HEALTH PLAN POLICY		
Policy Title: Member Privacy Rights		**Policy Number:** OPMS17 **Revision:** H
Department: Operations	**Sub-Department:** Member Services	
Applies to Product Lines: ☐Medicaid ☐Children's Health Insurance Plan ☒Health Insurance Exchange ☒Medicare		☒USFHP ☒Commercial Insured ☒Non Insured Business
Origination/Effective Date: 07/16/2015		
Reviewed Date(s):	**Revision Date(s):** 12/01/2015, 03/04/2016, 06/01/2017, 04/24/2019, 05/04/2020, 04/27/2021, 03/22/2022, 03/30/2023	

SCOPE:

The purpose of this policy is to specify and document the health plan policy in regards to compliance with federal, state, and local laws and regulations governing member privacy rights including but not limited to the Health Insurance Portability and Accountability Act ("HIPAA"), and applicable contractual requirements. It is the policy of the health plan that all members shall be afforded the privacy rights permitted under HIPAA and other applicable federal, state, and local laws and regulations, and applicable contractual requirements.

DEFINITIONS AND ACRONYMS:

- **Affiliate –** Medicaid business conducted by the direct and indirect subsidiaries of the health plan Inc.
- **Business Associate** – A person or entity that uses and/or discloses protected health information to perform a function or activity on behalf of the health plan or health plans.
- **Code of Federal Regulations (CFR)**
- **Confidential Communication –** Communication of protected health information to a member by an alternative method (e.g., to a different mailing address or location) if the health plan's standard method of communication would endanger the confidentiality of a member's protected health information.
- **Covered Entity –** Covered entity means a health plan; a health care clearinghouse; or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA standards. (45 C.F.R. Part 160 and Part 164, 45 CFR 160.103, 164.501)
- **Designated Record Set –** The set of electronic or paper records that may be accessed by members, their authorized representatives, or designated health plan personnel who, on behalf of the health plan or health plans, need access in order to carry out their job functions. Because these records contain protected health information, their use and disclosure is subject to federal, state, and local privacy laws. The designated (protected health information) record set includes enrollment, payment, claims adjudication, case management, and medical management records, as well as any other record (in whole or in part) used to make decisions about a member.
  - The following are excluded from the designated record set:
    - Quality assessment, credentialing or other peer review records
    - Psychotherapy notes

  - Information compiled by the health plan or health plans to prepare for or use in a civil, criminal, or administrative action
  - Information developed solely for the administration of the health plan or health plans, such as proprietary or confidential information used to make business decisions

- **Health Insurance Portability and Accountability Act (HIPAA)** – The Health Insurance Portability and Accountability is Public Law 104–191.
- **Member –** The individual member, enrollee, or beneficiary eligible and enrolled in a state or federally funded or commercial health care program.
- **Notice of Privacy Practices –** A formal written description of how health plans use and disclose protected health information and the member's rights with respect to that information.
- **Personnel –** Employees of the health plan, its affiliates, consultants, temporary or seasonal employees, student interns, volunteers, and any other class or type of full or part time employee who participate in the health plan administrative operations.
- **Privacy Rights –** The rights afforded to individuals under HIPAA and other applicable federal, state, and local laws and regulations.
- **Protected Health Information (PHI) –** Generally, health information contained in electronic or paper records that is individually identifiable (i.e., that identifies an individual or can be traced back to the individual). The use, disclosure, and transmission of protected health information are subject to privacy rules, regardless of the medium employed (electronic, paper, or verbal).

POLICY:

The objective of this policy is to assist the health plan and health plan personnel in meeting the privacy requirements of HIPAA and the response process to member or authorized representative exercising his or her privacy rights through privacy request, including:

- Making information available to members or their representatives about the health plan's practices regarding their protected health information ("PHI")
- Maintaining a process for members to request access to, changes to, or restrictions on disclosure of their PHI
- Providing consistent review, disposition, and response to privacy requests within required time standards
- Documenting requests and actions taken

Further, the health plan has responsibility for operations of its affiliated entities including health plans administered by such affiliated entities ("health plans") and oversight of affiliates' performance with their respective obligations, including compliance with member privacy rights under HIPAA and other applicable federal, state, and local laws and regulations, and applicable contractual requirements. Accordingly, the health plan requires, as set forth in this policy, each of its affiliates to implement companion compliance policies on protecting member privacy rights.

The health plan honors the following member rights related to their PHI ("privacy rights"):

- The right to know the practices related to using and disclosing PHI (health plan Notice of Privacy Practices)

- The right to make certain requests regarding PHI

To fulfill these obligations, health plans develop and make available as required their own Notice of Privacy Practices to members. The creation and review of all health plan Notice of Privacy Practice shall be with the Medicaid Business Unit compliance department; any proposed revisions by health plans shall be presented to the health plan compliance department. Health plans must also develop and maintain processes for reviewing and responding to requests from members or their representatives regarding the PHI of the member.

Health Plan Notice of Privacy Practices

The health plan Notice of Privacy Practices provides a formal written description of how the respective health plan may use and disclose PHI. At a minimum, the notice must explain members' rights to access, change, restrict or receive an accounting of disclosures of PHI. Health plans shall make their respective Notice of Privacy Practices available to members at enrollment and annually thereafter in accordance with HIPAA or and other applicable federal, state, and local laws and regulations distribution requirements. Additional copies are available to members or their representatives upon verbal or written request.

Member Privacy Requests

Members may make the following requests related to their PHI ("privacy requests") in accordance with federal, state, and local law:

- Make a privacy complaint
- Receive a copy of all or part of the designated record set
- Amend records containing PHI
- Receive an accounting of health plan disclosures of PHI
- Restrict the use and disclosure of PHI
- Receive confidential communications
- Receive a Notice of Privacy Practices

This policy applies to member privacy rights including right to receive Notice of Privacy Practices and right, as received from a member or his or her authorized representative (requester), to request activity related to use or disclosure of PHI by the health plan personnel.

Responsibilities

The Medicaid Compliance Director acts as the corporate privacy officer. The health plan compliance director administers and operates the health plan compliance department and this department is responsible for implementing and maintaining the corporate process and requirements related to upholding protections afforded to members under federal and state privacy laws and regulations, and applicable contractual requirements, including responding to member privacy requests. The health plan's designated Compliance Manager, located in the health plan compliance department and reporting to the health plan Director of Compliance is responsible for conducting daily operations, which include:

- Verification of an individual's identity and authorization to make a request
- Review, disposition, and response to requests in compliance with HIPAA guidelines, including time standards

- Documentation of privacy requests and responses
- Tracking and reporting of requests and actions taken

Privacy Request Requirements

A privacy request must be submitted by the member or member's authorized representative.

A member's representative must provide documentation or written confirmation that he/she is authorized to make the request on behalf of the member or the deceased member's estate.

Except for requests for a health plan Notice of Privacy Practices, requests from members or a member's representative must be submitted to the health plan in writing.

Privacy Process Requirements

The health plan's processes for responding to member privacy requests shall include components for the following:

Verification

If the requester is the member, the health plan personnel shall verify the member's identity. If the requester is a member's authorized representative, the health plan personnel shall verify the requester's identity and confirm his or her authority to obtain the member information or act on behalf of the member. Verification examples include asking for the last four digits of member's Social Security Number or member's date of birth.

Review, Disposition, and Response

The health plan personnel review and disposition of privacy requests shall comply with applicable federal, state, and local laws and regulations, and applicable contractual requirements, including those that govern use and disclosure of PHI. Responses to privacy requests shall conform to guidelines prescribed by HIPAA, including response time standards, and shall include a notice of administrative charges, if any, for granting the request.

Documentation

The health plan or health plan personnel shall retain documentation of privacy-related materials and actions, including but not limited to, the following:

- Members' or authorized representatives' written requests and health plan personnel's written responses (e.g., copies of correspondence)—template approval or denial forms are available by contacting the health plan compliance department
- Electronic or hard copy records maintained by the health plan personnel that contain PHI used by health plan personnel to make privacy-related decisions about members
- The health plan policies and procedures governing privacy rights and use and disclosure of PHI
- Reports summarizing privacy requests, their disposition, and report time frames

Health plan personnel shall retain this documentation for at least six years or longer if state or local law or applicable contractual requirements require.

Use and Disclosure Guidelines

The health plan or health plan personnel are required to use and disclose only the minimum amount of information necessary to accommodate the request or carry out the intended purpose.

Limitations

A privacy request may be subject to specific limitations or restrictions as required by law.

Health plan personnel may deny a privacy request under any of the following conditions:

- The health plan does not maintain the records containing the PHI.
- The requester is not the member and the health plan personnel are unable to verify his/her identity or authority to act as the member's authorized representative.
- Prohibit the use of PHI by employer or plan sponsor for employment or other benefit-related decisions.
- The documents requested are not part of the designated record set (e.g., credentialing information).
- Access to the information may endanger the life or physical safety of or otherwise cause harm to the member or another person.
- The health plan is not required by law to honor the particular request (e.g., accounting for certain disclosures).
- Accommodating the request would place excessive demands on the health plan or health plan personnel's time and the health plan or health plan resources and is not contrary to HIPAA.

Prohibition of Intimidating Discriminating, or Retaliatory Acts

The health plan or health plan personnel are prohibited from intimidating, discriminating or retaliating against an individual for exercising his or her privacy rights under the HIPAA or and other applicable federal, state, and local laws and regulations privacy standard or for:

- Filing a complaint with the Department of Health and Human Services (DHHS)
- Participating in an investigation related to the health plan's compliance with the HIPAA privacy standards
- Opposing any practice by the health plan that the individual believes is unlawful, the health plan privacy officer (Compliance Director) shall investigate fully any allegation of intimidation, discrimination or retaliation. If the investigation reveals that intimidating, discriminatory or retaliatory behavior did occur, the health plan Compliance Manager or designee shall take appropriate action against the personnel responsible in accordance with the health plan policy and procedures.

REFERENCES:

- 45 C.F.R. (Code of Federal Regulations): relevant sections of the HIPAA that provide member privacy rights and place restrictions on uses and disclosures of protected health information (§164.520, 522, 524, 526 and 528)
- State and local laws and requirements
- Contract agreements and privacy related policies and desktop procedures

RELATED DOCUMENTS:

None

REVISION HISTORY:

Revision	Date	Description of Change	Committee
New	07/16/2015	Initial release.	Board of Directors
A	12/01/2015	Added NCQA elements.	Board of Directors
B	03/04/2016	Updated to current template. Updated to include all product lines.	Board of Directors
C	06/01/2017	Yearly review. Changed signatory from Anita Leal, Executive Director to Nancy Horstmann, CEO.	Board of Directors
D	04/24/2019	Yearly review. Removed Medicaid and CHIP from lines of business. Corrected minor typos.	Executive Leadership
E	05/04/2020	Yearly review. Made minor grammar correction. No change to content.	Executive Leadership
F	04/27/2021	Yearly review. No change to policy content.	Executive Leadership
G	03/22/2022	Yearly review. No change to policy content.	Executive Leadership
H	03/30/2023	Annual review. Minor changes to policy section to remove NCQA 2015 standards as there are no longer applicable.	Executive Leadership