, neither local nor national. The physician was advised that the request was a form of phishing and to not sign or send it back, and that it would be best to destroy it.

While we generally relate phishing to email, we are starting to receive inquiries on similar faxes that follow much of the same tactics that phishing emails do. In Brian Johnson's April 2021 article Don't Take the Bait in 2021, he describes the objective of a phish attack to generally include ransomware, credential theft, fraud, and theft of intellectual property. Phishing relies on "human nature and social tendencies, tricking you into divulging sensitive information, clicking malicious links, downloading malware, and unknowingly enabling fraud." As with phishing emails, these phishing faxes "impersonate brands, companies, people, and processes you trust" … by playing on "emotional triggers that manipulate your social tendencies that include authority, urgency, fear, duty, and a desire to be helpful."[i] The faxes in question look to legitimately be from a trusted source and attempt to additionally give the fax some semblance of authenticity by referencing 45 CFR 164.508, which is a portion of the HIPAA Privacy Rule that addresses when authorizations are required and the general and core requirements for an authorization. Practices can generally trust requests coming from pharmacies for prescription verification, so this attempt utilizes those trusted processes to circumvent suspicion.

What are some red flags to watch for in these faxes? The first to scrutinize is the logo. Does the fax utilize the current logo? The fax referenced earlier does not include a logo, just the name of the pharmacy. Another red flag is that the phone and fax number do not utilize the same area code and no mailing address for the local pharmacy that should be sending the request is included, as would most typically be the case. Grammatical mistakes or strange wording is not as prominent as in the early days of phishing emails; however, it is still a good indicator that something is 'phishy', especially when the correspondence claims to be from a national chain. Watch for additional red flags in information that pharmacies generally do not request, such as requests for stamped signatures.

From a HIPAA standpoint, had this physician sent the fax back, it may have potentially been considered a breach of patient information since he would have disclosed patient information to an unintended party. HIPAA, however, is not the only concern when it comes to phishing faxes.

As we have seen over many years, healthcare is fraught with fraud and a physician signature is gold. Once these fraudsters have a signature and NPI, they can conduct all sorts of insurance fraud. They could potentially write prescriptions for drugs or bill for medical devices or procedures that patients do not actually receive. When the fraud is finally identified, providers who unknowingly provided their signature and NPI may be included in the investigation until they are able to prove they were not part of the fraud.

Just as the physician referenced at the beginning of this article, be on the lookout for anything suspicious or out of the ordinary. In other words, question everything. Look for

indicators that something may not be right with the request you are reviewing. Never call the number indicated on the form, but instead, research the number to see if it goes where you expect. A little bit of research and a lot of suspicion can go a long way in making sure you are not a victim of phishing.

If you experience a potential cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and asking to speak to the Claims department.

[i] https://www.svmic.com/resources/newsletters/268/dont-take-the-bait-in-2021
