HIPAA - Privacy Rule

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

27	HIPAA §164.510(a)(3) - Uses and Disclosures for Facility Directories in Emergency Circumstances
28	HIPAA §164.510(b)(1) - Permitted uses and disclosures
29	HIPAA §164.510(b)(2) - Uses and disclosures with the individual present
30	HIPAA §164.510(b)(3) - Limited uses and disclosures when the individual is not present
31	HIPAA §164.510(b)(4) - Uses and disclosures for disaster relief purposes
32	HIPAA §164.510(b)(5) - Uses and disclosures when the individual is deceased
33	HIPAA §164.512(a) - Uses and disclosures required by law
34	HIPAA §164.512(b) - Uses and disclosures for public health activities
35	HIPAA §164.512(c) - Disclosures about victims of abuse, neglect or domestic violence
36	HIPAA §164.512(d) - Uses and disclosures for health oversight activities
37	HIPAA §164.512(e) - Disclosures for judicial and administrative proceedings
38	HIPAA §164.512(f)(1) - Disclosures for law enforcement purposes
39	HIPAA §164.512(f)(2) - Disclosures for law enforcement purposes - for identification and location -
40	HIPAA §164.512(f)(3) - Disclosures for law enforcement purposes-- PHI of a possible victim of a crime
41	HIPAA §164.512(f)(4) - Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct
42	HIPAA §164.512(f)(5) - Disclosures for law enforcement purposes: crime on premises
43	HIPAA §164.512(f)(6) - Disclosures for law enforcement purposes
44	HIPAA §164.512(g) - Uses and disclosures about decedents
45	HIPAA §164.512(h) - Uses and disclosures for cadaveric organ, eye or tissue donation
46	HIPAA §164.512(i)(1) - Uses and disclosures for research purposes -- Permitted Uses and Disclosures
47	HIPAA §164.512(i)(2) - Uses and disclosures for research purposes -- Documentation of Waiver Approval
48	HIPAA §164.512(k)(1) - Uses and disclosures for specialized government functions -- Military
49	HIPAA §164.512(k)(2) - Uses and disclosures for specialized government functions -- National Security and intelligence activities
50	HIPAA §164.512(k)(3) - Uses and disclosures for specialized government functions -- Protective Services
51	HIPAA §164.512(k)(5) - Uses and disclosures for specialized government

	functions – Correctional institutions
52	HIPAA §164.512(k)(6) - Uses and disclosures for specialized government functions – Providing public benefits
53	HIPAA §164.512(l) - Disclosures for workers' compensation
54	HIPAA §164.514(b) & §164.514(c) - Requirements for De-Identification of PHI & Re-Identification of PHI
55	HIPAA §164.514(d)(1)-§164.514(d)(2) - Standard: Minimum Necessary & Minimum Necessary Uses of PHI
56	HIPAA §164.514(d)(3) - Minimum Necessary - Disclosures of PHI
57	HIPAA §164.514(d)(4) - Minimum Necessary requests for protected health information
58	HIPAA §164.514(d)(5) - Minimum Necessary - Other content requirement
59	HIPAA §164.514(e) - Limited Data Sets and Data Use Agreements
60	HIPAA §164.514(f) - Uses and Disclosures for Fundraising
61	HIPAA §164.514(g) - Uses and Disclosures for Underwriting and Related Purposes
62	HIPAA §164.514(h) - Verification Requirements
63	HIPAA §164.520(a)(1) & (b)(1) - Notice of Privacy Rule Practices
64	HIPAA §164.520(c)(1) - Provisions of Notice - Health Plans
65	HIPAA §164.520(c)(2) - Provisions of Notice - Certain Covered Health Care Providers
66	HIPAA §164.520(c)(3) - Provision of Notice - Electronic Notice
67	HIPAA §164.520(d) - Joint Notice by Separate Covered Entities
68	HIPAA §164.520(e) - Documentation
69	HIPAA §164.522(a)(1) - Right of an Individual to Request Restriction of Uses and Disclosures
70	HIPAA §164.522(a)(2) - Terminating a Restriction
71	HIPAA §164.522(a)(3) - Documentation
72	HIPAA §164.522(b)(1) - Confidential Communications Requirements
73	HIPAA §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3) - Right to access
74	HIPAA §164.524(d) (2) - Denial of Access
75	HIPAA §164.524(a)(2) - Unreviewable grounds for denial
76	HIPAA §164.524(a)(3) - Reviewable grounds for denial
77	HIPAA §164.524(a)(4) & (d)(4) - Review of denial of access
78	HIPAA §164.524(e) - Documentation

79	HIPAA §164.526(a)(1) - Right to Amend
80	HIPAA §164.526(a)(2) - Denying the Amendment
81	HIPAA §164.526(c) - Accepting the Amendment
82	HIPAA §164.526(d) - Denying the Amendment
83	HIPAA §164.528(a) - Right to an Accounting of Disclosures of PHI
84	HIPAA §164.528(b) - Content of the Accounting
85	HIPAA §164.528(c) - Provision of the Accounting
86	HIPAA §164.528(d) - Documentation
87	HIPAA §164.530(a) - Personnel designations
88	HIPAA §164.530(b) - Training
89	HIPAA §164.530(c) - Safeguards
90	HIPAA §164.530(d)(1) - Complaints to the Covered Entity
91	HIPAA §164.530(d)(2) - Complaints to the Covered Entity
92	HIPAA §164.530(e)(1) - Sanctions
93	HIPAA §164.530(f) - Mitigation
94	HIPAA §164.530(g) - Refraining from Intimidating or Retaliatory Acts
95	HIPAA §164.530(h) - Waiver of rights
96	HIPAA §164.530(i) - Policies and Procedures
97	HIPAA §164.530(j) - Documentation

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 §164.502(a)(1) - Uses and Disclosures

HIPAA - Privacy Rule	Other Requirements
§164.502(a)(1) Uses and Disclosures	N/A

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

A covered entity or business associate may not use or disclose protected health information, except as permitted or required.

Guidance
Does the health plan use or disclose for underwriting purposes, “Genetic Information” as defined at § 160.103, including family history? Inquire of management.

Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). Evaluate whether the underwriting policies are consistent with the established performance criterion.

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

Related Internal Controls
- HPR-1 - Uses and Disclosures: Ensure that the covered entity or business associate does not use or disclose protected health information, except as permitted or required.

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

HIPAA §164.502(a)(2) - Covered Entities: Required Disclosures

HIPAA - Privacy Rule	Other Requirements
§164.502(a)(2) Covered Entities: Required Disclosures	N/A

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

A covered entity is required to disclose protected health information to an individual and to the OCR for a compliance investigation.

Guidance
Patients are entitled to access their PHI and to have it shared as they authorize. Authorization is not required to share patient data for an OCR compliance investigation.

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

Related Internal Controls
- HPR-2 - Covered Entities: Required Disclosures: Ensure that the covered entity discloses protected health information as required to an individual and to the Office for Civil Rights for a compliance investigation.

References
- HIPAA Privacy Rule - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Individuals' Right to Access their Health Information - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

HIPAA §164.502(a)(3) - Business Associates: Permitted Uses and Disclosures

HIPAA - Privacy Rule	Other Requirements
§164.502(a)(3) Business Associates: Permitted Uses and Disclosures	N/A

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

A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements , if done by the covered entity, except for the purposes that are permitted by its contract or other arrangement.

Guidance
Business Associates may only access data as needed to provide services.

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

Related Internal Controls
- HPR-4 - Business Associates: Permitted Uses and Disclosures: A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements , if done by the covered entity, except for the purposes that are permitted by its contract or other arrangement.

References
- HIPAA Privacy Rule - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Business Associates - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

HIPAA §164.502(a)(5)(i) - Health Plan prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes

HIPAA - Privacy Rule	Other Requirements
§164.502(a)(5)(i) Health Plan prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	N/A

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

Health plans may not use or disclose genetic information for underwriting purposes.

Guidance
Does the health plan use or disclose for underwriting purposes, “Genetic Information” as defined at § 160.103, including family history? Inquire of management.

Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). Evaluate whether the underwriting policies are consistent with the established performance criterion.

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

Related Internal Controls
- HPR-5 - Health Plan prohibited uses and disclosures of genetic information for underwriting purposes: Health plans may not use or disclose genetic information for underwriting purposes.

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

HIPAA §164.502(b) - Minimum Necessary

HIPAA - Privacy Rule	Other Requirements
§164.502(b) Minimum Necessary	N/A

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

When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Guidance
Access to PHI is only allowed to accomplish a business purpose. Unauthorized access or use (even by users authorized to access an entire database) is prohibited. Access logs and log reviews are required to identify unauthorized activity.

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

Related Internal Controls
- HPR-49 - Standard: Minimum Necessary & Minimum Necessary Uses of PHI: Standard: Minimum necessary (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. (2) Minimum necessary does not apply. This requirement does not apply to: (i) Disclosures to or requests by a health care provider for treatment; (ii) Permitted uses or disclosures made to the individual; (iii) Uses or disclosures made pursuant to an authorization; (iv) Disclosures made to the Secretary; (v) Uses or disclosures that are required by law,; and (vi) Uses or disclosures that are required for compliance. Implementation specifications: Minimum necessary uses of protected health information. (i) A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access. (ii) A covered entity must make reasonable efforts to limit the access of such persons or classes to protected health information.

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

HIPAA §164.502(c) - Restricted Uses and Disclosures

HIPAA - Privacy Rule	Other Requirements
§164.502(c) Restricted Uses and Disclosures	N/A

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

A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

Guidance
Covered entities must abide by an individual's direction to restrict access, including identifying the method requested for communications.

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

Related Internal Controls
- HPR-65 - Restricted Uses and Disclosures: A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

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

HIPAA §164.502(d) - De-identified Protected Health Information

HIPAA - Privacy Rule	Other Requirements
§164.502(d) De-identified Protected Health Information	N/A

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

A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

Guidance
HIPAA defines 18 identifiers, ranging from specific names to "other ways to identify an individual." De-identifying information is difficult and requires expert knowledge.

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

Related Internal Controls

- HPR-48 - Requirements for De-Identification of PHI & Re-Identification of PHI: Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if: (1) A person with appropriate knowledge of any experience with generally accepted statistical scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify and individual who is a subject for the information; and (ii) Documents the methods and results of the analysis that justify such determination; or (2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current available data from the Bureau of the Census; (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial

numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. Implementation specifications: Re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: (1) The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

References

- HIPAA Privacy Rule - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- De-identification - https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

HIPAA §164.502(e) - Disclosures to Business Associates

HIPAA - Privacy Rule	Other Requirements
§164.502(e) Disclosures to Business Associates	N/A

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

A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

Guidance
A Covered Entity may disclose PHI to a Business Associate, which may disclose it to a Subcontractor Business Associate. Business Associate Agreements and full compliance with HIPAA are required of Business Associates.

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

Related Internal Controls
- HPR-3 - Disclosures to Business Associates: A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

References
- HIPAA Privacy Rule - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Business Associates - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

HIPAA §164.502(f) - Deceased individuals

HIPAA - Privacy Rule	Other Requirements
§164.502(f) Deceased individuals	N/A

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

PHI related to deceased individuals is protected for 50 years after their death.

Guidance
Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion? Inquire of management.

Obtain and review policies and procedures regarding use and disclosure of deceased individuals' PHIs. Evaluate whether the policies and procedures are consistent with the established performance criterion

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

Related Internal Controls
- HPR-6 - Deceased individuals: PHI related to deceased individuals is protected for 50 years after their death.

References
- HIPAA Privacy Rule - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- HIPAA Combined Regulation - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
- Health Information of Deceased Individuals - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

Truncated Sample Report