HIPAA - Breach Notification Rule

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

Purpose

The purpose is to ensure that healthcare providers and health plans that qualify as HIPAA Covered Entities, and qualifying vendors and partners that qualify as HIPAA Business Associates, meet all the requirements defined in HIPAA and associated guidance.

Scope

This policy applies to the organization workforce members and business associates that access, process, or store verbal, written, or electronic Protected Health Information (PHI).

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

HIPAA §164.414(a) - Administrative Requirements

HIPAA - Breach Notification Rule	Other Requirements
§164.414(a) Administrative Requirements	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Administrative Requirements.

A covered entity is required to comply with the administrative requirements of the Breach Notification Rule.

[Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation]

Guidance
Has the covered entity adequately implemented the required provisions as they relate to the Breach Notification Rule? Inquire of management.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-1 - Administrative Requirements: Administrative Requirements. A covered entity is required to comply with the administrative requirements of the Breach Notification Rule. [Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation]

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(b) - Training

HIPAA - Breach Notification Rule	Other Requirements
§164.530(b) Training	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All workforce members must receive training pertaining to the Breach Notification Rule.

Guidance
Does the covered entity train its work force and have policies and procedures to ensure all members of the workforce receive necessary and appropriate training in a timely manner as provided for by the established performance criterion?

Obtain and review such policies and procedures. Areas to review include training each new member of the workforce within a reasonable period of time and each member whose functions are affected by a material change in policies or procedures.

From the population of new hires within the audit period, obtain and review a sample of documentation of necessary and appropriate training on compliance with the HIPAA Breach Notification Rule that has been provided and completed.

Obtain and review documentation that workforce members have been trained on material changes to policies and procedures required by the HITECH Act.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-2 - Training: All workforce members must receive training pertaining to the Breach Notification Rule.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(d) - Complaints to the Covered Entity

HIPAA - Breach Notification Rule	Other Requirements
§164.530(d) Complaints to the Covered Entity	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.

Guidance
Does the covered entity have a process in place for individuals to complain about its compliance with the Breach Notification Rule? Obtain the covered entity's policies and procedures for individual complaints. Evaluate whether they are consistent with the requirement to provide a process for individuals to complain about the covered entity's compliance with the Breach Notification Rule.

Has the covered entity received any such complaints? If yes, obtain and review a list of complaints received in the specified period and the disposition of such complaints. Obtain and assess additional documentation of actions taken by the covered entity to investigate and resolve the complaints. Assess whether the actions were completed in accordance with these requirements and the entity's policies and procedures.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-3 - Complaints to the Covered Entity: All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(e) - Sanctions

HIPAA - Breach Notification Rule	Other Requirements
§164.530(e) Sanctions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.

Guidance
Obtain and review entity policies and procedures to determine if the entity has and applies sanctions consistent with the established performance criterion. Evaluate whether they are consistent with the requirement to sanction a covered entity's workforce members.

Has the covered entity sanctioned workforce members for failing to comply with its policies and procedures as they relate to the Breach Notification Rule? Obtain and review documentation of the application of sanctions to a sample of breach notification incidents to determine whether appropriate sanctions were applied. (Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate sanctions consistent with the entity policies have been applied.)

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-4 - Sanctions: All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(g) - Refraining from Retaliatory Acts

HIPAA - Breach Notification Rule	Other Requirements
§164.530(g) Refraining from Retaliatory Acts	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must have policies and procedures in place to prohibit retaliatory acts.

Guidance
Does the covered entity have appropriate policies and procedures in place to prohibit retaliation against any individual for exercising a right or participating in a process (e.g., assisting in an investigation by HHS or other appropriate authority or for filing a complaint) or for opposing an act or practice that the person believes in good faith violates the Breach Notification Rule? Obtain and review such policies and procedures.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-5 - Refraining from Retaliatory Acts: All covered entities must have policies and procedures in place to prohibit retaliatory acts.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(h) - Waiver of rights

HIPAA - Breach Notification Rule	Other Requirements
§164.530(h) Waiver of rights	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Guidance
Does the covered entity have appropriate policies and procedures in place to prohibit it from requiring an individual to waive any right under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits? Obtain and review such policies and procedures. If patient or health plan member intake forms are used, obtain and review to confirm that such a requirement is not contained within them.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-6 - Waiver of rights: All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(i) - Policies and Procedures

HIPAA - Breach Notification Rule	Other Requirements
§164.530(i) Policies and Procedures	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.

Guidance
Does the covered entity apply appropriate sanctions to members of the workforce who fail to comply with the breach notification policies and procedures of the entity or the Breach Notification Rule?

Does the covered entity have policies and procedures that are consistent with the requirements of the Breach Notification Rule?

• Obtain and review the covered entity's policies and procedures for evaluating the appropriate action under the Breach Notification Rule when there is an impermissible use or disclosure of PHI.

• Obtain and review the covered entity's policies and procedures for providing notifications to individuals, the media (if applicable), and the Secretary.

• Obtain and review the covered entity's policies and procedures for requiring business associates to report an impermissible use or disclosure of PHI to the covered entity and the covered entity's process for handling such reports.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-7 - Policies and Procedures: All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.530(j) - Documentation

HIPAA - Breach Notification Rule	Other Requirements
§164.530(j) Documentation	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

All covered entities must have policies and procedures in place for maintaining documentation.

Guidance
Does the covered entity have policies and procedures for maintaining documentation consistent with the requirements?

• Obtain and review documentation that the covered entity maintains its policies and procedures, in written or electronic form, until 6 years after the later of the date of their creation or the last effective date.

• Obtain and review documentation that the covered entity maintains all other required documentation until 6 years after the later of the date of their creation or the last effective date.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- HBNR-8 - Documentation: All covered entities must have policies and procedures in place for maintaining documentation.

References
- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.402 - Definitions: Breach - Risk Assessment

HIPAA - Breach Notification Rule	Other Requirements
§164.402 Definitions: Breach - Risk Assessment.	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or privacy of the PHI.

Except as provided, an acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

Guidance
Has the covered entity implemented policies and procedures regarding the determination of whether an impermissible acquisition, access, use or disclosure, requires notification under the Breach Notification Rule?

Obtain and review a list of breaches, by date, that occurred in the previous calendar year. Obtain and review a list of security incidents, by date, that occurred in the previous calendar year. Obtain and review a list of breaches reported to HHS, by date, that occurred in the previous calendar year.

Does the covered entity have a process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised?
If not, does the covered entity have a policy and procedure that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI?

Obtain and review policies and procedures regarding the process for determining whether notifications must be provided when there is an impermissible acquisition, access, use, or disclosure of PHI.

If the entity does not have a policy and procedure that treats all potential breaches as requiring notifications without conducting a risk assessment, review the covered entity's risk assessment policies and procedures. Evaluate whether they require the covered entity to consider at least the following four factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification

(ii) The unauthorized person who used the PHI or to whom the disclosure was made

(iii) Whether the PHI was actually acquired or viewed

(iv) The extent to which the risk to the PHI has been mitigated.

Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined there was a low probability of compromise to the PHI. Obtain and review all documentation associated with the conduct of the risk assessments. Assess whether the risk assessments were completed in accordance with these requirements and the entity's policies and procedures.

Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification were required.

Obtain and review all documentation associated with the conduct of the risk assessments. Assess whether the risk assessments were completed in accordance with these requirements and the entity's policies and procedures.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- HBNR-9 - Definitions: Breach - Risk Assessment.: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or privacy of the PHI. (2) Except as provided, an acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and (iv) The extent to which the risk to the PHI has been mitigated.
- HBNR-10 - Definitions: Breach - exceptions Unsecured PHI: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this

part. (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E 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: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

References

- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.402 - Definitions: Breach - exceptions Unsecured PHI

HIPAA - Breach Notification Rule	Other Requirements
§164.402 Definitions: Breach - exceptions Unsecured PHI	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E 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:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Guidance
Did the covered entity or business associate determine that an acquisition, access, use or disclosure of protected health information in violation of the Privacy Rule not require notifications within the specified period?

• If yes, did the covered entity or business associate determine that one of the regulatory exceptions to the definition of breach apply? If yes, obtain documentation of such determination. Use sampling methodologies to select and review documentation that such were completed.

• If yes, did the covered entity or business associate determine that the breach did not require notification, because the PHI was not unsecured PHI, i.e., it was rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the applicable guidance? If yes, obtain and review documentation. Use sampling methodologies to select and review documentation that such were completed.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- HBNR-9 - Definitions: Breach - Risk Assessment.: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted which compromises the security or privacy of the PHI. (2) Except as provided, an acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and (iv) The extent to which the risk to the PHI has been mitigated.
- HBNR-10 - Definitions: Breach - exceptions Unsecured PHI: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E 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: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii)

The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

References

- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

HIPAA §164.404(a) - Notice to Individuals

HIPAA - Breach Notification Rule	Other Requirements
§164.404(a) Notice to Individuals	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

Guidance
Does the covered entity have policies and procedures for notifying individuals of a breach of their protected health information?

Obtain and review a list of breaches that occurred in the specified period. Obtain and review related additional documentation of notifications provided to the affected individuals. Determine whether notifications were provided to individuals consistent with the requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- HBNR-11 - Notice to Individuals: A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

References

- HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

Truncated Sample Report