

North Dakota State Law (NDCC 51-30-01 et seq) –breaches involving unencrypted personal information

Who must give notice of a breach and to whom?

Owners and Licensees of data that include personal information must notify state residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

If more than 250 individuals are impacted, the owner or licensee must also notify the Office of Attorney General.

Persons who maintain data that include personal information data must notify Owners and Licensees of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

What is the time frame for giving notice?

Owners and licensees must give notice “in the most expedient time possible and without unreasonable delay...” Delays due to legitimate law enforcement needs (eg, for a criminal investigation) or necessary to determine the scope of the breach and repair the data system are not unreasonable.

Persons who maintain data must notify owners and licensees immediately upon discovery of the breach.

How must notice be given?

Notice may be written.

Notice may be electronic if the individual to be notified has consented to receive electronic records.

If (a) the cost of providing notice would exceed \$250,000, (b) notice would need to reach more than 500,000 individuals, or (c) the notifying entity lacks sufficient contact information for affected individuals, substitute notice is acceptable. Substitute notice: email (to the extent email addresses are available), conspicuous posting on the notifier’s website, and notification to major statewide media.

Certain financial institutions and health care entities are deemed compliant with state law if they follow their industry-specific federal requirements for breach notification.

Persons who maintain and use their own notification procedures as part of their information security policies are deemed compliant as long as those procedures are consistent with the timing requirements of this state law.

Who enforces breach notification requirements?

The Attorney General

Possible enforcement actions include but are not limited to: injunctions, subpoenas, civil penalties (\$5000 per violation), recovery of investigation and enforcement costs,

Key Definitions:

1. Breach: generally defined as an unauthorized acquisition of computerized data when access to person information has not been secured by making it unreadable or unusable.
2. Personal Information: a person's first name or initial and last name in combination with any of several enumerated data elements (when the name and element(s) are not encrypted). Personal information does not include information that is lawfully available to the public.
3. Person: an individual, organization, government, political subdivision, or government agency or instrumentality.

Health Information Portability and Accountability Act (HIPAA) – breaches involving unencrypted protected health information

Who must give notice of a breach and to whom?

Covered entities (and, under Federal Trade Commission rules, certain electronic health record vendors) must notify affected individuals and the Department of Health and Human Services when there is a breach of their unsecured protected health information.

If more than 500 individuals in any state or jurisdiction are affected, the covered entity must also notify prominent media outlets in the relevant state or jurisdiction

Business associates must notify covered entities of a breach of unsecured protected health information

However, if a covered entity or business associate can demonstrate there is a low probability that the protected health information has been compromised – based on a risk assessment set forth by the Department of Health and Human Services – they do not need to provide notice. This is a high threshold to meet.

What is the time frame for giving notice?

Covered entities must notify affected individuals without unreasonable delay and in no case later than 60 days following the discovery of the breach.

For breaches affecting 500 or more individuals, covered entities must notify the media and Department of Health and Human Services without unreasonable delay and in no case later than 60 days following the discovery of a breach.

For breaches affecting fewer than 500 individuals, covered entities must notify the Department of Health and Human Services no later than 60 days after the end of the calendar year in which the breach occurred.

Business associates must notify covered entities without unreasonable delay and in no case later than 60 days following the discovery of the breach.

How must notice be given?

Notice to individuals may be by first class mail.

Notice to individuals may be electronic if the individuals have consented to receive electronic records.

Substitute notice must be given to individuals if a covered entity lacks current contact information for 10 or more individuals. Substitute notice in this case is given by posting it on the covered entity's home page for at least 90 days or by providing notice in major print or broadcast media where the affected individuals likely reside.

Substitute notice may be given to individuals if a covered entity lacks current contact information for fewer than 10 individuals. Substitute notice in this case may be given by some type of alternate written notice, by telephone or "other means".

Covered entities must use an electronic breach report form when notifying the Department of Health and Human Services.

Business Associate agreements should specify how a business associate should notify a covered entity.

Media notification will generally be in the form of a press release.

Who enforces breach notification requirements?

The Office of Civil Rights within the Department of Health and Human Services

The Office of Civil Rights can refer cases to the Department of Justice when there is a possible criminal violation of HIPAA.

Key Definitions:

Covered entities: health care providers who transmit electronic information in connection with certain transactions, health plans (including government plans) and health care clearinghouses

Business associate: a person or entity who provides services to a covered entity and creates, receives, maintains, transmits or accesses protected health information. A member of a covered entity's workforce is not considered a business associate of the covered entity.

Protected Health Information: generally, individually identifiable health information

Gramm-Leach-Bliley Act - breaches of financial institutions' sensitive customer information

GLBA requires certain financial institutions to develop security measures to protect customer information. The security measures must include response programs to deal with detected or suspected data breaches. Federal interagency guidance says response programs should include breach notification procedures. That guidance applies to financial institutions regulated by the Federal Reserve Board, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency or the Office of Thrift Supervision.

Who must give notice of a breach and to whom?

Financial institutions should notify customers of unauthorized access to and possible misuse of their sensitive customer information

Financial institutions should have contractual provisions requiring third-party service providers to have appropriate breach response programs that may include customer notification

Financial institutions should notify their "primary federal regulator" of incidents involving unauthorized access to or use of sensitive customer information

Financial institutions should notify appropriate law enforcement authorities of any breaches that qualify as "suspicious activities" under their Suspicious Activity Report regulations

What is the time frame for giving notice?

When an institution determines there has been unauthorized access to sensitive customer information and the institution determines misuse of the information has occurred or is reasonably possible, the institution should notify the affected customer(s) as soon as possible.

Customer notice may be delayed for criminal investigation(s) for as long as notification will interfere with the investigation(s).

Financial institutions should notify their primary federal regulator as soon as possible after becoming aware of the breach

How must notice be given?

Financial institutions must notify customers "in any manner designed to ensure that a customer can reasonably be expected to receive it."

Key Definitions:

Sensitive customer information: customer's name, address or telephone number in conjunction with one or more of several enumerated data fields - or any combination of data fields that would allow someone to access a customer's account

Family Educational Rights and Privacy Act (FERPA)

FERPA requires educational agencies and institutions to maintain the privacy and of personally identifiable information in education records but does not those agencies and institutions to undertake proactive breach notifications. Instead, educational agencies and institutions must record unauthorized disclosures of a student's personally identifiable information. The student (or his or her parent) may request an accounting of disclosures and thereby find out whether there has been a breach.

Educational agencies and institutions must follow any applicable state or other laws requiring breach notification.

The federal Department of Education issued guidance to educational agencies and institutions on establishing breach notification policies and procedures.