SASH Privacy Officer
Summary of Duties and Responsibilities

General Description

The SASH system connects housing organizations that implement SASH to the larger health care system. By collecting health information from our participants and sharing it as needed with designated SASH partners, SASH staff are able to assist participants to navigate the complex health care system and attain the services and supports they need to remain safely at home. The information SASH staff collect and use in this way is protected under the Health Insurance Portability and Accountability Act (HIPAA). Under HIPAA, health care organizations are required to designate an HIPAA privacy officer. The privacy officer is responsible for overseeing the organization's development, implementation, and monitoring of privacy policies and ensures they are in accordance with federal and state guidelines. The privacy officer oversees activities and processes associated with creating, introducing and maintaining workplace privacy policies that meet state and federal legal requirements.

The privacy officer responsibilities fall into four main categories: Policies and Documentation, Employee Training, Monitoring and Investigation, and Ongoing Awareness.

Policies and Documentation

The privacy officer leads initiatives to establish and/or adopt the policies, procedures and key documents addressing confidentiality and privacy requirements. For the SASH program these documents include:

- A Privacy and Confidentiality Policy for the organization (includes a HIPAA breach policy)
- A Security Rule Policy
- An Employee Confidentiality/Privacy Acknowledgement form
- Authorization for Use and Disclosure Form (requires signature and renewed on an annual basis).
- Patient Consent for Viewing Electronic Protected Health Information (PHI)
- Waiver and Release Form
- Notice of Privacy Practices (provided annually at time of annual reauthorization of Use and Disclosure form)
- SASH Explanation of Benefits Form

Employee Training

The privacy officer champions activities to promote employee awareness of individual and organizational obligations under HIPAA. The privacy officer ensures that appropriate staff participate in all mandatory privacy training offered by Cathedral Square including:

- The initial HIPAA training (provided via VIT sites) that provides a comprehensive overview of HIPAA requirements and includes in-depth case studies and discussions.

- Silverchair Learning Systems on-line HIPAA training module to be completed on an annual basis. Training covers the Privacy Rule, Security Rule and Electronic Transmission related to HIPAA.

- Periodic site visit trainings as part of regular TA and model compliance visits to SASH sites by statewide administrative staff.

Monitoring and Investigation

The privacy officer oversees the periodic monitoring of data access and storage and investigations into suspected breaches and complaints. The privacy officer works closely with information technology team members to make sure adequate controls are in place to uphold privacy requirements. Controls range from data encryption to auditing of systems for proper access control levels.
The investigation of any suspected breaches is an absolute priority for the privacy officer. The privacy officer is responsible for the initial investigation utilizing the Privacy Breach Assessment form and following the Privacy Breach Policy. The Privacy Officer should notify Cathedral Square as soon as possible once a privacy breach is suspected.

Ongoing Awareness

The privacy officer fosters HIPAA privacy awareness on an ongoing basis within the organization. To promote the culture of awareness, the privacy officer stays abreast of updates to requirements at both state and federal level, and keeps employees informed. The privacy officer ensures the Notice of Privacy Practices is clearly visible with the organization and on any website.