Many psychologists are following the health care world’s general shift to maintaining protected health information (PHI) in electronic form (ePHI). The greater portability and accessibility of ePHI, while advantageous, may increase the risk of unauthorized persons gaining access to protected health information and violating the Privacy Rule under the federal Health Insurance Portability and Accountability Act (HIPAA).

HIPAA calls this unauthorized access a “breach.” The HIPAA Breach Notification Rule¹ requires HIPAA-covered psychologists to alert patients in the event of a breach of PHI. Many psychologists are aware of the HIPAA rule. Fewer are aware that 41 states have their own laws that also apply to breaches.

This article focuses on those laws and what additional obligations or penalties (beyond the HIPAA rule) those state laws pose for psychologists if they have a breach.

The law in your state

As noted in the chart on page 7, psychologists in nine states are not subject to any state breach notification laws and therefore need only follow HIPAA requirements. Of the 41 states with breach notification laws, only 16 impose additional breach notice requirements or penalties on psychologists beyond the requirements of HIPAA. In many of those 16 states, psychologists can avoid the additional state requirements or penalties by removing from their patient records “identity theft” information like social security numbers (SSN). Only seven states specifically protect “medical” information through their breach notification laws, while all states protect government identification and financial information. The reason is that state laws are primarily aimed at data breaches that can give rise to identity theft and other financial harm – as opposed to HIPAA’s focus on protecting the privacy of health information.

The 16 states, plus D.C., identified in the chart that impose additional requirements most often require additional notifications to the state attorney general and consumer credit reporting agencies. Florida, New Jersey and Vermont provide examples of the different types of breach laws seen in these states.

A psychologist who complies with HIPAA requirements will be in compliance with Florida’s breach notification law with two potential exceptions.² First, if more than 500 patients are affected by a given breach, the psychologist must notify the Florida Department of Legal Affairs within 30 days of discovering the breach. Second, if more than 1,000 patients are affected, the psychologist must also notify the national consumer credit reporting agencies.

Like Florida, New Jersey requires notification to consumer reporting agencies in the case of a breach affecting more than 1,000 people. However, New Jersey requires psychologists to report any breach, without regard to the number of patients affected, together with “any information pertaining to the breach,”³ to New Jersey’s Division of State Police in the Department of Law Enforcement and Public Safety. This must be done before any notification is made to the public.

Vermont has one of the most detailed and demanding state breach notification laws. Fortunately, it only requires three significant additions to HIPAA.⁴ First, psychologists must notify affected patients of a breach within 45 days of discovery, instead of HIPAA’s 60-day requirement. Second, the state attorney general must be notified within 14 days of discovery of the breach or when affected patients are notified.

---

whichever is sooner. Finally, if more than 1,000 patients are affected, the psychologist must notify the national consumer credit reporting agencies.

**Protected information**

Understanding what information is protected under state law (in addition to HIPAA) is important. HIPAA and state laws generally define a breach as unauthorized access to legally protected information. State breach laws use the term “personal information,” while HIPAA uses the term “protected health information” (PHI). The definition of protected information is split into two components, format and content. Format refers to the way the information is stored (such as encrypted and de-identified), while content refers to the type of information (such as name and SSN).

The format component is consistent across federal and state laws. HIPAA and all state breach notification laws apply only to “unprotected” information – patient information that is not maintained or transmitted in an encrypted or de-identified format. Therefore a breach of encrypted data need not be reported unless the encryption key (most often a password) is part of the lost data. Many states also specifically exclude sufficiently redacted data from breach notification requirements – for example, in Virginia, a SSN showing five or fewer digits. Redacting data involves removing or deleting sensitive information from a document prior to releasing it. The details of such requirements vary by state, so it is important that psychologists check their state laws.

HIPAA defines PHI as individually identifiable health information that (1) relates to the past, present or future physical or mental health condition of a patient; providing health care to a patient, or the past, present or future payment for the patient’s health care; (2) identifies the patient or could reasonably identify the patient; and (3) is transmitted or maintained in any form or medium. This definition of the content of PHI is expansive under HIPAA.

By contrast, the content component of protected health information varies across states. Many states’ definitions of protected information require there to be a first name or first initial, last name and one or more additional elements such as government ID number or financial information. Government ID numbers always include a patient’s SSN and state driver’s license number, with some states including passport numbers or other additional information. Financial information is generally defined as some combination of financial account numbers and password information sufficient for unauthorized use or access.

---

5 VA. CODE ANN. § 18.2-186.6(A) (2014).
State breach notification laws were originally motivated by concerns of identity theft and financial fraud. As noted previously, all state breach laws protect government ID and financial information, while only seven states specifically protect “medical” information. Those states define medical information in generally the same manner as HIPAA defines PHI. Apart from government ID, financial information and medical information, some states include biometrics, tax information and even mother’s maiden name. Georgia and Oregon protect “any combination” of listed information sufficient to perform or attempt identity theft, without requiring a patient’s name to be part of the data for it to be deemed protected information.

Even in those states that do not include medical information in the definition of protected information, the state breach law will apply if your patient record contains both patient names and a unique government ID number, such as SSN or state driver’s license number. (See Recommendation 2 on page 9.)

HIPAA breach notification requirements

The HIPAA Breach Notification Rule sets forth standards and requirements that providers must follow in the event a breach of patient data is suspected. These requirements are covered in detail in The HIPAA Final Rule: What You Need To Do Now resource available to members of the APA Practice Organization at apapracticecentral.org/update/2013/07-25/secure/hipaa-final-rule.pdf. In brief, however, HIPAA requires psychologists to notify affected patients of a breach of PHI “without unreasonable delay” and in no case later than 60 days after discovery, setting out detailed rules for what the notification must contain and how it must be made. HIPAA also includes detailed requirements for notifying the Secretary of HHS.

1 HIPAA Data Breaches on the Rise (April 14, 2015), MEDPAGE TODAY http://www.medpagetoday.com/MedicalNews/HIMSS/50983
If notifying by email, the psychologist would need to obtain prior patient consent for email communications as required by federal or state law.

**Penalties**

The potential penalties for violation of a breach notification law vary greatly between the states. Civil penalties are the most common, followed by liability for actual damages and court costs, and then criminal liability in a number of states. Some states impose a combination of all three.

Civil penalty provisions vary by state. For example, Alaska’s maximum civil fine is $50,000 per breach incident whereas the maximum in Texas is $300,000. Louisiana imposes no penalty except to allow patients whose information was compromised to sue for actual damages resulting from the breach. Arkansas, by contrast, punishes knowing and willful violation of its breach notification law as a Class A misdemeanor, a criminal charge which would likely have to be reported to the psychology licensing board.

**Recommendations**

Consider the following recommendations for minimizing the risks associated with breach notification laws.

1. **Encrypt data stored on mobile devices**

   Federal and state breach notification laws do not apply to encrypted data because encryption converts the data into a “scrambled” format that is difficult for unauthorized users to decode. While encryption of an entire computer system may be daunting, it is possible to encrypt a file or folder on your computer or tablet to protect ePHI in case the device is lost or stolen. Refer to the article “ABCs and 123s of Encryption” in the Spring/Summer 2014 issue of the APA Practice Organization’s Good Practice magazine for more information about encryption and different types. The National Institute of Standards and Technology guide on encryption, available at [1.usa.gov/1FDQPx9](http://1.usa.gov/1FDQPx9), may also be a helpful resource. A consultation with an IT professional may help you weigh your options and decide how best to use encryption to your advantage.

2. **Limit the patient information you put in the record**

   Many states’ breach notification laws protect a narrow definition of personal information, such that excluding basic elements like SSN and driver’s license numbers may be enough to avoid triggering state requirements. Consult with your attorney or professional liability company on the details of what information is protected under your state’s law and adjust your record-keeping accordingly, if possible.

3. **Make notifying patients easier for yourself**

   Many states, and HIPAA, allow notification via email but require prior notice or consent from the patient. Obtain the necessary consent from new and existing patients now to reduce potential breach notification costs in the future.

4. **Consult with an attorney or professional liability company to confirm you are in compliance with HIPAA and state law.**