Sit Up and Take Notice

By: William Palisano, Lincoln Archives

Fact: Per Eva Velasquez, CEO of the Identity Theft Resource Center in San Diego "Last year there were 1.85 million victims (of Medical Identity Theft) in the U.S., up 25% from the year before."[1]

Fact: Per Don Jackson, a researcher with Dell SecureWorks who has been tracking what he called "a surge" in medical identity theft: "A criminal puts together what is called a "kitz"- which includes a valid health insurance card, a supporting photo I.D. (usually a driver's license in the health cardholder's name but with the fraudster's picture), possibly even a credit card in the same name. That kitz, said Jackson, lately has been selling in online criminal bazaars for $1,200 and up - with most sellers taking Bitcoin, by the way, for buyers who want real anonymity."[2]

Fact: Per 'Security Week' (Internet and Enterprise Security News, Insights and Analysis): "These underground markets also sell health insurance credentials, which include the names of those covered by the plan, dates of birth, contract number, group number, type of plan (individual, group, HMO, PPO, etc), deductible, and co-pay, and insurer contact information, for $20 each. Additional services, such as dental, vision, and chiropractor plans, are available as add-ons for $20 each, the researchers found."[3]

According to Jackson, "there is a vast supply of health I.D. credentials on the market, much of it a result of data breaches in doctors' offices and small hospitals."[4]

OK, so despite everyone's efforts to protect PHI, that information is still getting out. As late as a few weeks ago, medical files were found in a dumpster outside Behavioral Health Network in Springfield, Mass. Per BHN Vice President Candace Darcy: "...that is absolutely against policy and we'll need to do an investigation to figure out how that happened."[5]

Even last week, Headlines: "Files with Sylvan Learning Center clients' information found in dumpster." (Beaverton, Oregon). Per Sylvan Learning Center branch owner Tom VanHouten: "They should have been, and were intended to have been shredded," said VanHouten. "But I wasn't here, and when the files were purged, they were put into a recycling box and out the door they went."[6]

So, these show that a VP in one case and an owner in the other case refer to a 'policy' in one case and a 'procedure' in the other. Unfortunately neither was followed. We work with many medical entities. Some have policies and procedures clearly written out in protecting PHI whether saved in medical files, or electronically; and these are 'taught' to every employee. Others have a 'loose' outline of what to do to protect the PHI , and 'loosely' explained to employees. Some had no real outline, and expected employees to use common sense in protecting the PHI that they touched.

To protect your practice, you MUST have policies and procedures in place and documented. You MUST communicate those policies and procedures to every employee that touches (or could potentially touch) PHI.

You should also document whatever training you do. Better yet, have each employee sign off that he/she was communicated/trained on proper handling and protection of your firm's PHI. (I don't have unlimited real estate here, so I'll only address 'discarded information'. I'm not even going to go into potential risks from your vendors/landlords/BA's who have access to your facilities and information infrastructure. Perhaps an upcoming article...).

Lastly, the best policies are useless if they are not enforced. Someone (practice administrator, office manager, HIM) must do some audits and spot checks. Yes, it's messy work to look through waste bins, trash cans and recycling totes. And nobody wants to do it. But, it must be done. (Especially look at recycling bins/toters; they are the biggest source of risk, based on twenty years of my experience. Some employees just don't get it: recycling services and document shredding services are not the same thing. One takes paper off of your hands, sells it and get's it back into circulation. The other destroys your information and protects your firm and patients.) That is the only way you'll know that your employees/team members are following procedures. You might find something that you don't like. But, better you find it and correct it instead of either DHHS or the six o'clock news...

[1]Robert McGarvey: "This Trend In Medical Identity Theft is Disturbing" published by MainStreet.com
[2]Robert McGarvey: "This Trend In Medical Identity Theft is Disturbing" published by MainStreet.com
[3]Fahmida Y. Rashid: "Cyber-criminals Selling Complete ID Theft 'Kitz' for Over $1,000 Per Dossier" published by securityweek.com
[4]Robert McGarvey: "This Trend In Medical Identity Theft is Disturbing" published by MainStreet.com
[5]ProperPHIDisposal.net (no author sited): "Medical Records were discovered in neighborhood dumpster in Massachusetts"
[6]katu staff writer: "Files with Sylvan Learning Center clients' information found in dumpster" published by katu.com