



COMMONWEALTH of VIRGINIA
Department of Health

Marissa J. Levine, MD, MPH
State Health Commissioner

Gary R. Brown
Director

P. Scott Winston
Assistant Director

Office of Emergency Medical Services
1041 Technology Park Drive
Glen Allen, VA 23059-4500

1-800-523-6019 (VA only)
804-888-9100 (Main Office)
804-888-9120 (Training Office)
FAX: 804-371-3108

Date:

DATA USE AGREEMENT

BETWEEN

OFFICE OF EMERGENCY MEDICAL SERVICES (OEMS)
VIRGINIA DEPARTMENT OF HEALTH

AND

Hospital Name:

Person Signing DUA:

This data use agreement is made between the Virginia Department of Health's Office of Emergency Medical Services (VDH/OEMS) and the named person and entity noted above for the purpose of sharing data from the Emergency Medical Services Patient Care Information System which includes the Emergency Medical Services Registry (commonly known as VPHIB) and its receiving hospital interface known as the Virginia Hospital Hub.

I. Purpose: Under this Data Use Agreement (DUA), the OEMS agrees to provide the receiving hospital with Hospital Administrator (HA) access to the VPHIB Hospital Hub which grants access to the EMS electronic medical records (EMR) for EMS patients transported to the receiving hospital's emergency department. Understanding that various types of data are available via Hospital Hub including:

- ✓ Protected Health Information (PHI)
- ✓ Potentially Protected Health Information (PPHI)
- ✓ Sensitive Information (SI)
- ✓ Non-protected Information

II. Scope of this Agreement: This agreement is limited to providing the receiving hospital with the ability to self-administer VPHIB Hospital Hub User (HU) accounts. HU accounts created by the HA must still meet the requirements within this DUA, the User

Account Request form, and the Hospital Security Agreement. Additional requirements may be added by the receiving facility, but the state product will not be altered to achieve hospital specific requirements.

III. Standard Terms of Agreement:

A. Hospital Staff Hospital Hub User (HU) Account Management

1. The HA does not need to be the signatory of this DUA.
2. The HA shall be a person(s) given the authority to access PHI for both the receiving hospital and the Virginia Hospital Hub.
3. The HA may be the hospital's IT service, clinical, non-clinical staffs, etc.
4. The HA role is designed to allow hospitals with large emergency department staffs to have a few select staff members internally manage the HU accounts of the larger staff.
 - i. HA accounts should not be requested when the role is not being used to manage a larger number of accounts.
 - ii. HA accounts shall not be given to all staffs at the receiving hospital.
 - iii. HA accounts are provided at the sole discretion of OEMS staff.
 - iv. HU accounts are available and VDH/OEMS staffs are available to administer those accounts.
 - v. If a hospital is provided with an HA account HU account requests will be referred to the hospital's HA(s).
5. The HA shall be knowledgeable of the need to understand PHI and have received some type of initial and ongoing PHI education whether internally or by extramural sources i.e. HIPAA training.
6. The HA agrees and will assure that all users at the receiving hospital follow the requirements of the User Account Request form and the Hospital Security Agreement.
7. The number of HAs at the receiving hospital shall be limited to the least number of persons to assure the maintenance of accounts for individual staffs needing to retrieve EMS EMRs 24/7/365 at the time of patient transfer. The OEMS recommends at least two.
8. Accessing EMS EMRs shall be done by individual/unique user accounts. Sharing a user account, leaving endless logons so multiple people may access EMS EMR's, or the use of "generic" accounts is a violation of HIPAA and the Commonwealth's Health Records Privacy Act § 32.1-127.03. This is to be narrowly construed.
9. Each user account created shall identify the individual staff person assigned to that account.
10. All user accounts should be inactivated when staff separates from employment or their job duties change and access is no longer needed.
11. User accounts should only be created in order for staff to perform authorized functions that facilitate patient safety and the continuum of patient care when transferred from an EMS agency to the receiving hospital. Utilization of this information for purposes other than direct patient care, assembling the patient's medical record, or meeting state mandated reporting activities is prohibited.

B. Data Usage

1. Safeguards against misuse of information. The data provided will be used solely for the purpose stated in this DUA. Additional usage must be obtained in writing from the VDH/OEMS.
2. The requestor will not utilize the data provided in a manner that misrepresents the data.
3. The data will not be utilized for any other purpose than to facilitate the continuum of care and patient safety around the time of patient transfer from EMS. Unauthorized usage includes, but is not limited to, performance improvement, marketing analysis, marketing, strategic planning, and any other activity not specifically mentioned in the DUA.
4. The receiving hospital shall have the goal of moving the EMS EMR into the hospital's EMR or paper record during the initial treatment period of that patient.

C. Protected Health Information

1. In all uses of the data, all parties will protect the confidentiality of protected health information (PHI) for any patient, a patient's employer, the patient's family, or a member of the patient's household as required by HIPAA and the Commonwealth's Health Records Privacy Act. PHI includes, but is not limited to the following data elements:
 - a. Name;
 - b. Street address;
 - c. Telephone and facsimile numbers;
 - d. E-mail addresses;
 - e. Social security numbers;
 - f. Certificate/license numbers;
 - g. Vehicle identifiers and serial numbers;
 - h. URLs (Uniform Resource Locators) and IP (Internet Protocols) addresses;
 - i. Full face photos and other comparable images;
 - j. Medical record numbers, health plan beneficiary numbers, and other account numbers;
 - k. Biometric identifiers to include finger prints and voice prints; and
 - l. Any content of an individual record that can by the very nature of its uniqueness be used to identify or potentially identify an individual.

D. Security

1. Once the data is in the possession of the receiving hospital it shall be the receiving hospital's responsibility to protect the PHI from unauthorized access and shall be responsible to manage any breach of information in accordance with any applicable local, state, or federal regulations and/or laws. Any breach shall be reported to the VDH/OEMS within 24 hours of discovery.
2. The VDH/OEMS may terminate this agreement in whole or by individual user accounts at any time and at its sole discretion for perceived or actual breach of this agreement.
3. The VPHIB/VSTR/Hospital Hub modules are managed using standards contained within the Commonwealth of Virginia, Information Technology Resource Management Standard Section 501-09 (ITRM Standard SEC501-09) or its current version. This standard and the following laws and regulations guide our

processes. The most current ITRM Standard can be found on-line at www.vita.virginia.gov and VDH SEC IT Security Policy VDH SEC Firewall and VPN Policy VDH SEC Security and Architectural Review Policy, and 45 CFR Department of Health and Human Services - Parts 160, 162, and 164 Health Insurance Reform: Security Standards: Final Rule

IV. Duration of agreement: This agreement becomes effective upon the date signed by the VDH/OEMS data owner/data steward and expires three years after this date. This DUA may be revoked at any time, for any reason by the VDH/OEMS. The VDH/OEMS will make every effort to provide advance notice of its intent to revoke or not renew this agreement. However, for matters relating to security advanced notice is not always considered appropriate.

V. Agreeing Parties:

Data Requestor:

Understanding that as a matter of state and federal law, an EMS EMR is a patient identifiable medical record that requires the same protection as the receiving hospitals medical records or those of another hospital transferring a patient. For this reason the person signing this agreement shall be authorized to enter into a contract of this type. **We recommend the signature be an executive officer, information officer, medical records leadership, data owner, compliance officer, or at minimum executive leadership of the emergency department.**

By: _____

Date: _____

Name: _____

Title: _____

VDH/OEMS Representative/Data Owner

By: _____

Date: _____

Gary Brown
Director, Office of Emergency Medical Services