AHS Policy Title: 6.04 VHC Privacy Governance Policy

Policy Information

Revision Date:

09/01/2023

Revision Number: 1.1

Attachments/Related Documents:

none

Effective Date:

12/24/2013

☒ Trauma Informed Review

☒ Racial Equity Review

Authorizing Signature:

Jenney Samuelson | Agency of Human Services Secretary

Policy Statement:

The purpose of this policy is to establish guidelines and standards for the governance of the privacy program as part of the functions of Vermont Health Connect (VHC).

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. The Affordable Care Act requires state-run health insurance exchanges to establish and maintain security and privacy programs to protect users' personally identifiable information and to establish a governance structure to maintain and enforce the programs (45 CFR 155.200).

Definitions:

Personally Identifiable Information (PII):

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PH can become PII whenever additional information is made publicly available in any medium and from any source that, when combined with other available information, could be used to identify an individual.

Federal Tax Information (FTI):

FTI includes tax return or tax return information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS pursuant to an Internal Revenue Code (IRC) § 6103(p)(2)(B) Agreement.

Services:

Services include work performed by a Business Partner for or on behalf of AHS to perform VHC Minimum Functions, which requires the use and/or disclosure of personally identifiable information (PII) (including Personal Health Information). "Services" does not include any work done that is not required to perform Minimum Functions.)

Minimum Functions:

Minimum Functions include all work performed (or contracted to be performed) pursuant to subparts D, E, F, H, and K of 45 CFR 155.200, if such work requires the Business Partner to create, collect, use, or disclose PU.

Business Partner:

Business Partner is an individual or entity who enters into an agreement with VHC and who will gain access to PII submitted to VHC or will collect, use or disclose PII gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing the functions outlined in the agreement with VHC.

Scope:

This policy applies to the VHC Privacy Officer, VHC Security Officer, staff appointed to be part of a VHC privacy and/or security team, and all other applicable AHS employees.

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:

One of the guiding principles for a health insurance exchange is the "minimum necessary" rule, which requires VHC to disclose only the minimum amount of PII to accomplish each intended purpose. AHS shall take all appropriate steps to ensure that the collection, creation, use and disclosure of PII is limited to, and consistent with, the minimum functions defined in 45 CFR 155.260.

Privacy Officer Responsibilities

In order to ensure the privacy and protection of individuals' PII, the Privacy Officer shall:

1. Administer and oversee the VHC Privacy Policy and all applicable VHC Standards and Guidelines.
2. Be responsible for the oversight and protection of personally identifiable information (PII).
3. Collaborate with AHS departments, and other entities including the Attorney General's Office and the Vermont Department of Information and Innovation to maintain VHC compliance with policies, procedures and federal and state laws.
4. Confer with the Security Officer regarding the establishment of physical safeguards and implement technology solutions in line with this concept, according to CMS and IRS guidance, and in adherence to 45 CFR155.260.
5. Maintain a complete understanding of relevant laws and regulations to create and enforce internal policies and procedures surrounding the retrieval and management of PII.
6. Develop and implement privacy initiatives in the areas of privacy leadership, privacy risk management and compliance, information security (in coordination with the Security Officer), incident response, notice and corrective action, privacy training and awareness, and accountability.
7. Partner with appropriate AHS employees to oversee the creation and modification of training materials, and to monitor staff compliance with training requirements.

8. Coordinate with the Security Officer to ensure that the technological infrastructure can meet privacy requirements.
9. Develop and maintain a privacy breach process. When a privacy breach is reported, follow the breach process to report to CMS and the VT Attorney General's Office, investigate the facts, resolve any issues, and work in tandem with the Security Officer and/or legal authorities if necessary, as expediently as possible.
10. Coordinate the revisions of policies as necessary to comply with changes in the law, regulations, and accreditation requirements and due to changes in business operations.
11. Serve as liaison to regulatory and accrediting bodies.
12. Provide reports regarding the status of compliance.
13. Ensure that Business Partners comply with privacy policies and procedures.
14. Conduct periodic reviews to assess compliance with privacy policies and procedures.
15. Develop and update short, simple, and informative materials to enable AHS staff and business partners to self-assess and identify privacy issues that should be escalated to the privacy officer.
16. Conduct periodic privacy assessments of the state of PII protection within the VHC. The Privacy Officer shall also work with the Security Officer to ensure that an assessment of privacy practices is included as an integral part of periodic risk assessments.
17. Coordinate with respective privacy and security teams in the development and review of privacy policies and procedure before approval by the applicable AHS Commissioners or designee.

Enforcement:

The Privacy Officer and Security Officer are responsible for 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. 11-2016) – Tax Information Security Guidelines For Federal, State and Local Agencies
- Affordable Care Act 45 CFR §155.200 – Function of an Exchange
- Affordable Care Act 45 CFR §155.260 – Privacy and security of personally identifiable information

References:

ACA	IRS	IRC
45 CFR §155.200	Pub 1075 (Rev. 11-2021)	§ 6103(p)(2)(B)
45 CFR §155.260		

Document Review and Revision Control

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

Appendix:

None.