Office of Health Insurance Programs

Division of Long Term Care

MLTC Policy 15.07: Potential Security Exposure with the UAS-NY

Date of Issuance: December 1, 2015

The purpose of this memo is to highlight potential security exposure for Managed Long Term Care Plans (MLTCP) related to the assignment of UAS-NY roles in the Health Commerce System (HCS), and to provide suggestions to minimize potential security exposure.

The UAS-NY web-based application is designed with several security features. One of the main features is that it is a role-based application. As such, each person who accesses the UAS-NY is required to have a UAS-NY role associated with an organization. This role governs what data the staff member may access and what functions the staff person may perform. Additional security features are detailed in the UAS-NY Implementation Guide.

Since the transition to the UAS-NY began for MLTC in October 2013, the New York State Department of Health has become aware of three general business scenarios related to the conducting of assessments. These scenarios are:

- MLTCPs use employees, including per diem staff, to conduct assessments;
- MLTCPs subcontract with a Licensed Home Care Service Agency (LHCSA) or Certified Home Health Agency (CHHA) to conduct assessments; or
- MLTCPs subcontract with other non-licensed or non-certified agencies to conduct assessments.

Within each of the above scenarios there are additional variations. Some examples of these variations are described below.

- The MLTCP assigns UAS-NY roles to its subcontractor (LHCSA, CHHA, or other) staff. These staff then access the UAS-NY under the auspices of the MLTCP and have access to the organization case list created by the MLTCP.
- The MLTCP HCS Coordinator creates HCS user accounts with Trust Level 3 assurance for staff that work for a subcontracting agency. This primarily occurs when an organization is not set up in the HCS or is set up in the HCS but does not have access to the UAS-NY application.

Each time a staff person accesses the UAS-NY, the staff person is required to select a UAS-NY role which is associated with a specific organization. Some staff have one role provisioned by one organization and other staff have multiple roles provisioned by a number of organizations. **If a staff person performs any action within the UAS-NY that could be construed as fraudulent, a security breach, or a violation of HIPAA or HITECH, the organization that assigned the UAS-NY role and the organization under which the Health Commerce System (HCS) user account was created may be held accountable for the security violation**.

Some examples of a potential security violation are presented below.

- **User has multiple UAS-NY roles provisioned by multiple organizations** – The user logs in to the UAS-NY for the purposes of conducting an assessment, chooses the ***incorrect*** organization and proceeds to conduct a statewide search, attests to a business need to access the record on behalf of the ***incorrect*** organization and adds the consumer to that organization's case list, and conducts an assessment for the ***incorrect*** organization.
  - ➔ This may be a HIPAA violation because the organization does not have a legitimate business need to access the consumer record. Depending upon the nature of the access, this may be considered an unintentional acquisition, access, or use of PHI by a member of the MLTCP's workforce or an inadvertent disclosure of PHI from a person authorized to access PHI in the MLTCP to another person authorized to access PHI in the MLTCP or one of the MLTCP's HIPAA-business associates, provided that the PHI is not further disclosed.

- **User has an HCS User account created by a former employer** – The original employer created an HCS User account for an individual. The user left that organization and is now working for a new employer, and continues to use the original HCS user account.
  - ➔ In failing to delete the HCS User account which they created, the original employer is in violation of the HCS Organization Security and Use Agreement.

- **User has a UAS-NY role created by a former employer** – The original employer assigned an appropriate UAS-NY role for a user. The user left that organization and is now working for a new employer and continues to have access to the role assigned by the former employer. The user conducts an assessment for a consumer under the role assigned by the former employer.
  - ➔ This may be a HIPAA violation since the organization does not have a legitimate business need to access the consumer record.
  - ➔ This is a violation of the HCS Organization Security and Use Agreement.

To minimize YOUR security exposure, each MLTCP is strongly encouraged to review its business operations and procedures for conducting assessments. Specifically, each MLTCP should review its internal procedures for:

- creating HCS user accounts and establishing Trust Level 3 assurance for staff and subcontractor staff;
- managing and updating UAS-NY role assignments for staff and subcontractor staff; and
- creating, managing and accessing the organization case list for the MLTCP.

To reduce YOUR security exposure, MLTCPs should have its subcontractors fulfill the aforementioned functions. Specifically, subcontractors should be responsible for:

- creating HCS user accounts and establishing Trust Level 3 assurance for its staff;
- managing and updating UAS-NY role assignments for its staff; and
- creating, managing and accessing the organization case list for the subcontractor. This case list will represent only those case records that the subcontractor is required to access.

As the MLTCP reviews its business operations and procedures, it is important to recognize that each MLTCP is required to adhere to its contractual requirements and applicable laws, regulations, and policies. In addition, each MLTCP must ensure that its subcontractors, vendors, and per diem employees adhere to MLTCP contractual requirements and applicable laws, regulations, and policies.

If you need additional information or have any questions, please email the Bureau of Managed Long Term Care at mltcworkgroup@health.ny.gov.