

UNC Greensboro

HIPAA BREACH NOTIFICATION PROCEDURES

1. Breach Notification Rule. The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates:

- 1.1 To provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, per the HITECH Act.
 - Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information, which is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.
- 1.2 Covered entities and business associates that secure information by encryption and destruction to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals are relieved from providing notifications following the breach of such information.

2. Definition of Breach

- 2.1 A breach is, generally, an impermissible use or disclosure under the HIPAA Privacy Rule that Compromises the security or privacy of the protected health information.
- 2.2 An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
 - a. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - b. The unauthorized person who used the protected health information or to whom the disclosure was made;
 - c. Whether the protected health information was actually acquired or viewed; and the extent to which the risk to the protected health information has been mitigated.
- 2.3 Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.
- 2.4. There are three exceptions to the definition of “breach:”
 - a. The unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.

UNC Greensboro

HIPAA BREACH NOTIFICATION PROCEDURES

- b. The inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized healthcare arrangement in which the covered entity participates.
 - In both cases above, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- c. If the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

3. Breach Notification Requirements

3.1. Individual Notice

- a. Covered entities must provide individual notice to all affected individuals in written form by first class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
- b. If the covered entity has insufficient or out-of-date contact information for 10 or more affected individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- c. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
- d. If the covered entity has insufficient or out-of-date contact information for fewer than 10 affected individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

3.2. Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible:

- a. A brief description of the breach
- b. A description of the types of information that were involved in the breach
- c. The steps affected individuals should take to protect themselves from potential harm
- d. A brief description of what the covered entity is doing to investigate the breach mitigate the harm, and prevent further breaches
- e. Contact information for the covered entity (or business associate, as applicable)

3.3. For a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate.

UNC Greensboro

HIPAA BREACH NOTIFICATION PROCEDURES

3.4. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual(s).

3.5. Media Notice

- a. Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.
- b. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected individuals.
 - Any press releases must be coordinated through the UNCG University Communications Department
 - Like individual notices, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

3.6. Notice to the Secretary

- a. Covered entities must also notify the Secretary of the Department of Health & Human Services of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form.
- b. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.
- c. If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary on an annual basis. Such reports are due to the Secretary no later than 60 days after the end of the calendar year in which the breach was discovered.

3.7. Notification by a Business Associate

- a. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach without unreasonable delay and no later than 60 days from the discovery of the breach.
- b. To the extent possible, the notification should identify each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals

4. Administrative Requirements and Burden of Proof

UNC Greensboro
HIPAA BREACH NOTIFICATION PROCEDURES

- 4.1 Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach.
- 4.2 Documentation should be maintained that all required notifications were made, or, alternatively, that notification was not required due to a risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure, or due to the application of any other exceptions to the definition of “breach”.
- 4.3 Covered entities are also required to comply with administrative requirements for breach notification. This includes:
 - a. Written policies and procedures regarding breach notification
 - b. Training for employees on such policies and procedures
 - c. Development and application of appropriate sanctions against workforce members who do not comply