HIPAA Individual Rights Policy

Description:

This policy explains the permitted and required uses and disclosures of protected health information (PHI), as well as authorization for use and disclosure of PHI, under the Health Insurance Portability and Accountability Act (HIPAA).

Reason for Policy:

All DHS employees who have access to PHI must follow HIPAA's privacy regulations to use and disclose PHI.

Applicability:

This policy applies to DHS' health care components. For a current list of DHS' health care components, refer to DHS' Designation as a HIPAA Hybrid Entity.

NOTE: DCT employees must follow all applicable DCT policies and procedures when using or disclosing information about DCT patients/clients.

Failure to Comply:

Failure to comply with this policy and its procedures may result in disciplinary actions, up to and including termination.

Policy

Under HIPAA, DHS' health care components must allow individuals to exercise certain rights with respect to their PHI. This includes:

- The individual's right to access certain records about them containing PHI.
- The individual's right to ask DHS to limit, or "restrict", certain uses and disclosures of their PHI.
- The individual's right to ask to receive communications of PHI from DHS in certain ways or places.

- The individual's right to request that DHS correct, or "amend", certain records about them containing PHI.
- The individual's right to request and receive a record, or "accounting", of certain disclosures of their PHI.

This policy addresses each of these five rights.

I. Right to Access PHI

Three different laws allow individuals to access health information that DHS has about them:

- HIPAA;
- Minnesota Health Records Act (MHRA); and
- the Minnesota Government Data Practices Act (MGDPA).

Except in certain circumstances, HIPAA provides individuals with the right to review and obtain a copy of their PHI in DHS's record set. The "designated record set" is the group of records maintained by or for a covered entity that is used, in whole or in part, to make decisions about individuals. It also includes a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims of adjudication, and case or medical management records systems.

However, the MHRA and MGDPA provide individuals with broader rights of access to health information. As a result, DHS must follow the requirements of the MHRA and MGDPA when providing individuals with access to their health information.

A. Information Included in the Right of Access

Under the MHRA and MGDPA, DHS must allow the individual to access their entire health record, unless:

- prior to the request, a licensed health care professional determines that the information is reasonably likely to be harmful to the patient's physical or mental health or to cause the patient to harm themselves or another; or
- the information is classified as confidential under the MGDPA.

B. Request for Access and Timely Action

DHS must permit an individual to request access to inspect or to obtain a copy of the PHI that is maintained in a designated record set. DHS may require individuals to make requests for access in writing, as long as DHS informs individuals of this requirement.

The MGDPA has the strictest timeframe for providing an individual with access to their health information. It requires DHS to respond within 10 days of receiving a data subject's request for access to their public and/or private data. DHS must comply with this timeframe because it is stricter than the timeframe specified in the MHRA ("promptly") or HIPAA (30 days).

C. Form of Access

If there is no legal basis for denying an individual's request for their health information, DHS must provide the individual with access to the information by:

- arranging a convenient time for the individual to look at, or "inspect" the information;
- if requested, providing the individual with paper or electronic copies of the information; or
- providing a summary of the information requested either in place of providing the information or to explain the information provided, as long as the individual agrees in advance to the summary and to any fees that will be charged to the individual for the summary.

DHS must provide the individual with the information in the form and format requested by the individual, if it is readily producible in that form or format. If it is not readily available in that format, then DHS must provide the individual with the information in a readable form and format agreed to by DHS and the individual.

D. Allowable Costs for Access

If the individual requests a copy of the health information, DHS may impose a reasonable fee. Under both HIPAA and the MGDPA, DHS may only require that the individual pay fees that address:

- the cost of labor and supplies for making copies of the data;
- costs for mailing the information, if requested; and
- the cost of preparing an explanation of summary of PHI.

DHS may not charge the individual when the individual inspects, but does not request copies, of the health information. DHS may not charge a fee when the patient/client requests a copy of their health record for purposes of reviewing their current medical care. Refer to DHS' Guide to Responding to Data Requests for more information.

E. Denying Access

If DHS denies an individual's request for access, in whole or in part, DHS must provide the individual with a written denial of their request that is written in plain language and explains the grounds for the denial. Under the MGDPA, DHS must cite to the statutory section that permits DHS to deny the request.

If DHS denies access because a licensed health care official, in the exercise of professional judgement, has determined that access to the requested PHI is (1) reasonably likely to endanger the individual or another person, (2) reasonably likely to cause substantial harm to a person named in the PHI, or (3) to a personal representative and is reasonably likely to cause substantial harm to the individual or another person, then the written denial must also include:

- A statement that the individual has the right to request review of the decision to deny access and an explanation of how the individual may request review; and
- An explanation of how the individual may make a complaint to DHS or the U.S. Department of Health and Human Services.

If the individual requests review of the decision to deny access to their PHI, the DHS health care component must designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access. This designated reviewer must determine, within a reasonable time period, whether to deny access. The health care component must then provide the individual with written notice of the reviewer's determination and take actions to carry out the reviewer's decision (i.e., to deny or grant access).

II. Right to Ask DHS to Limit Uses or Disclosures of PHI

A. Requests to Limit Uses or Disclosures

DHS health care components must allow an individual to ask DHS to limit, or "restrict", how it:

- uses or discloses certain PHI treatment, payment, or health care operations; or
- discloses PHI to family members or other persons involved in the individual's care.

A request to restrict uses or disclosures of PHI must:

- be in writing;
- explain what information the individual wants to restrict; and
- identify the individual to whom they want the restrictions to apply.

The applicable DHS Notice of Privacy Practices explains how an individual can make a request to restrict uses or disclosures of PHI. Refer to HIPAA Privacy Notices about Protected Health Information Policy for more information.

B. Agreeing to a Request for Restriction

DHS is not required to agree to restrict uses or disclosures of PHI. Additionally, DHS cannot agree to restrict uses or disclosures of PHI that are required by law.

However, a DHS health care component **must** agree to restrict disclosures of PHI that:

- are to a health plan;
- are for the purpose of carrying out payment or health care operations and are not otherwise required by law; and
- relate only to a health care item or service for which the individual, or person other than the individual's health plan, has paid the item or service in full.

If a DHS health care component agrees to an individual's request to restrict uses or disclosures of their PHI, the health care component must:

- document this agreement in writing;
- inform the individual, in writing, about what requested restrictions DHS agrees to follow; and
- take the necessary steps to make sure that appropriate staff are aware of the agreed-upon restriction(s) and do not use or disclosure the individual's PHI in a restricted way.

- Once a DHS health care component agrees to restrict certain uses or disclosures of PHI, it must follow those restrictions unless a restricted use or disclosure of PHI is necessary to provide emergency treatment to the individual. If a DHS health care component discloses restricted PHI to another health care provider for emergency treatment, the DHS health care component must ask the other health care provider to not further use or disclose the PHI.

C. Ending a Request for Restriction

DHS may end a restriction if the individual agrees to or requests the termination in writing, or the individual orally agrees to the termination and DHS documents the oral agreement.

DHS may end a restriction if it first informs the individual it is ending the restriction. Ending a restriction this way is only effective with respect to PHI that the DHS health care component creates or receives **after** informing the individual that it is ending the restriction.

A DHS health care component may not end a restriction to which it is required to agree (refer item II.B, above) unless the individual asks the health care component to end the restriction.

D. Documentation

DHS health care components must maintain documentation of a restriction for at least 6 years.

III. Confidential Communications

A. Requesting Confidential Communications

HIPAA allows individuals to ask to receive communications of PHI from a DHS health care component in a certain way or in a certain place. For example, an individual can ask a DHS health care component to send PHI to their work address instead of their home address.

A DHS health care component may require individuals to make their requests in writing. The applicable Notice of Privacy Practices must explain how individuals can ask to receive PHI in a certain way or place.

B. Granting a Request for Confidential Communications

Whether and when a DHS health care component must grant, or "accommodate", a request for communication of PHI in a certain way or at a certain place depends on whether the health care component is acting as a health care provider or health plan:

- If a DHS health care component is acting as **health care provider**, DHS must grant any reasonable request for communications of PHI in a certain way or certain place. A DHS health care component acting as a health care provider **cannot** require the individual to explain why they are making the request.
- If a DHS health care component is acting as a **health plan**, DHS must grant a request if it is reasonable and if the individual clearly states that they would be in danger if the health care component did not grant the request.

A DHS health care component may require the individual making the request to:

- When appropriate, provide information about how payment for health care services will be handled; or
- Specify the alternative address or other method of contacting the individual.

IV. Right to Request Amendment of PHI

A. Requesting Amendment and Timely Action

HIPAA gives individuals the right to have DHS health care components amend or correct their PHI in a "designated record set" when that information is inaccurate or incomplete.

The applicable DHS Notice of Privacy Practices must explain how an individual can request amendment of their PHI. DHS health care components may require an individual to submit requests for amendment in writing and to explain why the information they are asking to change is wrong or incomplete, as long as individuals are informed in advance of this requirement (for example, in the Notice of Privacy Practices).

Under the MGDPA, a DHS health care component must either accept or deny the requested amendment within 30 days. Although HIPAA allows a longer period, Minnesota law is stricter and therefore governs.

B. Granting a Request for Amendment

If a DHS health care component **grants** an amendment, DHS must:

- Make the appropriate changes or additions to the individual's PHI. At a minimum, this requires (1) identifying the records in the individual's designated record set that are affected by the amendment, and (2) appending or providing a link to the amended information.
- **Inform the individual**: This means (1) informing the individual that the amendment has been accepted; and (2) asking the individual to identify who needs to be informed about the amendment and getting the individual's written agreement that the DHS health care component may notify the identified persons about the amendment.
- **Inform others:** This means that the DHS health care component must make reasonable efforts to provide the amendment to others, including:
    - persons identified by the individual as having previously received PHI about the individual and needing to receive the amendment; and
    - persons, including business associates, who the DHS health care component knows have the PHI that was amended. Note that although HIPAA only requires sharing the amendment when the information may negatively affect the data subject, the MGDPA is more restrictive and therefore governs.

C. Denying a Request for Amendment

DHS may deny an individual's request to amend if the PHI:

- was not created by DHS, unless the individual provides a reasonable basis to believe that the person or entity who originated the PHI is no longer available to act on the requested amendment;
- is not part of a designated record set;
- is not available for the individual to access (refer to section I above); or
- is accurate and complete.

If a DHS health care component denies an individual's request for amendment, the health care component must, within 30 days, provide the individual with a written denial. The denial must be written in plain language and contain the following:

- An explanation of why the request is denied;
- Notice that the individual has the right to submit to DHS a written statement disagreeing with the denial and an explanation of how the individual may do so;
- A statement that, if the individual does not submit a written statement of disagreement, they may request that the DHS health care component provide a copy of the request for amendment and denial of the request with any future disclosures of the PHI that relates to the request;
- An explanation of how the individual may make a complaint to DHS or the Secretary of the U.S. Department of Health and Human Services.

Individuals may submit a written statement disagreeing with the denial. The health care component may place reasonable limits on the length of the written statement.

DHS may prepare a written rebuttal to the individual's statement of disagreement, if one is submitted. The individual must be provided with a copy of the rebuttal. DHS must identify the record in the individual's designated record set that is the subject of the denied request, and append or link the individual's request for amendment; the health care component's denial of the request; the individual's written statement of disagreement, if any; and the health care component's rebuttal, if any.

In future disclosures, DHS must include the following documents with the designated record set:

- If the individual submitted a statement of disagreement, DHS must either include all of the documents listed above or an accurate summary of these documents.
- If the individual did not submit a statement of disagreement, DHS must include the individual's request for amendment and the denial of the request only if the individual requests that DHS do so.

D. Amendment Requests Granted by Another Covered Entity

If a DHS health care component is informed by another HIPAA covered entity of an amendment to an individual's PHI, the DHS health care component must amend any corresponding PHI in the individual's designated records set.

E. Documentation Requirement

DHS' health care components must document the titles of the person or offices responsible for receiving and processing requests for amendments and retain this documentation for at least six years.

V. Request for an Accounting of Disclosures of PHI

A. Right to Accounting of Disclosures

An individual has the right to receive an accounting of all disclosures of PHI made by a DHS health care component in the six years before the date on which the accounting is requested.

However, HIPAA does not require accounting for disclosures:

- to carry out treatment, payment, or health care operations;
- to the individual (or their personal representative);
- incident to otherwise permitted or required uses or disclosures;
- pursuant to an authorization;
- to persons involved in the individual's care;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials; or
- as part of a limited data set.

The individual may request an accounting for a period of less than six years from the date of the request. Contact your business area's assigned legal counsel for guidance.

B. Content of the Accounting

If an individual requests an accounting of their disclosures, DHS must provide a written accounting that meets the following requirements:

- All disclosures that occurred during the six years, or the shorter period of time requested by the individual except as listed above.
- For each disclosure:
    - the date of the disclosure;
    - the name of the person or organization who received the PHI and their address, if known;
    - a brief description of the PHI disclosed; and
    - a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

In certain situations a DHS health care component may create summaries that cover multiple disclosures, rather than documenting each disclosure in an individual entry. Contact your business area's assigned legal counsel for guidance.

C. Providing the Accounting

When an individual requests an accounting of their disclosures, DHS must respond to the individual within 60 days after receiving the request. A DHS health care component may respond:

- by providing the individual with the requested accounting; or

- if DHS is unable to provide the accounting within 60 days, by providing the individual with a written statement of the reason(s) for the delay and the date by which the DHS health care component will provide the accounting. DHS may extend the time to provide the accounting by no more than 30 days and is only allowed one extension per request for accounting.

In any 12-month period, an individual is entitled to one free accounting of their disclosures. After an individual has been provided with a free accounting of their disclosures, DHS may charge a reasonable, cost-based feed for any additional requests the individual makes in the 12-month period, provided that, (1) DHS informs the individual in advance of the fee, and (2) gives the individual an opportunity to withdraw or modify their request for accounting to avoid or reduce the fee.

D. Suspension of Right to an Accounting

Under certain circumstances, a DHS health care component must temporarily suspend an individual's right to receive an accounting of disclosures of their PHI to a health oversight agency or law enforcement official, when requested by such agency or official. Contact your business area's assigned legal counsel for guidance.

E. Documentation

The DHS health care component must document the following and retain the documentation for at least 6 years:

- the information required to be included in an accounting for all disclosures of PHI that are subject to an accounting;
- the written accounting that is provided to the individual, upon request; and
- the titles of the persons or offices responsible for receiving and processing requests for an accounting.

Procedure(s) that Apply:

Workforce members of DHS health care components who have access to PHI should be familiar with HIPAA- and other privacy-related procedures in their business area that are specific to their work. Questions about HIPAA and other privacy-related procedures should be directed to your business area. Business area procedures must comply with the standards in this policy.

Forms that Apply:

DHS employees who have access to health information about individuals should be familiar with HIPAA- and other privacy-related forms used by their business area that are specific to their work. Many of these forms can be found in DHS' electronic document library ("eDocs"). Questions about HIPAA- and privacy-related forms not available in eDocs should be directed to your business area.

Related Policies and Reference(s):

- DHS' Designation as a HIPAA Hybrid Entity
- DHS Guide for Requesting Data about You
- DHS Guide to Responding to Data Requests
- Forensic Services Policy 330-3005 (Designated Record Set)
- MSOP Policy 135-5300 (Health Information Record Designation)
- MHSATS Policy 330-4030 (Designated Record Set)

Training:

All DHS employees must pass annual privacy and security online training modules to have continued access to DHS systems and data. Four of these online training modules relate to protection of health information about individuals and are available on the DHS Central Office Learning Center:

- Data Security and Privacy;
- How to Protect Information;
- Managing Security Information Problems; and
- PHI.

Questions about training specific to your work should be directed to your business area leadership.

Legal Authority:

- 45 C.F.R. §§ 164.502(c), (h); 164.522; 164.524; 164.526; 164.528
- Minn. Stat. § 144.292, subds. 2, 5-7
- Minn. Stat. §§ 13.04, subds. 3, 4; 13.46, subd. 5; 13.384, subd. 3

Definition(s):

DHS HIPAA Privacy glossary

Policy Contact(s):

General Counsel Office; **Email:** dhs.privacyoffice@state.mn.us

Policy History:

Issue Date: 12/08/2023
Effective Date: 12/08/2023

Version 1.0
10/21/2024 (Contact updated)
10/31/2023 (Revised)
08/29/2023 (Reaffirmed)
02/04/2020 (Initial release)

This policy and its procedures remain in effect until rescinded or updated.