THIN ICE AHEAD
Reach of 1996 HIPAA law still being felt

by Harry A. Lattanzio, RPh
and Joshua Potter

The headlines proclaim it—HIPAA has come roaring back with a vengeance and plaintiffs’ attorneys have your pharmacy in their crosshairs.

“Walgreen Case Opens Door For State Law HIPAA Claims”

“HIPAA Settlement May Herald New HHS Offensive”

“HIPAA Settlement Continues to Emphasize the Importance of Security Policies and Procedures”

“HIPAA Doesn’t Preempt Negligence Claims—Connecticut High Court”

“Provider Beware: HIPAA and State Privacy Laws May Inform Negligence Suits”

“Connecticut Ruling Expands HIPAA Liability For Medical (Healthcare) Providers”

And the list goes on.

These articles, many written by legal experts, are a warning that pharmacy owners need to take a closer look at their compliance with the existing HIPAA rules and the new enforcement landscape. This article will extract a few pearls of wisdom and lessons from those headlines, take a closer look at why after almost 19 years HIPAA is back on the pharmacy industry radar, and why pharmacy owners need to be concerned.
Several recent rulings by state courts and the Department of Health and Human Services Office of Civil Rights (OCR) have dramatically increased liability for covered entities, including pharmacies, and their business associates under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. We’ll address a number of these issues, and we have provided our contact information at the end of the article for those seeking more detail and clarification on any of the topics discussed here.

FAR-REACHING IMPLICATIONS
The first case we’ll look at is sure to have far-reaching implications for HIPAA-related lawsuits going forward. A Connecticut provider disclosed the protected health information (PHI) of a patient pursuant to a subpoena, but did not follow the proper HIPAA procedures while doing so. Consequently, the patient sued under state law using HIPAA as the “standard of care,” since she had not been notified that the provider had been subpoenaed and planned to comply and had previously requested her PHI not be handed out without her consent.

The Connecticut Supreme Court sided with her and recently ruled that HIPAA does not prevent individuals from bringing claims under state law against providers that have exposed their PHI, and that patients can sue for negligence if providers violate HIPAA regulations designed to protect a patient’s confidentiality. This is a huge—and distressing—change because, heretofore, individuals were not permitted to file a lawsuit claiming violations under the HIPAA regulations because HIPAA, itself, doesn’t provide individuals with a way to sue when their rights are violated. Instead, HIPAA is enforced by OCR, and OCR addresses any violations.

Daniel J. Solove, a George Washington University law professor, explained, “Even though HIPAA lacks a private right of action, plaintiffs can still use HIPAA to establish a duty or standard of care under state common law. That means that the requirements of HIPAA can readily become the basis of a lawsuit, as there are many common law causes of action (such as negligence) that can be used to bring lawsuits for privacy and data security incidents.”

As a claim of “you violated HIPAA” doesn’t work, attorneys have been looking for a way to sue for HIPAA violations. This case potentially creates a way for them to do just that.

Connecticut now joins several other states (Tennessee, Missouri, Delaware, Indiana, and West Virginia among them) that have similar rulings that stipulate HIPAA as a
basis in establishing the “standard of care.” We can expect other states to follow suit. Experts believe their respective courts will be hesitant to unravel years of negligence and other state law rulings by doing otherwise. These rulings will open the door for individuals to sue under state laws claiming violations of privacy using the HIPAA regulations as the “standard of care.” This is not good news for pharmacies, business associates, or any covered entity.

1. Has a computer virus or malware program ever appeared on any computer that houses or has access to protected health information (PHI) entrusted to your pharmacy?

2. Are you aware of the requirements for reporting breaches to the federal government and the patients subject to the breach, including timeliness and content?

3. Do you realize that the legal concept of respondeat superior applies to pharmacy owners? In essence, that every employer is liable and accountable for the negligent behavior of employees, including negligence of HIPAA regulations?

4. Did you perform a risk analysis to identify threats and vulnerabilities to e-PHI and your computer networks? Do you review and amend your risk analysis to address changes to your systems and personnel?

5. Do you have a documented disaster recovery plan that is practiced and is periodically updated at least once a year?

6. Are all of your business associate agreements updated to comply with the new requirements put in place on Sept. 22, 2014?

7. If your pharmacy fails to give a patient the Notice of Privacy, is it permissible to wait and give it to that patient on another visit?

8. Are your written HIPAA policies and procedures (P&Ps) customized to your pharmacy?

9. Is everyone in the pharmacy actually following your written P&Ps?

RISK ASSESSMENT IMPORTANT

Another case reported in a recent OCR bulletin ended in a settlement that emphasizes the importance of compliance with the Security Rule. An Alaska provider reported a breach of unsecured electronic protected health information (e-PHI) caused by malware—scary, since malware attacks are often in the news and have impacted most of us at one time or another. Upon investigation, OCR found that the provider “failed to conduct a thorough risk assessment, failed to implement Security Rule policies and procedures, and failed to implement technical security measures to protect e-PHI through the use of firewalls and regularly supported and updated software.” The provider agreed to pay $150,000 and adopt a corrective action plan to address compliance with the HIPAA Security Rule. OCR further stated that “although the provider had adopted sample Security Rule policies and procedures, it failed to follow those policies and procedures.” The OCR report underscored the importance of having an ongoing procedure to conduct risk assessments and to update and revise them based on finding additional threats.

This next OCR ruling may signal an expansion of OCR’s campaign against those providers who, in OCR’s view, may not be taking their HIPAA responsibilities seriously enough. A provider paid a $150,000 fine to settle claims that it violated the privacy, security, and breach notification rules of HIPAA after an unencrypted thumb drive containing e-PHI was stolen from the locked vehicle of one of its employees. This provider was the first to be fined for failure to have policies and procedures in place to address the breach notification provisions of HITECH. Lose a laptop with unencrypted PHI, forget to erase the hard drive of a leased or disposed office copier and/or fax machine used for PHI, and you could wind up paying a similar settlement to OCR.

“An ounce of prevention is worth a pound of cure” now takes on a whole new urgency where HIPAA is concerned. These OCR settlements were both preventable had the providers put into place a compliant, easily updateable version of the required HIPAA and HITECH policies and procedures (P&Ps); trained employees properly on those specific P&Ps (general, off-the-shelf, HIPAA training does not meet the requirements); and actually followed the P&Ps as written.

And now for the ruling that will make you cringe. An Indiana Superior Court jury decision cost the Walgreen Company $1.44 million when one of its pharmacists violated HIPAA. It is the first appellate court decision in which a provider has been held liable for violations of HIPAA committed by an employee.

www.americaspharmacist.net
EMPLOYERS HELD ACCOUNTABLE FOR EMPLOYEE ACTIONS

The suit against Walgreens claims that because the pharmacist's actions violated HIPAA, the pharmacist had breached the “standard of care” and should therefore be held liable for the harm caused. And, because the pharmacist had acted within the scope of her employment, it was argued that Walgreens also was liable for the pharmacist’s actions. The lesson here is that sometimes courts do hold employers liable for an employee’s actions, even if the employer didn’t do anything wrong. In this case, the court referenced the legal doctrine of “respondeat superior,” which holds that, in many circumstances, an employer is responsible for the actions of employees performed within the course of their employment. Thus, employers are vicariously liable, under the “respondeat superior” doctrine, for negligent acts or omissions by their employees.

The Walgreen Company’s decision to appeal this ruling has created a precedent for courts nationwide that privacy breach victims may hold employers accountable for the HIPAA violations of their employees. The message to providers: implement the required HIPAA policies and procedures, be sure your employees are properly trained, and keep both up to date.

As HIPAA continues to receive attention from attorneys seeking to use the regulation to establish the “standard of care” in cases involving the improper disclosure of PHI, providers must be aware that, depending on the law of the state in which they are licensed, their potential liability for HIPAA violations could extend far beyond just fines by OCR. It is clear from these decisions that attorneys are becoming more sophisticated in using HIPAA and other state privacy laws as tools for suing providers. NCPA emphasizes the importance of providers staying informed on legal decisions related to privacy and security to ensure that appropriate policies and procedures are in place and that those policies and procedures do not become obsolete, increasing the potential legal risks. It is critical to reduce this risk because the cost of a legal defense in these cases can be quite high. And, the bad press could be even more costly.

STRONG HIPAA COMPLIANCE PROGRAM ESSENTIAL

Attorneys advise covered entities, including your pharmacy, to have a robust and effective HIPAA compliance program to help avoid state law claims altogether. This removes a plaintiff’s ability to allege that the “standard of care” had been violated. If your employees are appropriately trained on the technical requirements of uses and disclosures and are strictly following the rules of HIPAA, then you have done what you can to minimize your risks. It is important not to let your set of P&Ps go stagnant. The law, as you can see, is constantly changing, just like your business. The P&Ps and your employees need to change as well.

Not sure if your pharmacy is compliant? It is a disturbing fact that a vast majority of independent pharmacy owners think they are HIPAA compliant and following the employee training requirements, when, in reality, most are not. Take the compliance survey at http://prspharmacyservices.com/compliance-survey/ and see how your pharmacy measures up. If you don’t like the results, take some action. Not doing so, as you have seen, could become very costly, very quickly.

Providers with questions about these cases or compliance with HIPAA laws should contact the authors, Harry A. Lattanzio, RPh, or Joshua Potter, at 800-338-3688, or visit www.prsrx.com or their own privacy counsel.

It is clear from these decisions that attorneys are becoming more sophisticated in using HIPAA and other state privacy laws as tools for suing providers.