VERMONT
AGENCY OF HUMAN SERVICES

AHS Policy Title: 6.05 VHC Information Privacy Policy

Policy Information

Revision Date:

09/01/2023

Revision Number: 1.1

Attachments/Related Documents:

none

Effective Date:

12/20/2013

☒ Trauma Informed Review

☒ Racial Equity Review

Authorizing Signature:

Jenney Samuelson,
Agency of Human Services Secretary

Policy Statement:

This Policy governs the collection, use, and storage of personally identifiable information (PII). This document is used by the State of Vermont, Agency of Human Services, and its contractors and grantees to guide their privacy practices in connection with the functions of Vermont Health Connect (VHC), the Health Benefit Exchange.

Background:

The Patient Protection and Affordable Care Act of 2010 (ACA) required the creation of health insurance exchanges (i.e., marketplaces) to help individuals find and enroll in affordable health insurance coverage. Vermont has implemented a state-run Health exchange. In May 2011, the Vermont legislature enacted its own comprehensive reform of healthcare delivery and payment that envisions a healthcare system decoupled from the traditional employer-sponsored insurance model, which ultimately evolves into a single-payer system. This law, Act 48 (An Act Relating to a Universal and Unified Health System), authorized VHC and established it within the Department of Vermont Health Access (DVHA), the department within the Agency of Human Services (AHS) responsible for administering the state's Medicaid program.

Definitions:

Personally Identifiable Information (PII): is information that can be used to distinguish -or trace an individual's identity, such as his/her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Types of PII VHC may collect, use, or disclose include, but are not limited to name, address, social security number, federal tax information concerning household income, citizenship data, and enrollment records. Please note: VHC will not be collecting health information from health care providers, insurers, or medical records. VHC may only collect, use, or disclose PII for purposes necessary to carry out VHC functions. The Policy and the underlying privacy standards apply to PII regardless of its format. For example: PII includes paper or electronic records, phone calls, recorded conversations, and photographic information.

For the purpose of this Policy, it is useful to distinguish between privacy and security:

- **Privacy**: refers to the rights of individuals to exercise some control over the way their personal information is collected, used, and stored. Privacy encompasses knowledge about who is authorized to access an individual's PII and under what conditions PU may be accessed, used, and/or disclosed to a third party. Privacy also encompasses providing individuals with a simple and timely means to access their PU, to dispute the accuracy or integrity of their PU, and to have erroneous information corrected.

- **Security (or Safeguards):** refers to the mechanisms in place to protect the privacy of PII. This includes the ability to control access to an individual's PII, as well as to safeguard an individual's PII from unauthorized disclosure, alteration, loss, or destruction. Security will be accomplished through managerial, operational, and technical controls implemented within VHC.

Scope:

This policy governs VHC Information Privacy protocols related to the collection, use, and storage of personally identifiable information and implementation of associated standards and procedures.

Roles and Responsibilities:

AHS Secretary – Responsible for making a final review and approval of this policy.

AHS Policy Committee - Responsible for making a final review of this policy.

DVHA Commissioner or Designee – Responsible for reviewing and approving this policy prior to AHS Policy Committee.

AHS Information Security Director; AHS Privacy Officer – responsible for:

- Creating procedures and standards to meet the requirements established in this policy.
- Reporting all matters pertaining to the AHS's compliance with this policy to the DVHA Commissioner/Designee and the AHS Secretary; and
- Ensuring that this policy is reviewed and updated (if necessary) at least annually.

Protocols:

General

The nature of VHC operations necessitates the collection, storage, and use of certain limited personal information so that VHC can make the right eligibility determinations for individuals, help those individuals enroll in coverage and, if applicable, provide financial assistance. VHC's need for and use of sensitive information may cause individuals to have concerns about the privacy and protection of their personal information. Unless individuals trust that the privacy and security of their personal and financial information is being protected, they will be reluctant to take advantage of VHC's benefits. VHC employees, contractors, and grantees who will access, use, or disclose Personally Identifiable Information (PII) through their work on VHC must be fully cognizant of these understandable concerns, must follow VHC policies and procedures to ensure the privacy and security of all PII, and will receive mandatory training regarding the privacy and security of PII. Data will be captured electronically from individuals and from State and Federal sources, such as the Centers for Medicare and Medicaid Services (CMS) and/or the Internal Revenue Service (IRS) and will be used and stored to accomplish VHC functions. VHC will operate through interactions with multiple electronic sources and interfaces. Consequently, VHC will be the repository for a large volume of sensitive PII using relatively complicated technology.

Information technology offers benefits for privacy protection by improving security, limiting access, monitoring users and stripping data of individual identifiers before it is shared with third parties. But technology does not resolve the larger policy questions and legal limits regarding how PII should be used and shared. The technology can help to protect information, but only a privacy policy and standards can articulate what limits are appropriate.

The following are important concerns regarding information privacy in VHC:

- Increasing the capacity to handle (collect, store, sort, and distribute) more information makes PII harder to protect.
- Increasing the potential to integrate information from different sources to support more informed decision-making may increase the likelihood of the use of information for unjustified purposes.
- Demanding increased capacity to link information brings heightened pressure for strong integrity of such information. The sensitivity of some types of information, like social security numbers and household income, requires robust controls on the use and dissemination of such information.
- Increasing the oversight by federal agencies can lead to civil and criminal penalties if PII is not adequately protected.
- Losing public confidence in AHS and VHC could undermine the goal of getting as many citizens as possible to take up coverage.
- Failing to implement certain programs if the privacy policies and procedures are not robust enough, and/or are not followed (e.g., if Federal Tax Information (FTI) is misused or IRS stops sending it) will result in delays, which could be detrimental to VHC.

As noted above, strong privacy protection can help to build client trust and ensure that when information is properly shared, it is complete and reliable, and only shared for the purpose for which it was intended. VHC will require access to certain PII about individuals who seek

coverage and financial assistance. Exacting privacy requirements to protect this PII have been established by the state and the federal governments. These requirements underlie this Policy and make adherence mandatory.

Information Privacy Protection Framework

This policy is based on the following information privacy protection framework. The purposes of this framework include:

- Creating and ensuring adherence to privacy-sensitive information handling practices within AHS which comply with the privacy requirements of Title I of the Affordable Care Act (ACA) and accompanying regulations, the Health Information Portability and Accountability Act (HIPAA) and accompanying regulations, and IRS Safeguards for Federal Tax Information (FTI).
- Providing consistency across operations in relation to how privacy issues are addressed.
- Building public and governmental confidence in the ability of AHS, DVHA and VHC to protect and manage PII in accordance with privacy principles that are consistent with national standards.

Additional Privacy Supports

This Policy is also supported by the following:

- Education and training to ensure that employees and business partners have the requisite knowledge and skills to implement the Policy and comply with its information privacy standards.
- A public information strategy to help individuals understand the limited purposes for which their personal information will be used, and how VHC plans to ensure the privacy and security of that information.
- Periodic privacy self-assessments of the state of PU protection within VHC.
- Incident response procedures for the reporting of privacy breaches and security incidents and to address claims from individuals that VHC or a business partner has committed an act that violates their privacy rights.
- Agreements with business partners to ensure their compliance with privacy requirements.
- A list of the types of data created, collected, used, and disclosed by VHC and the permitted uses of that data.
- A notice of privacy practices to advise individuals and the public about their privacy rights.

- Standard operating procedures (SOPs) applicable to performance of VHC's functions.

Types of Entities that Share PII in the VHC Environment

- Applicants
- Medicaid/CHIP Beneficiaries
- Contractors
- Qualified Health Plans (Insurers)
- Navigators
- Authorized Representatives
- State Shared IT Services
- VHC Enrollees
- Business Partners
- Employers & Employees
- Employees, Agents, or Contractors of VHC
- Agents and Brokers
- External sources of data (third party Federal or State sources)
- Certified Application Counselors

Summary of VHC Privacy Requirements

This section describes the requirements VHC must adhere to in implementing this Privacy Policy. Each specific requirement and the methods chosen to ensure compliance with each are set out in more detail within separate written standards, guidelines, and procedures. Copies of these will be posted on the VHC website.

The requirements concern:

1. Creation, collection, use, and disclosure limitations
2. Individual Access, Choice, and Correction
3. Openness and Transparency
4. Data Quality and Integrity
5. Safeguards
6. Accountability

Requirements:

1. Creation, Collection, Use, and Disclosure Limitations

1.1 Purpose of creating, collecting, using, and disclosing personal information

Where VHC creates, collects, uses, or discloses PII for the purposes of determining eligibility for enrollment in a qualified health plan, determining eligibly for other insurance affordability programs, VHC may only use or disclose such PII to the extent such information is necessary to carry out the functions of VHC.

1.2 Manner of information creation, collection, use, and disclosure

VHC will collect PII by lawful, fair, and non-intrusive means to prevent undue pressure or coercion being placed on individuals when their information is collected. It will create, collect, use, and disclose PII in a manner that is consistent with VHC privacy and security standards, and in compliance with State and Federal law.

1.3 Notification regarding data collection

Before PII is collected from individuals utilizing VHC or by third parties (see also section 1.5), reasonable steps will be taken to inform them about why their PII is being collected, the use to which the information will be put, and their rights to access and correct this information.

1.4 Source of PII

Where practicable, VHC will collect PII directly from individuals or from a trusted State or Federal data source where their information is held.

1.5 Notification regarding data collection from third parties

VHC will collect some information about individuals from third parties such as a State or Federal data source. VHC will advise individuals that this collection will occur as part of VHC processes.

2. Individual Access, Choice, and Correction

2.1 Access

Individuals will be provided with a simple and timely means to access their PII in a readable form and format. To ensure the PII requested is not inadvertently disclosed to an unauthorized individual, before providing access, the identity and authority (when someone is acting as the designated representative on behalf of another individual) of the individual making the request will be validated.

2.2 Choice

Individuals will be provided a reasonable opportunity to make informed decisions about the collection, use, and disclosure of their PII. As noted above, VHC will offer public educational forums, make available a Notice of Privacy Practices, and provide training to customer service representatives and Navigators.

2.3 Correction

Individuals will be provided with a means to dispute the accuracy or integrity of their PII. VHC will have a procedure for correcting inaccurate information and documenting a dispute if a request is denied. The methods made available to individuals for executing these processes will be simple and clearly communicated. The appropriate VHC users will handle the requests for corrections in a timely manner.

3. Openness and Transparency

3.1 Open and Transparent Use of PII

Policies, procedures, and technologies that directly affect individuals and/or their PII will be open and transparent. Prior to providing their information, individuals must have a clear understanding of the reasons for the collection of their information, who it will be shared with, how it will be used, how it is being protected, how long it will be kept, and how it will be destroyed.

3.2 Clearly Written Materials

Whenever possible, materials will be easy to locate, clearly written, and easily understandable by their intended audiences. Explanatory documents will be consistent, accurately reflect information handling practices, and remain current as any change in practice occurs.

3.3 Privacy Notices

Privacy notices and policies posted to the websites will address all applicable state and federal legal requirements governing web privacy content, including topics such as connecting to external websites and the use of such techniques as cookies, beacons, etc.

3.4 Distribution of Information Regarding Openness and Privacy

Information about openness and transparency will be provided through a variety of methods, including:

- Privacy statements on forms and notices.
- Notice of Privacy Practices posted for all portals, VHC and application interfaces.
- Privacy statements on all log-on screens.

4. Data Quality and Integrity

4.1 Accuracy

In order to ensure quality and integrity of data, it is important that the personal information created, collected, used, and disclosed by VHC be accurate, complete, and up to date. VHC will take reasonable steps to ensure that information it collects and uses is accurate and has not been altered or destroyed in an unauthorized manner.

4.2 Methods for Ensuring Data Integrity

To meet the requirement of ensuring that PII remains accurate, complete, and up to date, VHC will use methods including, but not limited to, the following:

- Tracking PII movement and uses. VHC will identify types of PII and map its entry and exit from VHC to ensure that information is created, collected, used, and disclosed only for authorized purposes to authorized individuals and entities.
- Reviewing PII samples selected through a defined risk management process to ensure integrity, accuracy, relevancy, and timeliness.
- Tracking disputes regarding PII.
- Validating all PII to ensure accuracy, completeness, and timeliness of information that is created, collected, used, or disclosed by VHC.
- Establishing a governance structure that provides leadership and visibility for compliance with this Privacy Policy.

5. Safeguards

5.1 Methods for safeguarding PII

To meet the requirement of ensuring that PII will be protected with reasonable operational, administrative, technical, and physical safeguards, VHC will, in addition to adopting VHC security standards and measures:

- Monitor the current state of compliance with the ACA's privacy and security requirements as set forth in 45 C.F.R. §155.260 in a variety of ways, including using automated tools, self-assessment checklists, and independent third-party reviews.
- Develop a privacy breach response plan that addresses identification, reporting, investigation, notification, and mitigation.
- Implement a process for verifying the ongoing compliance of the individuals and entities with whom PII is shared.

6. Accountability

6.1 The all-encompassing privacy standard

Accountability brings together all of these privacy requirements. VHC will not create, collect, use, or disclose information unless done so in a manner consistent with the Privacy Policy of VHC. It is the responsibility of VHC to ensure that all employees, contractors, and grantees receive training about and are accountable for meeting VHC privacy requirements. VHC and its contractors and grantees will ensure adherence to the requirements above through appropriate monitoring. In addition, VHC will put in place procedures for reporting and mitigating non-adherence and breaches. As appropriate, VHC will notify affected individuals when a privacy incident has occurred.

Enforcement:

It is the responsibility of VHC to ensure that its employees, contractors, and grantees comply with this Privacy Policy and protect the confidentiality, integrity, availability, and accuracy of PII while preventing unauthorized or inappropriate access, use, or disclosure.

The AHS Secretary may initiate reviews, assessments, or other means to ensure that policies, guidelines, or standards are being followed.

Authorities:

- IRS Publication 1075 (Rev. 11-2021)
- Affordable Care Act 45 CFR §155.260
- Minimum Acceptable Risk Standards for Exchanges (MARS-E) Document Suite, Version 2.0

References:

ACA	IRS	CMS
45 CFR §155.260	Pub 1075 (Rev. 11-2021)	MARS-E (V 2.0)

Document Review and Revision Control

Version	Review Date	Author/Reviewer	Description
1.1	09/01/2023	Greg Needle	Renewal

Appendix:

None.