THE WASHINGTON STATE DATA BREACH NOTIFICATION ACT (RCW 19.255.010)

Significant Changes Health Care Providers Need to Know

By Stephen D. Rose

The improper release of protected health information (PHI) information should trigger a risk assessment to determine whether the release of that information constitutes a "breach" under HIPAA.[1] Most states also have a state law to protect "personal information." If the improper release of medical information is sufficient to trigger a HIPAA risk assessment, it is usually also sufficient to trigger an assessment under state law. In Washington State the statute is known as the Data Breach Notification Act (DBNA).

Beginning July 24, 2015, there will be significant changes in the DBNA that health care providers need to know. Fortunately, the new version of DBNA exempts Covered Entities under HIPAA and deems that if the Covered Entity is in compliance with HIPAA, they are also in compliance with DBNA. However, the reason why it is important for health care providers to be aware of the changes to DBNA is that there may be instances where personal information that is not PHI is improperly released, such as the mistaken release of employment records that contain personal information. This type of breach of personal information that is not PHI would require a breach analysis under the DBNA, but not under HIPAA.[2] If you mistakenly apply the HIPAA deadlines instead of the DBNA deadlines, you may run afoul of the law where DBNA requires a quicker response than does HIPAA. This paper details some of those changes.

TYPE OF INFORMATION COVERED

Originally, DBNA only applied to computerized data containing unencrypted[3] personal information.[4] Coverage by DBNA has expanded greatly so that it now applies to all data including hard copy data in addition to computerized data that is not "secured."[5] Both HIPAA and DBNA apply the same standard for encryption, which is the NIST standard or other process that makes the data "unusable, unreadable or not decipherable."[6]

BREACH DEFINITION AND STANDARD OF REVIEW FOR DETERMINING BREACH

Under DBNA the improper release of personal information requiring breach notification occurs where the personal information released is "reasonably likely to subject consumers to a risk of harm."[7] The security of a system is breached with the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of the personal information.[8] This standard of review under DBNA looks remarkably similar to the "risk of harm standard" originally used by HIPAA that was abandoned in 2013. Good faith acquisition of personal information by an employee or agent of the business maintaining the personal information is not considered to be a breach of the security of the system when the personal information is not used or the subject of further unauthorized disclosures.[9]

Stephen D. Rose
srose@gsblaw.com
206.816.1375

BREACH NOTIFICATION

Under DBNA, if the Business Entity determines that a breach has occurred, written notification must be provided to the affected individuals just as with HIPAA. However, DBNA differs from HIPAA in three significant ways. First, DBNA allows the written notification to be provided to the affected individuals either by first class mail or, under some circumstances, by email.[10] HIPAA requires that the notification be by first class mail unless the affected individual has agreed to electronic notice.[11]

Second, the notification must be sent to the affected individuals without unreasonable delay, "No more than forty-five calendar days after the breach was discovered.[12] HIPAA also requires notification without unreasonable delay, but sets the deadline at 60 days after the breach was discovered.[13]

Third, if the Business Entity is required to issue a notification to more than 500 Washington residents as a result of a single breach, the Business Entity must submit, electronically, a single sample copy of the breach notification, excluding any personally identifiable information, to the Washington State Attorney General.[14]

NOTICE CONTENTS

The prior version of DBNA required that written notice be given for a breach, but did not detail what information needed to be included in that written notice.[15] The new version of DBNA now defines the content for the written notice. The written notice must be written in plain language and include the name and contact information for the Business Entity responsible for the breach. It must also include a description of the types of personal information believed involved in the breach and the toll-free phone numbers and addresses for the major credit reporting agencies.

CONCLUSION

It is not the purpose of this paper to point out each and every difference between HIPAA and DBNA, only some of the more significant changes brought about by the changes in DBNA set to become effective on July 24, 2015. As always, the specific facts of any situation can impact the analysis under HIPAA and DBNA. You should contact your own legal counsel to discuss your specific issues.

---

[1] HIPAA refers to the Health Insurance Portability and Accountability Act of 1996, Public Las 104-191. All of the HIPAA rules are located at 45 CFR Parts 160, 162, and 164. The last major modification of the HIPAA rules occurred in 2013 with the publication of the HIPAA Omnibus Rules, 78 Fed. Reg. 5566 (January 25, 2013) ("HIPAA Omnibus Rules").

[2] With respect to breaches that involve PHI, the DBNA provides that if the health care provider (covered entity) complies with HIPAA/HITECH, they are deemed to be in compliance with the DBNA.

[3] While the statute on its face stated that it applied to "unencrypted" personal information, it did not define what constitutes "encryption" or "unencrypted" data. As detailed below, these terms are now defined.

[4] As originally defined, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (a) social security number; (b) driver's license number or Washington identification card number; (c) account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. RCW 19.255.010 (5). As detailed below, this definition has had some minor changes made to it.

[5] RCW 19.255.010 (1).

[6] RCW 19.255.010 (7); 74 Fed. Reg. 19006.

[7] RCW 19.255.010 (1).

[8] RCW 19.255.010 (4).

[9] Id.

[10] RCW 19.255.010 (8).

[11] 45 CFR § 164.404 (d)(1).

[12] RCW 19.255.010 (16).

[13] 45 CFR § 164.404 (b).

[14] RCW 19.255.010 (15).

[15] RCW 19.255.010 (14).