HEALTH COMMERCE SYSTEM POLICY

User Security and Use Policy

Persons who execute a user account request are bound to the terms of this policy.

I. Introduction

The Health Commerce System (HCS) has been developed by New York State Department of Health (NYSDOH) as a secure system for collecting and distributing data among state entities, health facilities/providers and partners. The purpose of this document is to:

- Describe the policy that the user of the HCS must agree to and the conditions that must be met in order to obtain and retain an HCS account.
- Enroll using the HCS User Account process to permit an HCS account to be established for a new user of the HCS.
- Describe the policy for and methods of providing an existing user of the HCS with an association to this organization.

II. Joint Organizational - User Attestation Requirements

There are two joint organizational-user attestation requirements for HCS account creation: account establishment and organizational affiliation.

a. Establishing and Retaining Account Access

You are eligible to apply for, receive and use an HCS user account if:

- You are employed by or otherwise under the authority of an HCS organization.
- You and your organization can justify the need for your access to the HCS.
- An HCS Coordinator designated by your organization agrees to sponsor you as a user.
- You agree to all the terms and conditions of this User Security and Use Policy.
- An HCS Coordinator prepares enrolls the user using the HCS Paperless User Account process.

This process will bind you and the co-signing/enrolling organization to the policies outlined in this document and will establish your account. Your HCS Coordinator enrolls/affiliates you at an HCS organization. Should your need for access or your employment status with the co-signing/enrolling organization changes, and there is no other enrollment for you from another organization on file with the Commerce Accounts Management Unit (CAMU), your account will be deactivated. In this case, your account will be deactivated until you enroll using the HCS User Account process.

b. Establishing Organizational Affiliations

HCS users may be employed by, or be affiliated with, multiple HCS organizations. If you are engaged in activities in which you access the HCS on behalf of multiple HCS organizations, then you and the respective organization(s) must establish an affiliation with those organizations on the HCS as well. This can be achieved through the HCS Coordinator approval process.

- You can enroll using the HCS User Account process for each HCS organization through the standard HCS Coordinator approval process. This is the preferred practice as it preserves your account in the event that you leave employment of one organization. Roles do not preserve an account. You are required to notify CAMU of any change in employment status.

III. Binding Effect

This document supersedes all previous versions. The user indicates that they understand and agree to the responsibilities and duties described in this document. The user understands and agrees that they are bound by this agreement regardless of organization or location from which the HCS is accessed. The user also understands that

future modifications to this agreement may be made and that the user's agreement with these changes may be affected on the HCS. The user understands and agrees that they will be bound by the agreement.

By enrolling/affiliating a user, the HCS Coordinator indicates they understand and agree on behalf of the HCS organization that:

- The user has a valid affiliation with the organization and the Coordinator has exercised due diligence in verifying this fact (e.g., checked with the HCS Director of the organization or user's Department Head).
- The user has valid need to access the HCS for this organization.
- The organization will enforce the terms and conditions of this agreement as it applies to this user.
- The organization will be responsible for actions of this user regarding their compliance with the HCS policies, at all times and places and under all conditions.

IV. Security

Authorized HCS users can create their own user ID, password and PIN using the HCS User Account process., a Personal Identification Number (PIN), and a password by CAMU. These codes are unique for every user and must be saved securely for future reference. The PIN and password may **not** be shared with others. The consequences of sharing an HCS access account are severe and can include revocation of the account. Multiple instances of violations that compromise the security of account usage may result in the inability of your organization to do business on the HCS.

Because HCS uses passwords and PIN codes to manage and control access to data, including confidential information, CAMU must be notified immediately at camu@health.ny.gov or 1-866-529-1890 if a user suspects that any of these confidential access codes may have been compromised.

The HCS has routines in place to prevent unauthorized access of HCS data. Users will not attempt to circumvent these routines.

For both security and performance reasons, all HCS user accesses is logged and/or monitored. Users, therefore, understand that these logs and monitoring sessions can trace their activities on the HCS and agree that their activities on the HCS may be logged and monitored.

Users must notify the HCS Coordinator (HCSC) immediately about any change in their employment or duties that will affect authorized HCS access. To notify CAMU if the HCSC cannot be contacted, call 1-866-529-1890 or write camu@health.ny.gov

V. Access and Usage of Data

The HCS is a series of data collection and distribution systems developed by various programs. Appropriate use of HCS resources, and effective security of those resources, require the participation and support of the individuals using or accessing such resources. NYS agencies and program areas that are responsible for collection and maintenance of particular data shall authorize access to that data via the HCS. The same program area is also responsible for responding to questions about the data to which they authorize access.

a. Acceptable Use

Acceptable use is use that is authorized by the HCS organization, unless otherwise indicated by NYS, and is consistent with public health functions and all applicable policies, laws, and regulations such as NYS Policy on Acceptable Use of Information Technology Resources (NYS-P14-001).

b. Unacceptable Use

Examples of unacceptable use are:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information.
- Unauthorized use or disclosure of State information and resources.
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
- Transmitting unencrypted private information, as defined by the Internet Security and Privacy Act.
- Using HCS resources to circulate unauthorized solicitations or advertisements for non-State purposes including religious, political, or not-for-profit entities.
- Providing unauthorized third-parties, access to the HCS information or resources.

- Tampering, disengaging, or otherwise circumventing NYS or third-party IT security controls.
- Using HCS resources for personal purposes, and conflicts with the proper exercise of duties of the user.

The guidelines established with the policy are intended to be illustrative of the range of acceptable and unacceptable uses of the HCS and its facilities and are not exhaustive. Questions about specific uses not set forth in this policy should be directed by e-mail to camu@health.ny.gov. Instances of specific unacceptable uses must be reported by email to camu@health.ny.gov immediately.

VI. Reason for Access

Users requesting access to the HCS must have a valid and acceptable reason for access. This typically involves a user satisfying a state mandated reporting activity on behalf of the organization, performing health activities such as assurance/surveillance/planning/preparedness/response, or serving a critical role at the organization that is associated with these activities and requires access to data/information as part of that role.

State entities and program areas are responsible for controlling access to their applications and data. They will review requests and act on them via their own protocols for access approval. It is therefore understood that granting of access requests to applications and data on the HCS is subject to state entities and program area approval and protocols.

VII. Data Disclosure

Data/information originating from the HCS is protected under state and federal confidentiality laws as well as policy/procedures. Employees or agents of HCS organizations who have acquired knowledge of personal or health data/information from the HCS **shall not disclose this information to any other person unless** that person is authorized by the state entity or a program area and has official reason to see that information.

VIII. Enforcement

Violations of this policy can result in termination of HCS services for the person(s) at fault. Unauthorized use, fraudulent use, unacceptable use, abuse of computing on network facilities, or unauthorized disclosure of information will lead to suspension of the user's account and/or referral for appropriate legal action. Legal consequences may include suspension or revocation of a professional license, fines and/or imprisonment.

IX. HCS User Responsibilities and Duties

Because the Health Commerce System (HCS) is a secure system for collecting and distributing data between state entities, health facilities/providers and partners, it is very important for each user to accept the responsibilities of this document and perform the duties expected of them when using the HCS.

Individuals initiating/creating/requesting an account on the HCS must read, understand, and attest to the SAUP as part of the enrollment HCS User Account process.

Duties of each user with an established HCS account include:

- Adhering to the terms and conditions of this agreement in its entirety (including its schedules) regardless of the location from which the user accesses the HCS.
- Assuring the PIN number and password of the HCS account are kept confidential in a secure place and are not shared with anyone other than a CAMU representative (PIN number used by CAMU for authentication and authorized account access.,
- Updating the contact information recorded in the Communications Directory when necessary, so that it is accurate at all times.
- Maintaining the confidentiality of all data and information accessed on the HCS.
- Accessing only that information on the HCS for which the user has been duly authorized.
- Reporting any indications of fraudulent use, including being asked to use another's account to gain access to information not specifically authorized to yourself or by witnessing such an action from another user.
- Contacting the HCS Coordinator(s) at the HCS organization(s) for which they are to access the HCS at least 3 business days prior to any change in the user's HCS responsibilities or in the user's employment status affecting the standing of the account or notifying CAMU at 1-866-529-1890 if contacting the HCS Coordinator is not possible.