# Data Use Agreement
**Between**
**Vermont Department of Health**
**And**
**Centers for Disease Control and Prevention ("CDC"), National Healthcare Safety Network ("NHSN")**

The Vermont Department of Health and CDC/NHSN enter into this Data Use Agreement (the "Agreement") effective 1 / 22 / 2018 ("Effective Date"). CDC/NHSN and the Vermont Department of Health shall be referred to individually as a "Party," or collectively as the "Parties."

This Agreement establishes a formal data access and data use relationship between CDC/NHSN and the Vermont Department of Health. This Agreement covers individual- and institution-identifiable data, received by the CDC/NHSN subject to the Federal Privacy Act, 5 USC §§552 and 552a, from the NHSN Patient Safety Component, Healthcare Personnel Safety Component, and Dialysis Component as listed in the attached document that have been voluntarily submitted to NHSN by healthcare institutions in Vermont and for which there is no State or applicable local mandate for reporting of such individual- or institution-identifiable data ("COVERED DATA"). However, COVERED DATA shall NOT include data pertaining to federal or tribal healthcare institutions.

The Parties shall abide by all applicable Federal and State laws, rules, and regulations including, without limitation, all patient confidentiality and medical record requirements and any applicable Institutional Review Board ("IRB") requirements.

## STATE'S OR MUNICIPALITY'S USES OF COVERED DATA

Vermont Department of Health agrees to use the COVERED DATA for surveillance and/or prevention purposes only (e.g., evaluating the impact of a targeted program to reduce central line-associated bloodstream infections). Vermont Department of Health specifically agrees not to use the COVERED DATA obtained under this data use agreement for purpose of public reporting of institution-specific data or any regulatory or punitive actions against healthcare institutions, such as a fine or licensure action. The Parties acknowledge that COVERED DATA is limited to those data specified in the attached document, which identifies the complete set of data items, e.g., facility survey data, central line associated bloodstream infection numerator data, that Vermont Department of Health will have access to as a result of this Agreement.

Vermont Department of Health agrees to designate an NHSN Group Administrator and CDC/NHSN agrees to grant the State's designated NHSN Group Administrator access to the State's COVERED DATA. In the event that the NHSN Group Administrator leaves that role prior to assigning a replacement via the NHSN application, CDC/NHSN requires notification in writing on official letterhead from the signatory or the signatory's successor to assure continuity.

- The designated NHSN Group Administrator for Vermont Department of Health is Meredith Graves, PhD; Epidemiologist IV; Meredith.Graves@vermont.gov; Burlington, VT.

Vermont Department of Health agrees that access to individual- and institution-identifiable data provided under the terms of the Agreement will be limited solely to department staff or contractors who are explicitly authorized to use those data for surveillance and/or prevention purposes only.

**DATA PROTECTIONS**

CDC's legal authorities to obtain COVERED DATA from healthcare institutions are 42 U.S.C. section 241(a) (Public Health Service Act section 301(a)), pertaining to CDC's broad public health authority to conduct research and investigations, and 42 U.S.C. section 242k (Public Health Service Act section 306), pertaining to the collection of statistical data. CDC's authority to keep the COVERED DATA confidential (i.e., protected from an unauthorized release) is 42 U.S.C. section 242m (Public Health Service Act section 308(d)) and the Federal Privacy Act, 5 USC §§552 and 552a.

Vermont Department of Health acknowledges that Federal statutes, including 18 U.S.C. section 1001 (providing penalties for making false statements to the Government of the United States), may be implicated if the State does not protect the COVERED DATA from release pursuant to this Agreement.

Vermont Department of Health acknowledges that it will be the custodian of COVERED DATA stored in its data files and, as such, will be responsible for establishing and maintaining appropriate administrative, technical, and physical safeguards to prevent unauthorized access to or use of these files, for example, security awareness training and signed rules of behavior for all persons who have access to COVERED DATA, strong passwords and auditing for all access to COVERED DATA, approved encryption of COVERED DATA stored digitally.

The State or municipality will use the following safeguards to protect COVERED DATA stored in its data files:

**Data Access and Confidentiality**
Access to data files is restricted to specific project staff, and access by non-project staff is not permitted. VDH uses the concept of least privilege, which involves granting the smallest amount of privileges or permissions to each user required to complete his or her job.

**State IT Employees**
NOTE: State IT employees providing desktop support do NOT have access to confidential data and have not signed confidentiality statements. When desktop support specialists conduct remote desktop support, VDH employees MUST first close any applications displaying PHI.

All state IT employees with access to confidential data are required to sign a confidentiality statement.

Violation of HIPAA or State laws protecting patient confidentiality will subject an individual to civil and criminal penalties as well as discipline as stated under contractual agreement between the State of Vermont and the Vermont State Employees' Association (if applicable).

The AHS Director of Data Services monitors the individuals who fill at least one of the following roles: AHS Domain Administrator, AHS Server Administrator on a server on which VDH data are hosted, or AHS Database Administrator on a server on which VDH data are hosted. These three roles fall under a parent role of "IT Custodian" in terms of VDH Data Governance. Though they may not have reason to, these individuals do have the ability to access confidential data. Therefore, they are required to sign a confidentiality statement.

**Workstations**

Access to restricted areas and information is limited to authorized personnel. Access controls include: a security guard on duty to control building access, key-card passes for access to the office suite, and key-card passes at night and on weekends to prevent unauthorized intrusion into the facility at all entrances. VDH personnel wear a photo ID at all times. Employees are responsible for compliance with HIPAA Security and Privacy policies in their workstations. Authorized personnel have only the appropriate level of access necessary for the completion of their job responsibilities. Visitors are escorted at all times in secured areas.

**Physical Files**

All physical files containing identifying information are stored in a locked file cabinet or within a locked room and are secured when not in use. Access to file cabinets or locked rooms is restricted to authorized personnel. After business hours, offices with such files are securely locked and remain accessible only to authorized personnel. Duplicate hard copies of information are kept to a minimum and are shredded before disposal. All confidential materials that do not require storage are shredded or otherwise destroyed when no longer needed.

**Fax**

The fax machine used for receiving confidential information is located in a secure, limited-access area. When sending/receiving a fax to/from reporting facilities in which confidential data are involved, VDH personnel use an official cover sheet, confirm the fax number before sending the fax, and obtain acknowledgment that the fax was received.

**Mail**

For mailings containing a small amount of PHI, VDH employees seal materials in an opaque envelope or container, and mails the sensitive PHI materials using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (e.g., UPS). This is consistent with DHS Privacy Office's Handbook for Safeguarding Sensitive PII, https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII_0.pdf.

The US Post Office and courier services do not need to have a business associate agreement to transfer mail. It is legally understood in HIPAA terms that the usual "sealed envelope" is enough to protect the PHI and deny potential access to it by the service provider. (Source: U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates/, accessed 11/15/2017.)

Electronic Security

The Agency of Digital Services (ADS) has security protocols in place that protect VDH's databases regarding the privacy of individually identifiable health information contained in the database, including user authentication, access controls, data backup protocol and disaster recovery, timed log out and access tracking. VDH follows ADS computer security policies (http://dii.vermont.gov/policy/policy), including change control, digital media and hardware disposal, incident response, information security, intrusion detection and prevention, malicious software protection, physical security for computer protection, and backup.

The state employs a multi-layered security program including, but not limited to, infrastructure (firewalling, VLANs, intrusion detection), host-based controls (anti-malware and/or host-based intrusion detection), application level security controls (passwords, encryption, parameterized queries to backend data sources), and procedural enforcement/education (periodic vulnerability scans, employee training).

**Data Receipt**

VDH uses secure Internet-based mechanisms to receive electronic data from reporting sources. Receipt and processing logs are maintained to document data receipt, file processing, and report production.

**Data Storage**
VDH has the following security protocols in place to protect databases regarding the privacy of individually identifiable health information contained in the database: user authentication, access controls, data backup protocol and disaster recovery, timed log out and access tracking. Access to electronic VDH data is controlled by means of role-based authentication/access, a locked server room, and an internal firewall. External firewalls are in place to prevent remote access by unauthorized users.

**User ID's and Passwords**
Each VDH computer user is identified with a unique username, which is assigned by AHS IT Administration. User ID's are promptly disabled when an individual leaves State service or the access is no longer needed. All usernames have a password associated with them; a password is required to complete the authentication process.

For ADS standards about passwords, refer to State of Vermont Information Security Policies: Policies and Best Practices, August 4, 2017, Section 2.1 Authentication, pp. 6-8, http://dii.vermont.gov/sites/dii/files/PDF/Policies_Reports/InformationSecurityPolicies_FINAL.pdf.

**Personal Computers**
Workstation computers are in a secure location that is only accessible to authorized personnel. Computers are kept in a locked facility during non-business hours. All computers lock after a period of inactivity. VDH staff members consistently lock their computers if away from their work stations.

**Servers**
All data are stored on Local Area Network (LAN) and Structured Query Language (SQL) servers, where they are protected and backed up. VDH follows the ADS computer security policies to perform the backups, and secure media in a controlled location that is kept locked and only accessible to authorized personnel. Virus checking is routine, as are updates to the data files and engines to provide maximum protection of data files.

Computer servers are in areas where access is limited to authorized persons only. Unauthorized people are not allowed in these areas without an escort. Areas in which unattended servers are located are secured with locked doors. For ADS standards about servers, refer to State of Vermont Information Security Policies: Policies and Best Practices, August 4, 2017, Section 4.4, Server Management, pp. 12-13, http://dii.vermont.gov/sites/dii/files/PDF/Policies_Reports/InformationSecurityPolicies_FINAL.pdf.

**Virus Protection**
Servers and workstations are equipped with virus protection software. Virus detection software is configured to monitor at all times. Virus definitions are updated on a daily basis.

**E-mail Encryption**
VDH prohibits sending confidential information by e-mail, unless encryption is used.
VDH employees must follow these instructions for sending/receiving encrypted mail: http://dii.vermont.gov/sites/dii/files/PDF/Support/MSO365-EncryptionHowTo.pdf
VDH employees must follow these instructions to send to recipients of encrypted mail: http://dii.vermont.gov/sites/dii/files/PDF/Support/MSO365-EncryptionHowTo-Recipients.pdf

Vermont Department of Health specifically agrees that, to the extent permitted by local, State and federal law, it will not release COVERED DATA requested under a State's or municipality's open records laws;

to media; for litigation purposes; that is proprietary and if disclosed could cause competitive harm; or to anyone other than department staff or contractors who are explicitly authorized to use those data for surveillance and/or prevention purposes only.

The following State or municipal statutes, regulations, or policies provide additional safeguards that protect against the release of COVERED DATA:

> Vermont law at 18 V.S.A. § 1917 provides that any data or reports received by the Department regarding adverse events occurring in hospitals are confidential and privileged. 18 V.S.A. § 1919 requires data contained in hospital community reports be aggregated to protect the privacy of patients and not identify the individual hospitals.
>
> In addition, Vermont's Public Records Act exempts from disclosure "records which by law are designated confidential or by a similar term." 1 V.S.A. § 317 (c)(1).

Vermont Department of Health agrees to inform CDC/NHSN in advance of any forthcoming changes to State or municipal law(s) that will reduce legal safeguards that protect against release of COVERED DATA. Vermont Department of Health acknowledges that CDC/NHSN may terminate the Agreement as a result of this information.

**PROVISION AND MANAGEMENT OF THE DATA**

Vermont Department of Health acknowledges that its access to COVERED DATA will be for adverse healthcare events and/or processes of care that occur subsequent to signing this agreement, specifically occurring on or after the first day of the fourth month following the signing date. COVERED DATA reported to NHSN for prior events or processes will not be accessible.

Vermont Department of Health agrees to notify CDC in the event that the Vermont Department of Health is obligated or chooses to release COVERED DATA for a purpose other than surveillance and prevention.

**TERM AND TERMINATION OF AGREEMENT**

This Agreement shall be effective for a period of 5 years beginning on the Agreement Effective Date, The Agreement may be terminated before the 5-year period upon submission by either Party of written notice by Signatory or Signatory successor, in which case the Agreement shall cease 5 days after the date that CDC/NHSN submits the notice to the [Department of Health] OR 5 days after CDC/NHSN receives a notice submitted by the Vermont Department of Health.

In addition, upon CDC/NHSN's knowledge of a pattern or practice that constitutes a material breach of this Agreement by Vermont Department of Health, CDC/NHSN may immediately and unilaterally terminate this Agreement.

CDC requires that in the absence of a conflict with State or local law the Vermont Department of Health must delete or otherwise destroy COVERED DATA stored in its files within one year of the conclusion of this Agreement or a successor Agreement. CDC will retain all COVERED DATA in its files.

NOW, THEREFORE, by signing below, the Parties agree that they have read, understand, and agree to the conditions set forth above:

Vermont Department of Health

Signature _____

**Mark Levine, M.D.**
**Commissioner, Vermont Department of Health**

Date 1/12/18

CDC/NHSN

Signature _____

**Daniel A. Pollock, M.D.**
**Branch Chief, Surveillance Branch**
**CDC Division of Healthcare Quality Promotion**

Date Jan 22, 2018