

HIPAA Hybrid Entity Status Policy

Description:

This policy explains DHS' responsibilities as a hybrid entity under HIPAA and how HIPAA applies to different parts of DHS. It must be read and applied in conjunction with all other policies, procedures, and guides relating to data privacy and security at DHS.

Reason for Policy:

As a hybrid entity, DHS must maintain and implement policies and procedures that protect PHI created or received by DHS' health care components from unauthorized disclosure to or access by DHS' non-health care components

Applicability:

This policy applies DHS-wide.

Failure to Comply:

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

Policy:

I. Designation of DHS' Health Care Components

The [DHS Hybrid Entity Designation](#) identifies DHS' health care components. DHS' designated health care components include:

- Any component that would meet the definition of "covered entity" if it were a separate legal entity; and
- Other components of DHS to the extent they use PHI to support one or more of DHS' covered functions.

DHS reserves the right to revise the [DHS Hybrid Entity Designation](#). As needed and at least every two years, the DHS Legal and Compliance Office will review this Designation and advise DHS senior leadership on any

recommended changes. DHS senior leadership is responsible for approving this Designation and changes to this Designation.

DHS must retain the Hybrid Entity Designation and related documentation for at least six years, consistent with HIPAA requirements and the applicable retention schedule.

II. Responsibilities of DHS' Health Care Components to Comply with HIPAA

- DHS' health care components must comply with HIPAA and related DHS policies.
- Certain business areas within DHS are identified as a health care component only to the extent they use PHI to support one or more of DHS' covered functions. These parts of DHS must comply with HIPAA when conducting activities that involve the use of PHI.

III. Limitations on Disclosure of PHI to Non-Health Care Components

For the purposes of disclosing PHI, DHS' health care components must treat administrations, divisions, offices, or staff in DHS' non-health care components as if they are a separate organization. This means that:

- DHS' health care components may not disclose PHI to DHS' non-health care components unless HIPAA would allow DHS to make the disclosure to a person or organization outside of DHS.
- Staff in DHS' non-health care components may not access electronic PHI stored in DHS information systems unless HIPAA would allow DHS to provide the access to a person or organization outside of DHS.
 - In collaboration and consultation with Minnesota IT Services ("MN.IT"), DHS will implement and maintain controls that safeguard electronic PHI stored in DHS information systems from unauthorized disclosure, access, or use by DHS' non-health care components.
- DHS staff that perform duties for both DHS' health care component and DHS' non-health care component may not use or disclose PHI that the staff creates or receives while working on behalf of DHS' health care component to DHS' non-health care component unless the disclosure would be permitted under HIPAA as to a third party.
- DHS staff must report any unauthorized access, use, or disclosure of PHI between a DHS' health care component and non-health care component to the DHS Privacy Office using the [Privacy Incident Reporting Form](#) (DOC) or to MN.IT (651-297-1111), if the incident involves DHS information systems or equipment.

Consult DHS' HIPAA-related policies and/or DHS' Legal and Compliance Office for guidance about permitted disclosures to and uses of PHI by DHS' non-health care components.

IV. Relationship to Other Law

All parts of DHS, including DHS' non-health care components, must comply with all other applicable state and federal data privacy laws, including the Minnesota Government Data Practices Act (Minnesota Statutes, chapter 13) and Minnesota Health Records Act (Minnesota Statutes, sections 144.291-144.198).

Forms:

- [Privacy Incident Reporting Form](#) (DOC)

Related Policies and Reference(s):

- [Minnesota Department of Human Services' Designation as Hybrid Entity](#)

Legal Authority:

45 C.F.R. §§ 164.103 and 164.105

Definition(s):

Covered Entity: For purposes of HIPAA, a covered entity means a health plan, health care provider, or health care clearinghouse.

Covered Function: The functions that make an organization a health plan, health care provider, or health care clearinghouse for purposes of HIPAA.

Health Insurance Portability and Accountability Act (HIPAA): DHS business area that performs a covered function by acting as a health care provider or health plan. DHS' health care components are listed in [DDHS' Designation as a Hybrid Entity](#).

Health Care Component: DHS business area that performs a covered function by acting as a health care provider or health plan. DHS' health care components are listed in [DHS' Designation as a Hybrid Entity](#).

Non-Health Care Component: DHS business area that does not perform a covered function. DHS' non-health care components are listed in [DHS' Designation as a Hybrid Entity](#).

Hybrid Entity: A single legal entity that performs both covered and non-covered functions as defined by HIPAA and that elects to be a hybrid entity in compliance with the requirements of 45 C.F.R. § 164.105.

Protected Health Information (PHI): Individually identifiable health information created or received by or on behalf of one of DHS' health care components, as defined under HIPAA (45 C.F.R. §§ 160.103 and 164.105(a)(2)(i)(C)).

Policy Contact(s):

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

Policy History:

Original Publication Date: 5/17/2019

Last Revision Date: 6/14/2019

Version 1.0

10/21/2024 (Contact updated)

08/29/2023 (Reaffirmed)

06/14/2019 (Revised)

05/17/2019 (Initial Release)

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