Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Ohio

Ohio Rev. Code, 1347.12, 1349.19

H.B. 104 (signed into law Nov. 17, 2005), amended by S.B. 126 (signed into law Dec. 29, 2006)

Effective February 17, 2006 (amendment to exclude "covered entities" under HIPAA effective March 30, 2007)

Application. Any individual, corporation, business trust, estate, trust, partnership, or association (collectively, Entity) that conducts business in OH and owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of PI owned or licensed by an Entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of OH.

- Good faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.
- Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system to any individual whose principal mailing address as reflected in the records of the Entity is in OH and whose PI was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Notification to Consumer Reporting Agencies. If an Entity notifies more than 1,000 residents of OH, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notice.

- This requirement does not apply to HIPAA covered entities.

Third-Party Data Notification. Any Entity that, on behalf of or at the direction of another Entity or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes PI shall notify that other Entity or governmental entity of any breach of the security of the system in an expeditious manner, if the PI was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of OH.

Timing of Notification. In the most expedient time possible but not later than 45 days following discovery or notification of the breach in the security of the system, consistent with any measures necessary to determine the scope of the breach, including which residents' PI was accessed and acquired, and to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following that are widely distributed:

- Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television, or any type of media similar in nature;
- Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to any bona fide newspaper, journal, magazine, radio or television news media, or any types of media similar in nature; or
- Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation, or any type of media similar in nature.

Notice Required. Notice may be provided by any of the following methods:

- Written notice;
- Telephonic notice; or
- Electronic notice, if the Entity's primary method of communication with the resident to whom the disclosure must be made is by electronic means.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of subject residents to whom notification is required exceeds 500,000 persons, or that it does not have sufficient contact information to provide written, telephonic or electronic notice. Substitute notice under this division shall consist of all of the following:

- Email notice, if the Entity has an email address for the resident to whom the disclosure must be made;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of the population of OH.

Substitute Notice Exception. If the Entity demonstrates it has 10 employees or fewer and that the cost of providing notice will exceed $10,000. Substitute notice under this division shall consist of all of the following:

- Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the Entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for 3 consecutive weeks;
- Conspicuous posting of the disclosure or notice on the Entity's website if the Entity maintains one; and
- Notification to major media outlets in the geographic area in which the Entity is located.

Exception: Compliance with Other Laws.

- **Financial Institution.** A financial institution, trust company, or credit union or any affiliate thereof that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of the statute.

Exception: Preexisting Contract. Disclosure may be made pursuant to any provision of a contract entered into by the Entity with another Entity prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section.

Other Key Provisions:

- **Delay for Law Enforcement.** The Entity may delay the disclosure if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the Entity shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.
- **Attorney General Enforcement.** The Attorney General may conduct an investigation and bring a civil action upon an alleged failure by an Entity to comply with this statute.