HEALTH COMMERCE SYSTEM POLICY

Director, Coordinator and Security Coordinator Organization Security and Use Policy

Persons who execute a Director, Coordinator or Security Coordinator account request form are bound to the terms of this policy.

I. Introduction

The Health Commerce System (HCS) is a secure system managed by New York State Department of Health (NYSDOH) for electronically collecting and distributing data among state and local governmental entities, health facilities and providers, and other types of entities to support public health and health oversight activities. The real-time nature of information access and interchange required for effective detection and response to public health events demands both individual and organization-level accounts in the HCS. In order for the organization to utilize HCS effectively, a Director or Security Coordinator must be named and made personally accountable for execution of the security protocols in Organizational Security Coordinator (OSC) role and responsibilities of this document and assume responsibility for organization-level data exchange via an Automated File Transfer (AFT) business-to-business account.

The purpose of this document is to:

- Define the security terms, conditions, and responsibilities that organizations must agree to in order to have their employees or individuals affiliated with their organization access and use the HCS.
- Provide for the assignment of HCS Coordinator(s) (HCSC) and define the duties and responsibilities for individual(s) assigned by the organization to act in this role. The HCSC has the ability to manage and monitor many of the organization's interactions with the HCS and state entities. By definition the Director (head) of the organization will be given this role. However, the organization may assign a number of their trusted employees to this HCSC role.
- Provide for the assignment of HCS Organizational Security Coordinator(s) (OSC) and define the duties and responsibilities for individual(s) assigned by the organization to act in this role. The OSC has the ability to manage and monitor Automated File Transfer (AFT) account and has the ability to fulfill the role of HCSC for the organization.
- Establish HCS accounts for the Director of the organization and all assigned HCSCs and OSCs.

II. Overall Security

Each organization is responsible for the security and confidentiality of HCS data accessed and used by its employees/agents. This includes validation of users who need to access the HCS, physical security of computers on its network, security of data that is removed from the HCS, and immediate notification to the correct state entity when the status of the authorized user changes due to reassignment of duties or change of employment. Send email to **camu@health.ny.gov** or call **1-866-529-1890** to report status changes to the Commerce Accounts Management Unit (CAMU).

III. Data Disclosure

Employees/agents of the organizations who have obtained information from the HCS shall not disclose this information to any other person unless that person is legally authorized to obtain and has official reason to see that information.

Unauthorized disclosure may be a violation of law and subject the organization, its employees and/or its agents to fines, imprisonment or suspension or revocation of a professional license.

IV. Responsibility

The organization's employees/agents requiring access to the HCS will be given a User Security and Use Policy (Document 2). The organization agrees to the terms of the Organization Security and Use Policy (Document 1) and the User Security and Use Policy (Document 2) and agrees to require its employees, agents, and affiliates to comply with the terms and conditions of both documents. The organization will be responsible for the actions of any of its employees/agents with regard to compliance with HCS policies. It is absolutely forbidden for any employee/agent to share an HCS account or to use an account assigned to another HCS user. Absent an appropriate organizational response to account violations, user account privileges will be removed upon a first offense.

Each organization will designate HCSC(s) who will be personally accountable for execution of the responsibilities defined in section XI of this document and who will have the authority to legally bind the organization in matters relating to the HCS. The organization will be held responsible for actions of an HCSC who is remiss in these responsibilities.

The organization may designate OSC(s) who will be personally accountable for execution of the roles and responsibilities defined in section XII of this document. The organization will be held responsible for actions of an OSC who is remiss in these responsibilities, any unauthorized access or usage of specialized account, and any actions of its employees/agents not in compliance with the HCS policies and protocols.

V. Coordinator (HCSC) Role

The Health Commerce System Coordinator (HCSC) role for management of organization user accounts on the HCS. Organizations are required to designate at least one HCSC as the principal point of contact concerning HCS access. By definition, the HCSC must have the authorization and responsibility within the organization for execution of the roles and responsibilities for an HCSC delineated in section XI of this document. Upon execution of this account request form, the Director of the organization will be given an HCS account and assigned an HCSC role. An additional HCSC may be enrolled using a Paperless HCS Coordinator Account Request process with the Coordinator Account Request Form, who will also be given an HCS account. Every HCSC must have an active HCS account. The organization agrees that HCSCs within their organization shall also be bound by the terms and conditions of the User Security and Use Policy (Document 2). The organization agrees to ensure that designated HCSCs routinely access the HCS and carry out their duties and responsibilities in a timely manner. Should the HCSC not fulfill the responsibilities as described herein, e.g., is unresponsive to inquiries or alerts from CAMU or the state entity, CAMU or the state entity may direct the organization to appoint a replacement and the organization shall comply.

VI. Organizational Security Coordinator (OSC) Role

The Health Commerce System Organizational Security Coordinator (OSC) role for management of the specialized account for the organization. Organizations are required to designate at least one OSC before the organization accesses the specialized account. The OSC is the principal point of contact concerning HCS access from any specialized account. The OSC must have the authority and responsibility within the organization for execution of the roles and responsibilities for an OSC delineated in section XII of this document. Upon execution of this account request form, the Director will be given an HCS account and assigned to the roles of HCSC and OSC. Every OSC must have an active HCS account. The organization agrees that OSCs within their organization shall be bound by the terms and conditions of the User Security and Use Policy (Document 2). The organization agrees to ensure that designated OSCs routinely access the HCS and carry out their duties and responsibilities in a timely manner. Should an OSC not fulfill the responsibilities as described herein, e.g., is unresponsive to inquiries or alerts from CAMU or the state entity, CAMU or the state entity may direct the organization to appoint, and the organization shall appoint a replacement or have the specialized account deactivated.

VII. Notification

The organization agrees to notify CAMU at camu@health.ny.gov or 1-866-529-1890, at least three business days prior to any change in employment or affiliation affecting HCS access status or work/trust status of any of the following:

- The users.
- The HCSC. The organization is responsible for designating and establishing a replacement HCSC. The organization is encouraged to designate additional HCSCs as backup.
- The OSC. The organization is responsible for designating and establishing a replacement OSC. Once the specialized account is established for the organization, there must be at least one OSC for the organization at all times. The organization is encouraged to designate additional OSCs as backup.
- The HCS Director. An existing HCSC is responsible for having the new HCS Director establish an account.

The organization agrees to notify CAMU immediately upon discovery of suspected or confirmed breaches of protocol, access or security that affect this security agreement. It is particularly important to notify CAMU regarding sharing of an HCS account or use by an employee/agent of an account assigned to another HCS user. Notification will be via electronic systems on the HCS, or if unavailable, via phone at 1-866-529-1890 within 24 hours of the incident. In the absence of an appropriate organizational response to account sharing, user account privileges will be deleted.

VIII. Investigations

The organization will notify CAMU of any actual or suspected violations of this policy and will cooperate with NYSDOH and other state authorities in any subsequent investigations or prosecution. Detailed logging and monitoring of all communications for user activity on the HCS occurs continually. Extended logging and/or monitoring may be required by state authorities during the course of an investigation.

IX. Revocation of Access

Access to the HCS is a privilege. NYSDOH may direct a participating party to be replaced and/or reserves the right to revoke the use of an account or the organization's participation if violations of HCS security policies occur.

X. Modification of Agreement

This agreement may be modified in the following ways:

- Additional HCSCs may be added by completing additional Coordinator Account Requests.
- As enhancements and new capabilities are added to empower the organization with additional HCS user account management capabilities, it will provide revisions to section XI to the HCSC on the HCS. Substantive changes and enhancements will be accompanied by the corresponding security policy. By virtue of their designation as HCSC, the HCSC shall be authorized by the organization to accept such changes on its behalf. Acceptance of the revision by the organization's HCSCs will be signified by the HCSC's agreement to the changes on the HCS. The organization agrees that it will be bound by the acceptance of these changes.
- Additional OSCs may be added by completing additional Organizational Security Coordinator Account Requests.
- Additional organizational account management roles may be defined and relayed to the organizations by adding sections to this document for new organizations and by notices to current organizations on the HCS.

XI. Coordinator Duties and Responsibilities

HCS Coordinators (HCSCs) are designated by the Director of the organization as having the responsibility and authority to engage in HCS management activities on behalf of the organization. It is the responsibility of the organization to ensure that these management activities are completed in a timely and effective manner. These management activities are facilitated by a series of 'tools' provided to the HCSC as part of their HCS account. (Training is available to the HCSCs for using the 'tools'.) The organization agrees that it will require it's designated HCSC(s) to use their HCS accounts to execute the organization's HCS management responsibilities and keep their accounts active.

The current HCSC management responsibilities include the following (see Section V):

- Approve new HCS account requests for users employed by the organization by either:
  - Enrolling users using a HCS User Account process (valid photo ID required); or
  - Enrolling a user using the HCS User Account process for a new user establishes an account and formally affiliates the user with the requesting organization. The HCSC account will be given access to tools to request or enroll accounts for the user and filing a notification of the account request. The HCSC account is also given access to review all accounts at the organization and to verify whether the requesting user has an existing account.
- Establish organizational affiliations for HCS users with existing HCS accounts. HCS users may be employed by, or be affiliated with, multiple HCS organizations. If the user is engaged in activities for which the user accesses the HCS on behalf of multiple HCS organizations, then the user and the respective organization(s) are responsible for establishing an affiliation with those organizations on the HCS as well. This can be achieved through the HCS coordinator approval process.
  - The HCSC can enroll the user using the HCS User Account process for each HCS organization through the HCS coordinator approval process. This is the preferred practice as it preserves the user account in the event that the user leaves employment of one organization. Roles do not preserve an account. (Users

and HCSCs are required to notify CAMU of any change in employment status.)

- Manage HCS user accounts. The HCSC account provides access to a variety of tools to review account information for users at their organization. The HCSC is responsible for reviewing the user accounts and notifying CAMU (1-866-529-1890) of any appropriate changes that need to be made in the account (such as account deactivation in the event of change in employment status of an HCS user).
- Manage the organization's entries in the Communications Directory (ComDir). The HCSC is responsible for the following activities on behalf of the organization:
  - Active management of organizational contact information. The HCSC enters and regularly updates their organization's contact information (i.e., phone, fax, etc.) for key roles/locations in their organization into a central database. This provides the organization with control over the authoritative source for this information and eliminates the need to continually respond to external requests for contact information. It is therefore important that this information be regularly reviewed and kept current by using the HCSC 'tools' on the HCS.
  - Active management of user roles at the organization. ComDir allows the organization to give members of its staff access to certain public health response applications and data. The HCSC acts as the organization's proxy in this task by assigning designated staff to role-based information systems on the HCS via ComDir. It is therefore essential that the role assignments be appropriate, accurate, and current. It is also essential that the HCSC work with the organization to ensure that the individuals in these roles have and maintain active HCS accounts.

By reading, understanding, and checking the attestation/affirmation, the Coordinator Account Request Form, the HCSC indicates their understanding and agrees personally and on behalf of the HCS organization that they will maintain and actively use the HCS account to execute duties and responsibilities defined herein, in a timely manner with due diligence.

XII. Organizational Security Coordinator Duties and Responsibilities

HCS Organizational Security Coordinators (OSCs) are designated by the HCS Director of the organization as having the responsibility and authority to engage in management activities for specialized accounts as well as user accounts on behalf of the organization. It is the responsibility of the organization to ensure that these management activities are completed in a timely and effective manner. These management activities are facilitated by a series of 'tools' provided to the OSC as part of their Commerce account. (Training materials are available for using the 'tools'.)

The current OSC management responsibilities include the following (see Section VI):

- Act as a coordinator for the organization and accept the duties and responsibilities of that role as stated in section XI of this document.
- Have a background in information technology and security and currently serve in an information technology security capacity for the organization.
- Is held personally accountable by the organization for execution of the security policies of this document.
- Notify CAMU immediately upon discovery of suspected or confirmed breaches of specialized account and HCS protocol, access or security.
- Maintain an active Commerce account in order to view and maintain specialized and user account information.
- Protect account and key access information, issue account information to designated employees, and submit reports on account usage.
- Retrieve user and/or specialized account information from Commerce (available to the OSC only) and store it in a locked, safe location known to the OSC and HCS Director.
- Ensure that updates to specialized account software systems are applied properly and in a timely manner.
- Monitor the use of specialized account software systems and designate operators for systems if necessary.
- Follow guidelines listed in New York State and Federal cybersecurity policies and standards for all hardware and software used by the specialized account.

By reading, understanding, and checking the attestation/affirmation, the Organizational Security Coordinator indicates their understanding and agrees personally and on behalf of the organization that their will maintain and actively use the Commerce account to execute duties and responsibilities defined herein, in a timely manner with due diligence.