VCN Data Repository Policies and Procedures

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **VCN Data Use Policies**

VCN Policy Number: **2015100**
Effective Date: **12/01/15**
Revised Date: **5/2/16**

The purpose of this policy is to describe appropriate and acceptable use of the data that resides in the VCN Data Repository:

Compliance with State and Federal Regulations:

The data stored in the VCN data Repository will be managed in accordance with all applicable privacy and security laws of the state of Vermont, including Federal laws that apply. This includes, but is not necessarily limited to: Vermont Patient Privilege, HIPAA and 42 CFR part 2. Data will be managed to the most stringent standard, thereby complying with all lesser standards.

Data Use:

The primary purpose of the VCN data Repository is to compile data from our member agencies to facilitate communication to our myriad stake holders, and to provide centralized data analysis for our system of care. Additionally the Repository will be used to provide data analysis for our individual members. Lastly, it is our intention to connect the VCN Repository with other data resources in the State of Vermont, as federal regulations allow, to provide the information needed to support fully integrated care.

Types of use:

Reports to Stake holders:

The VCN Data Governance Committee will approve regular, periodic reporting that is required by State or Federal agencies. The specifications and descriptions of these reports will be maintained by VCN and made available to member agencies on request.

Centralized Data Analysis:

The VCN Data Governance Committee will approve data analytics and reporting that are created for the simultaneous use of all member agencies. The Data Governance Committee will serve as a central point for data analytic requests. Requests will be submitted, evaluated and processed per Data Repository policy 2015300: Data Request Policy and Procedure. It is expected that member agencies will have an active role in developing and using these analytics, and will thus be informed throughout the process. The specifications and descriptions of these analysis will be maintained by VCN and made available to member agencies on request.

Automated connectivity from other data sources to the Repository:

Data extracts and automated interfaces will only be constructed that fully conform to all applicable regulations. Interfaces will be vetted and approved by the member agencies through the Data Governance Committee. The specifications and descriptions of these interfaces will be maintained by VCN and made available to member agencies on request.

Data Transport:

In compliance with HIPAA standards, data that contains Protected Health Information (PHI) will only be transported using secure methods of transport to ensure, to the greatest extent possible, that only the intended recipient will receive the data. Regular data imports to the Repository will be through established secure means such as dedicated secure connections, or encrypted transport mechanisms, or both. Ad hoc data transfers may likewise only be moved by secure means.

Data use restrictions and guide lines:

Data collected and maintained by each member agency will be maintained such that a sending agency will be able to access and analyze their own data without restriction. Member agencies will manage access to the data that they contributed, for staff within their own organizations, as appropriate and in compliance with applicable regulations. They will also comply with VCN Policy 2015105 Data Access.

Data collected and aggregated for system wide analysis will only be accessible as agreed upon by participating VCN members. This data will be restricted to de-identified data, and is intended for broader analysis such as trending and population management, as opposed to specific tasks that require client identities.

Accessing, downloading or transferring of data must be in compliance with the Repository policies and procedures. Exports or data transfers will only go to vetted and agreed upon entities and will be managed by the VCN member agencies via the Governance Committee. VCN will record and file the data request, purpose for an extract and the expectations for use of that data. The data will not be used for any purpose for which it was not originally requested without express permission. All recipients of data will have appropriate agreements in place, such as Business Associates Agreements etc., and will be bound by them.

Redisclosure:

As of this writing there is no technical solution available to the Repository to meet the redisclosure and consent requirements of 42CFR Part 2. As a result, information that falls under 42 CFR Part2 will not be allowed to leave the Repository until such time as technical or regulatory changes make it possible.

Data transfer within the Repository:

In its current incarnation the Repository is not designed to facilitate data transfer between member agencies. The Repository will aggregate data to facilitate consolidated reporting analysis and interfaces to appropriate third parties. Data from individual member agencies will remain logically segregated, and will not be moved from one member agency to another at this time.

If it is determined that this capability is necessary in the future, it will be done in full compliance with all applicable laws and regulation, and a procedure will be developed and agreed upon by all participating members.

Restrictions on commercial use:

The VCN data Repository is not intended as a commercial venture. Information may not and will not be sold or disclosed to any third party for commercial purposes. Data that is exported from the Repository will not be used for commercial purposes, and recipients of same will acknowledge this in writing before receiving data.

Signature: _____ Date: _____

Name: Simone Rueschemeyer

Title: Executive Director Vermont Care Network

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **Data Access Policy**

VCN Policy Number: **2015105**
Effective Date: **12/1/2015**
Revised Date: **5/2/2016**

The purpose of this policy is to describe how access to the VCN Data Repository is to be granted, managed, and revoked:

Access Assignment:

The Repository security administrator(s) will work with the member agencies to identify security delegates for each member agency. Agencies will also identify to the repository security administrator, their respective HIPAA electronic security officer. Agencies will be responsible for updating the repository security administrator with changes of either the HIPAA electronic security office, or the security delegate.

Access to the data repository for end users will be assigned through their respective security delegate. The security delegates will be responsible for maintaining the list of active users, and revoking inactive user's access to the Repository. Security delegates will also be responsible for setting and maintaining the appropriate access level for the users.

Revoking Access:

Staff that leave the employment of member agencies will have their access revoked in a timely fashion by their respective security delegate.

VCN reserves the right to revoke access for any user if there is reason to believe they are compromising the security or integrity of the Repository or its data, or they are intentionally or unintentionally violating HIPAA regulations. VCN will notify the associated HIPAA electronic security officer of such an event in a timely fashion.

Access and security audits:

Periodically, or on request, the Repository will produce a report of each agencies users, their respective access role, and current status. The purpose of this report will be to aid agencies in their maintenance of their user access. Details of this activity may be found in VCN Policy 2016310; Access Auditing Policy.

Consistent with HIPAA compliance, the data repository will maintain an audit trail of user's access to the Repository. Reports of user activity will be made available to any member security delegate that requests it.

Unauthorized access to data:

If an audit indicates an unauthorized access, or attempt of unauthorized access to the Repository or portion of the Repository, from within the system, the repository security officer will investigate and file a report with the agency that the user is associated with and the agency that owns the affected data set. Affected agencies will be notified as appropriate per VCN Data Repository policy number 2015205 Data Breach Policy.

Breaches of the repository from outside the member community will be investigated by and reported on by the Repository vendor. Affected agencies will be notified as appropriate per VCN Data Repository policy number 2015205 Data Breach Policy, and the repository vendor policy.

Signature: _____

Name: Simone Rueschemeyer

Title: Executive Director, Vermont Care Network

Date: _____

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **VCN Data Breach Policy and Protocol**

VCN Policy Number: **2015205**
Effective Date: **12/01/15**
Revised Date: **3/7/16**

Purpose: The purpose of this policy is to establish VCN response to a suspected data breach of the VCN Repository:

Definitions:

Breach: For the purposes of this policy, breach will be defined as per HIPAA Privacy and Security Rule 45 CFR Section 164.402. (See attached procedures below)

Internal breach: A breach that occurs, through an affiliated member organization, which might otherwise have legitimate access to the Repository. Examples of this would be; unauthorized access to a member system that results in subsequent unauthorized access to the Repository, or inappropriate use of otherwise legitimate agency credentials to gain access to the Repository.

External breach: A breach that occurs through the Repository vendor host system, having no direct relation to a member system's access. Examples would include gaining unauthorized physical access to host computing resources, or accessing VCN hosted systems through adjacent systems in the host environment.

Policies:

Internal Breaches:

Member Breaches:
If a member agency experiences a data breach that may or actually does expose the Repository to unauthorized access, the member agency will notify the Repository Security Officer promptly. The Repository Security Officer will either unilaterally, or in cooperation with any affected agencies conduct a breach review and risk assessment, as outlined below, and develop an appropriate response plan for the Data Repository. Member agencies will be responsible for investigating and remediating their own systems beyond those related to the Repository.

VCN Discovered Breach:
If a breach is discovered as a result of VCN security audits, the Repository Security Office will notify the affected agencies promptly. The Repository Security Officer will then either unilaterally, or in cooperation with any affected agency, conduct a breach review and risk assessment and develop an appropriate response plan. The Repository Security Officer will promptly share the results with any affected agency. As with a member breach, member agencies will be responsible for investigating and remediating their own systems beyond those related to the Repository. VCN investigations will be primarily focused on the Repository, and immediately related systems.

External Breaches:

In the event that the VCN Data repository experiences an external breach, the VCN Data Repository Security Officer will work with the NORC data security personnel as necessary to assist their investigation. The VCN Security Officer will report back to the member agencies promptly, and provide updates as to the results of any and all investigations and any resulting mitigation and remediation plans. Reviews and remediation of the host system will meet or exceed the standards outlined below in this policy or the laws of the State of Vermont, whichever is more stringent.

Procedure:

BREACH NOTIFICATION REVIEW AND RISK ASSESSMENT

Purpose

This document provides a review protocol for the AGENCY to follow in determining whether to provide notification of a breach of unsecured protected health information ("PHI") under the HIPAA Privacy and Security Rules as modified by the Omnibus Final Rule and or a breach of personally identifiable information (PII) under Vermont's Security Breach Notice Act.

Upon receipt of a report, depending on the type of alleged violation, the privacy officer or security officer, in cooperation with the compliance officer, will initiate an investigation to make a determination as to whether or not the violation is a breach and must be reported to the individual, the federal government and in some circumstances the Vermont Attorney General.

If the privacy or security violation is ongoing, the privacy officer or security officer will take immediate steps to stop it regardless of its impact on the investigation.

HIPAA

I. Basic Definition

A. A breach is defined in the HIPAA Privacy and Security Rules, 45 CFR Section 164.402, as:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Regulations which compromises the security or privacy of the PHI.

An acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Regulations is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the PHI has been compromised.

B. The definition of breach excludes:

(i) unintentional access by workforce member in good faith which does not result in further unauthorized use or disclosure;

(ii) inadvertent disclosure by person authorized to use PHI to another workforce member and PHI is not further used or disclosed; or

(iii) disclosure of PHI where there is good faith belief that unauthorized person would not reasonably have been able to retain it.

C. To determine whether an unauthorized acquisition, access, use or disclosure of PHI does not constitute a breach, a risk assessment of at least the following factors must be made and well documented:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the PHI or to whom the disclosure was made;
(iii) Whether the protected health in-formation was actually acquired or viewed; and
(iv) The extent to which the risk to the PHI has been mitigated.

II. Breach Assessment Protocol.

STEP ONE: Determine whether there has been an impermissible use or disclosure of PHI under the Privacy Rule.

For an acquisition, access, use or disclosure of PHI to constitute a breach, it must:
(i) involve unsecured (unencrypted) PHI;
(ii) constitute a violation of the Privacy Rule; and
(iii) not be excluded from the breach definition under II(B) above.

STEP TWO: If there was an impermissible use or disclosure of PHI, is the agency able to demonstrate that there is a low probability that PHI has been compromised? To answer this, the agency must undertake a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

To assess this factor the agency must evaluate the nature and the extent of the PHI involved, such as whether the disclosure involved information that is of a more sensitive nature. *For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, this may involve considering not only the nature of the services or other information but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).*

Considering the type of PHI involved in the impermissible use or disclosure will help entities determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests. Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, the agency should determine whether there is a likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information. *For example, if the agency impermissibly disclosed a list of patient names, addresses, and client identification numbers, the PHI is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised, dependent on an assessment of the other factors discussed below. Alternatively, if the agency disclosed a list of client discharge dates and diagnoses, the agency would need to consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the agency, or whether the*

unauthorized recipient of the information may have the ability to combine the information with other available information to re-identify the affected individuals.

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

The second factor requires consideration of the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made. The agency should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. *For example, if PHI is impermissibly disclosed to another entity obligated to abide by the HIPAA, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.*

If the information impermissibly used or disclosed is not immediately identifiable, the agency should determine whether the unauthorized person who received the PHI has the ability to re-identify the information. *For example, if information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work.*

(iii) Whether the protected health in-formation was actually acquired or viewed; and

The third factor requires an investigation of an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. *For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed. In contrast, however, if a covered entity mailed information to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.*

(iv) The extent to which the risk to the PHI has been mitigated.

The final factor included in the final rule requires the agency to consider the extent to which the risk to the PHI has been mitigated. The agency should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

The agency may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.

****

The analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor discussed above. Other factors may also be considered where necessary. The overall probability that the PHI has been compromised must be evaluated by considering all the factors in combination. The written risk assessment must be thorough, completed in good faith, and the conclusion reached reasonable.

STEP THREE: If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required. <u>The agency may decide to skip Step Two and go ahead and provide notification without evaluation of the probability that the PHI has been compromised</u>.

III. Breach Notification

If it is determined that notification of breach is required under the above analysis and, if it involves social security, financial or driver's license number information, notice shall also be made in compliance with Vermont's Security Breach Notice Act, 9 V.S.A. § 2435. See section below regarding these breaches. Additionally, appropriate measures should be taken to address associated effects of the breach, such as arranging a system or assigning responsibility to communicate with clients who have questions.

A. Notification to individuals. Following the discovery of a breach of PHI, notify each individual whose PHI has been, or is reasonably believed by the agency to have been, accessed, acquired, used, or disclosed as a result of such breach.

B. Discovery of breach. A breach shall be treated as discovered as of the first day on which such breach is known, or, by exercising reasonable diligence should have been known. The agency shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence should have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the agency.

C. Timeliness of notification. Provide notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

D. Content of notification. The notification shall include, to the extent possible:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the agency is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

E. Methods of individual notification.

(1) Written notice.

(A) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) If known that the individual is deceased and address of the next of kin or personal representative of the individual is available, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

(A) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(B) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(i) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the agency, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(ii) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's PHI may be included in the breach.

(3) Urgent situations - additional notice. In any case requiring urgency because of possible imminent misuse of PHI, information should be provided to individuals by telephone or other means, as appropriate, in addition to notice otherwise required.

F. Notice to the media. For a breach of PHI involving more than 500 residents of a State or jurisdiction, notify prominent media outlets serving the State or jurisdiction.

G. Notification to the Secretary. Notification to the Secretary of the United States Department of Health and Human Services is required:

(1) Breaches involving 500 or more individuals. For breaches involving 500 or more individuals, provide notification to the Secretary contemporaneously with the notice to the individuals and in the manner specified on the HHS Web site. Note there could be a situation when notification is required to the Secretary but media notice is not required because the 500 individuals came from different states.

(2) Breaches involving fewer than 500 individuals. For breaches involving fewer than 500 individuals, a log or other documentation of such breaches must be maintained and, not later than 60 days after the end of each calendar year (by March 1), provide notification for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.

IV. Breach Mitigation/Prevention

Following any event requiring breach assessment, consider what actions can be taken to mitigate harm of unauthorized use or disclosure of PHI and to prevent it in the future. Establish a follow up work plan and document all efforts taken. Be prepared for the potential that the Office of Civil Rights may audit compliance with all provisions of the HIPAA Privacy and Security Rule.

Vermont

I. Basic Definitions

"Personally identifiable information" (PII) means an individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or data elements are not removed or protected (e.g. encrypted) that makes them unreadable or unusable by unauthorized persons:

(a) A full Social Security number;
(b) A driver's license number, non-driver ID card number;
(c) A financial account number, credit or debit card number; or
(d) Account passwords or personal identification number or other access codes for a financial account.

"Security breach" is the unauthorized acquisition of information of electronic information, or a belief of an unauthorized security breach, that compromises the security, privacy or integrity of the information maintained by the agency. Breach does not include good faith but unauthorized acquisition of the PII by a workforce member for a legitimate purpose as long as the PII is not used or a purpose unrelated to the agency's business or is further disclosed.

"Security breach" **does not include** good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the agency for a legitimate purpose of the agency, provided that the personally identifiable information is not used for a purpose unrelated to the agency's business or subject to further redisclosure.

II. Breach Assessment

To determine if there was a breach under the State's Security Breach Notice Act, the agency must determine if the Personally Identifying Information (PII) has been acquired or is reasonably believed to have been acquired by an unauthorized person. The following factors, among others, must be considered:

(a) indications that the information is in the physical possession and control of a person without valid authorization (e.g. lost laptop);
(b) indications that the information has been downloaded or copied;
(c) indications that the information was used by an unauthorized person (e.g. fraudulent account opened); or
(d) that the information has been made public.

III. Breach Notification

Notification to Individuals. Following the discovery of a breach, the individual will be notified in the most expedient time possible and without unreasonable delay, but no later than 45 days after the discovery, consistent with the legitimate needs of the law enforcement agency, with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data system.

The notice to the individual may be delayed upon request of a law enforcement agency. The law enforcement agency may request a delay if it believes that notification may impede a law enforcement investigation, or national or homeland security investigation or jeopardize public safety or national or homeland security interests. If the request is in a manner other than in writing, the agency will document the request in writing and include the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The agency will provide notice to the individual without reasonable delay upon receipt of a written communication from the law enforcement agency withdrawing its request for delay.

Notification to Attorney General. The agency shall notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 days, consistent with the legitimate needs of law enforcement, of the discovery of the security breach or when the agency provides notice to the individuals.

(a) If the date of the security breach is unknown at the time notice is sent to the attorney general, the agency shall send the attorney general the date of the breach as soon as it is known.
(b) The agency shall notify the attorney general of the number of Vermonters affected, if known to the agency, and shall provide a copy of the notice provided to individuals.
(c) The agency may send to the attorney general a second copy of the notice, from which is redacted the type of PII that was subject to the breach, and which the attorney general shall use for any public disclosure.

Content of Notice. The notice to an individual shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the agency:

(a) The incident in general terms.
(b) The type of PII that was subject to the security breach.
(c) The general acts of the agency to protect the PII from further security breach.
(d) A telephone number, toll-free if available, that the consumer may call for further information and assistance.
(e) Advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.
(f) The approximate date of the security breach.

Method of Notice. Direct notice to individuals may be provided by one of the following methods:

(a) Written notice mailed to the individual's residence;
(b) Telephonic notice provided that telephonic contact is made directly with each affected individual, and the telephone contact is not through a prerecorded message.
(c) Electronic notice, for those individuals for whom the agency has a valid email address if the agency does not have an address or a telephone number, the agency's primary method of communication with the individual is by electronic means, the electronic notice does not request or contain a hypertext link to request an individual provide personal information, and the electronic notice conspicuously warns individuals not to provide personal information in response to electronic communications regarding security breaches.
(d) Substitute Notice. If the agency demonstrates that the cost of providing written or telephonic notice to affected individuals would exceed $5,000.00 or that the affected class of affected individuals to be provided written or telephonic notice exceeds 5,000 or the agency does not have sufficient contact information. The substitute notice shall consist of all of the following:
    i. Conspicuous posting of the notice on the agency's website page; and
    ii. Notification to major statewide and regional media.

Misuse is not reasonably possible. Notice is not required if the agency establishes that misuse of personal information is not reasonably possible and the agency provides notice of the determination that misuse of personal information is not reasonably possible. If the agency establishes that misuse of the personal information is not reasonably possible, the agency shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the attorney general.

If the agency establishes that misuse of personal information was not reasonably possible and subsequently obtains facts indicating that misuse of personal information has occurred or is occurring, the agency shall provide notice to the individual and the attorney general.

Additional notification: consumer reporting agencies. If the agency provides notice to more than 1,000 individuals at one time, the agency will notify, without reasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. Note - a consumer reporting agency is an agency that regularly engages in the practice of assembling or evaluating, and maintaining files, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity.

Signature: _____

Name: Simone Rueschemeyer

Title: Executive Director Vermont Care Network

Date: _____

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **Data Quality Guidelines**

VCN Policy Number: **2015108**
Effective Date: **12/01/15**
Revised Date: **10/19/15**

The purpose of this policy is to describe data quality guidelines and set expectations for members that are participating in the Data Repository.

Member agencies that are contributing data to the Repository will have their own procedures and training in place to ensure that the data they collect is as complete, accurate and consistent as possible. VCP will publish standards for data quality, for contributing members. All members will meet or exceed these standards for data quality.

The Repository will provide member agencies with feedback reports that can be used to monitor, maintain and improve data quality. VCP, as needed, will provide support in the form of documentation, reference materials and training to assist members in improving the quality of the data that is contributed to the repository.

Member agencies that are contributing to the data repository will supply data extracts and updates in a timely fashion. The Repository will process and provide feedback on batch uploads promptly. Feedback reports for real time data feeds will be scheduled to run frequently in order to provide members with sufficient feedback to support their data quality maintenance and improvement efforts.

Data quality analysis and reports may be provided to third party stakeholders to demonstrate the quality of the data in the Repository. Data quality reports will not include EPHI, and will be abstracted from de-identified data. Member agencies will be notified of such reporting.

Signature: _____
Name: Simone Rueschemeyer
Title: Executive Director Vermont Care Network
Date: _____

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT**:** **Data Retention Policy**

VCN Policy Number: **2015106**
Effective Date: **12/1/2015**
Revised Date:

The purpose of this policy is to describe the data retention period for data that is held in the Vermont Care Network (VCN) Data Repository:

Signature:
Name: Simone Rueschemeyer
Title: Executive Director Vermont Care Network
Date:

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **Data Request Policy and Procedure**

VCN Policy Number: **2015300**
Effective Date: **1/1/2016**
Revised Date: **2/22/16**

Purpose: The purpose of this policy is to describe how data, in the form of report(s) or data analysis may be requested from the VCN Data Repository and how those requests are processed and fulfilled.

A request for data from the VCN Data repository may come from:

- A VCN Member agency
- VCN
- State agency: AHS, DMH, GMCB, DVHA etc.
- Federal Agency
- A third party with a legitimate interest: I.E. The State Legislature, One of Vermont's ACO etc.
- An entity that is a partner or other member of the healthcare community.

What do we do if we receive a request from law enforcement?

Receipt of a completed request in no way obligates VCN or its members to fulfil the request. The steps for processing a data request are as follows:

1.) A completed request form is received by the Data Governance Committee:
2.) The request is scored by members of committee or their appointees
3.) Based on the scoring, and discussion within the committee, the request is accepted or rejected.

If a request is rejected: A rejected request is returned to the submitter with a brief explanation of the reason for rejection.

Fulfilling requests: If a data request is accepted by the committee, further evaluation by the committee, or its designees, will prioritize the request among others in the queue for development. Requests will be processed in order of priority established by the committee. Records of the data requests, scores, and status will be maintained by VCN.

Sample report request and request scoring sheets are attached.

Request Sheet:

VCP Data Analytics Request Form

Requestor (primary contact)

Requestor Name:		Request Date:	
Requestor Organization:		Requested Delivery Date:	
Requestor Email:			
Requestor Phone:			

Grant or Associated Funding Source:		Frequency: (Once, Daily, Weekly, Monthly etc.):	
Governing or Regulatory Body or Related Standard(s): I.E. ACO, Outcomes, COE, DA, DMH, ADAP:		Number of recipients of output:	
Organization that will be receiving this information:		Output Method: (CSV, XLS, HL7, Other):	
Re-Release/ Re-Disclosure:(Will this data be going beyond the requesting organization?):		Identifiable Data (PHI):	

Brief Description:	Calculations:
Filters:	Output Columns:
Grouping / Sub Totals / Totals:	Additional Comments:

VCN Repository Data Request Scoring Sheet

Brief Description: *Description of request goes here.*

One Time Request ☐
Recurring Report ☐

Notes: enter a number in the score column. Higher is more likely to move forward

Category	Item	Recommended score		Score
Difficulty		Yes	No	
	Is there an existing model in place?	10	0	
	Is it similar to, but different from, existing?	5	0	
	Totally new idea?	0	10	
	Are new data elements required?	0	10	
Origin	Federal Mandate	10	0	
	State Mandate	10	0	
	ACO	10	0	
	State Request	5	0	
	DA System wide request: Committee or Group	10	0	
	Individual DA	5	0	
	Other Body			
	Individual Contributor			
Funding	Is there funding associated? (amount of funding should be reflected in score)	10	0	
Impact	Executive level request impacting entire system (something all agencies could use)			
	Upper management request with broad impact (something all agencies could use)			
	Upper management request with intra agency impact (something all programs in a given agency would use)			
	Middle management with cross agency impact (something all agencies could use)			
	Middle management with intra agency impact (something all programs in a given agency would use)			
	How many clients would be impacted?	Lots = 10	few = 1	

	How many agencies would be impacted?	All = 10	few = 1	
	How many staff need it?			
	Pilot: If effective, this may be replicated across the system			

Purpose	Clinical	
	Political	
	Funding requirement	
	Operational	

Other	Other reasons that this is a good idea that we should consider	

Total Score	0

Signature: _____

Name: Simone Rueschemeyer

Title: Executive Director Vermont Care Network

Date: _____

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **User Access Auditing Policy**

VCN Policy Number: **2016310**
Effective Date: **6/1/2016**
Revised Date: **5/2/2016**

Purpose: The purpose of this policy is to document the procedure for confirming and maintaining appropriate user access to the VCN Data Repository (DR). In addition this policy will document the procedure for monitoring and ensuring appropriate access to the information within the VCN Data Repository, by users.

User Access Audits:

The VCN Repository Manager, or a delegate, will periodically run a report, or create a data extract, that will list the usernames, security role(s) and active status of all users that have access to the Data Repository. This information will be able to be separated out by member agency and distributed to the respective agency DR security administrator. This will allow the administrator to reconcile this list and maintain its accuracy. This information will be updated and made available on a monthly basis.

Data Access Audits:

The VCN Repository Manager, or a delegate, will periodically produce reports, or data extracts, showing which dashboards are being viewed, how often and by whom. This will be used in conjunction with the user access reports to ensure appropriate data access by the DR users. The agency security administrators will be responsible for analyzing the content of these reports and adjusting their user accounts as necessary. This information will be updated and made available on a monthly basis.

Inappropriate Access:

Patterns that suggest inappropriate access to the DR data may be investigated by the agency security administrator for an effected agency. Unauthorized, or inappropriate, access across agencies must be reported to the VCN Repository Manager. Unauthorized access that is found to be egregious, or reaches the level of a breach will be considered under policy 2015205 VCN Data Breach Policy.

Signature: _____
Name: Simone Rueschemeyer
Title: Executive Director Vermont Care Network
Date: _____

Vermont Care Network
DATA REPOSITORY POLICY

SUBJECT: **Subpoena or Law Enforcement Request for Data**

VCN Policy Number: **2018350**
Effective Date: **5/1/2018**
Revised Date: **5/1/2018**

Purpose: The purpose of this policy is to describe what actions should be taken in response to a subpoena or law enforcement request for data.

This policy sets forth the different actions that should be taken depending on which type of data stored in the VCN data Repository is requested: (1) client data collected and maintained by each member agency, or (2) de-identified data collected and aggregated for system-wide analysis.

Member Agency Client Data:

The confidentiality of member agency client data is subject to the protections for substance use disorder patient records set forth in 42 CFR Part 2, as well as Vermont law and the HIPAA privacy and security regulations. No client data contained in the VCN data Repository will be released in response to a subpoena or request from law enforcement officials. If a subpoena is received and accompanied by a Vermont court order issued in compliance with 42 CFR Part 2, Subpart E, then specific client data may be released. Nonetheless, upon receipt of a subpoena or request from law enforcement for access to member client data in the VCN data Repository, VCN shall notify such member agency so that the member agency may determine how it wishes to respond, including whether to seek a protective order or other appropriate remedy to protect its identifiable client data from disclosure.

De-identified Aggregated Data and Reports:

Data which has been collected, de-identified and aggregated in the VCN data Repository for analytic purposes is non-public data which is proprietary to VCN and its member agencies. Reports made from this data may be public or non-public depending upon their purpose. No non-public, de-identified aggregated data or any private reports created from such data shall be released in response to a subpoena or request from law enforcement officials unless such subpoena or request is accompanied by a Vermont court order to release such information. Upon receipt of a subpoena or request from law enforcement for access to non-public, de-identified aggregated data in the VCN data Repository, or any private or public reports on same, the VNC Data Governance Committee shall determine if such data or reports should be disclosed. If the Committee concludes that there should be no disclosure (and no court order requiring disclosure has been issued), VCN shall contact the sender to object to the subpoena or request. If the sender will not withdraw the subpoena or request, VCN shall file a Motion for Protective Order or shall pursue such other appropriate remedy as needed.

Signature: _____
Name: Simone Rueschemeyer
Title: Executive Director, Vermont Care Network
Date: _____