Ohio | Department of Insurance

Mike DeWine, Governor
Jon Husted, Lt. Governor

Jillian Froment, Director

50 West Town Street
Third Floor – Suite 300
Columbus, OH 43215-4186
(614) 644-2658
www.insurance.ohio.gov

The Ohio Department of Insurance (ODI) believes safeguarding consumer's nonpublic information is paramount for any licensee when conducting business with Ohio consumers. Ohio has long required licensees to follow reporting and mitigation procedures when data loss does occur. (R.C. 3904.13, Bulletin 2009-12 (Loss of Control of Policyholder Information).) Recently enacted R.C. Chapter 3965 bolsters data loss reporting requirements and adds a requirement for some licensees to develop and maintain an information security program. Below you will find some key obligations of this new law, initial guidance regarding the HIPAA exemption, and information on forthcoming guidance.

R.C. Chapter 3965. New Obligations for Licensees

Some key new requirements include:

- All licensees are required to develop, implement, and maintain a comprehensive information security program based on a risk assessment (R.C. 3965.02). This program should reflect the size and complexity of the organization. There are exemptions to having an information security program that can be found in R.C. 3965.07.
- A licensee shall exercise due diligence in selecting its third-party service provider (R.C. 3965.02 (F)).
- All licensees are required to notify the superintendent as promptly as possible after a determination that a cybersecurity event involving nonpublic information has occurred, but in no event later than three business days after that determination (R.C. 3965.04).

The above highlights only a few key requirements. Licensees should review R.C. Chapter 3965 in its entirety.

Additional information is forthcoming on the methods and deadlines for certifying to the presence of an information security program. In addition, ODI will be reviewing and updating the existing bulletin on reporting the loss of consumer nonpublic data to incorporate these new obligations.

Information Security Program Exemptions/Guidance for HIPAA Exemption

One of the exemptions to having an information security program is commonly referred to as the "HIPAA" exemption.

R.C. 3965.07 (B) (1) states:

> "A licensee subject to and in compliance with the privacy and security rules of 45 C.F.R. Parts 160 and 164 shall be deemed to meet the requirements of this chapter, except those pertaining to notification under section 3965.04 of the Revised Code. The licensee shall submit a written statement to the superintendent certifying its compliance with 45 C.F.R. Parts 160 and 164."

We are aware that some licensees may already be in compliance with the HIPAA privacy and security rules and therefore wish to certify now. You may do so by completing the attached form and emailing it to INSINFOSEC@insurance.ohio.gov.

It is important to note that claiming the HIPAA privacy and security rule exemption only exempts a licensee from Section 3965.02 regarding information security programs. Licensees certifying an exemption are still obligated to report a loss of consumer nonpublic information as required in Section 3965.04.

Additional guidance on the remaining exemption statuses and their application is forthcoming.

Future Guidance and Information

We will be placing this information and all future guidance related to information security on the ODI website. On the website, you will soon be able to; find useful tools such as checklists and FAQ's, sign up to receive updates, contact us with questions; and electronically submit a data loss/breach notification.

We would encourage all interested parties to sign up for updates through our Information Security Resource Center web page.

If you have any questions please email them to INSINFOSEC@insurance.ohio.gov.