PHARMACY MARKETING GROUP, INC

Rx AND THE LAW

By Don. R. McGuire Jr., R.Ph., J.D.

This series, **Pharmacy and the Law**, is presented by Pharmacists Mutual Insurance Company and your State Pharmacy Association through Pharmacy Marketing Group, Inc., a company dedicated to providing quality products and services to the pharmacy community.

CYBERSECURITY

Cybersecurity continues to make the news and to be a source of concern for all business owners. The recent WannaCry ransomware attack affected companies and governments in more than 150 countries. Data breaches and cyberattacks also occur in healthcare. In Rhode Island, the car of an employee of the state's largest health network was broken into and a laptop was stolen. The laptop contained sensitive information on about 20,000 of the network's patients. A healthcare provider in Texas had an unencrypted hard drive stolen. The hard drive contained information (e.g., social security numbers, dates of birth, driver license numbers, insurance information, etc.) about its patients going back to 2009. It is critical for pharmacies to assess their data security and take steps to strengthen it.

Stronger regulations are sure to come, but improvements to your data security now will minimize the chances that your pharmacy ends up as your community's lead news story. As an example, the New York Department of Financial Services recently promulgated new rules for cybersecurity of financial institutions.[1] This includes banks, insurance companies, and other financial services institutions. It does not apply to health care organizations or entities. The regulations contain 15 requirements for a cybersecurity program. This article will not review all of them, but will address some that apply to the situations we have already seen.

The regulations require penetration testing and vulnerability assessments. This would mean at least annual testing of firewalls and other portions of the overall cybersecurity program. This should alert you to any shortcomings in your security and give you the opportunity to remedy them before an incident occurs.

Also required is training and monitoring for your system's users. Training is an integral part of a security program because a leading cause of data breaches is the people using the system. Phishing attacks and similar techniques succeed because they fool a

1 23 NYCRR 500.00 to 500.23

user into allowing unauthorized access to the pharmacy's data.

Encryption is another important tool and New York's regulation is going to require it. The regulation requires that data be encrypted both while being transmitted (such as by e-mail) and also while resting on hard drive. This requirement would help secure data that is physically taken, such as in the stolen laptop or server examples. Many people think to encrypt data while it is in transit, but steps should also be taken while it is being stored.

The regulation also requires that organizations periodically dispose of sensitive information no longer needed for business operations. This will require the organization to assess the need to retain sensitive information and then follow their own policies and procedures to securely dispose of unneeded information. This action may have mitigated the damage done when the hard drive containing seven years of data was stolen in Texas.

The world continues to move toward more virtual and digital realms, so these challenges are not going away. Dealing with data breaches is expensive. Some studies estimate around $200 per record affected. For the data of those 20,000 patients on the laptop, this equates to around $4 million. And this doesn't take into account your reputational damage. The pharmacist-patient relationship is built on trust and data breaches will seriously damage these relationships. Ransomware can also be devastating to your pharmacy. Having your system held hostage until you pay the ransom (or can re-construct your system from back-ups) will, at a minimum, inconvenience your patients. It may cause them to question whether they should share their personal information with you.

There is no reason to wait for a law or regulation to be passed before shoring up your data security. You are already holding sensitive patient information and there are already numerous threats out there in cyberspace. A cyber incident can cause significant financial and reputational damage to your practice. This is not the time to take an ostrich approach to your data security.

This article discusses general principles of law and risk management. It is not intended as legal advice. Pharmacists should consult their own attorneys and insurance companies for specific advice. Pharmacists should be familiar with policies and procedures of their employers and insurance companies, and act accordingly.