

Part D	SAHP	IHN	SEL	SCP	COHO	ADMIN
X	X	X	X	X	X	X

HP-10 Health Insurance Portability and Accountability Act (HIPAA) Security

Health Insurance Portability and Accountability Act of 1996

Samaritan Health Plan Operations (SHPO), in an effort to comply with HIPAA, maintains that protected health information (PHI) must be kept secure, private and confidential.

Policy:

SHPO engages in security practices that ensure that member PHI is safeguarded. These security practices encompass:

- Security Orientation and Training
- Facility Security
- Use of electronic mail
- Use of Facsimiles
- Access to and use of Facets
- Access to and use of other applications and electronic storage media
- Access to and use of Facets, applications, and databases by 3rd parties
- Monitoring

Many of the policies that govern security were developed by and are enforced by Samaritan Health Services (SHS). These policies are all available in the [“Policies and Procedures” section of the SHS Insider](#).

Definitions (from *The HIPAA Training Handbook*, © 2008 by the Healthcare Compliance Association, Minneapolis, MN)

Privacy: the right of an individual to control his or her own personal information and to keep it from being divulged or used by others against his or her wishes.

Confidentiality: a means of protecting information, usually by safeguarding it from an unauthorized use or disclosure.

Security: the spectrum of physical, technical, and administrative safeguards put in place to protect the integrity, availability, and confidentiality of information and the systems on which it is stored.

Procedures:

Security Orientation and Training

- All SHPO staff must read, complete, and sign the SHS “Computer Access and Security Guidelines.”
- All SHPO staff must complete the annual SHPO HIPAA training.

Facility Security

- All SHPO staff are required to wear an employee badge.
- The employee badge gives employees who have received prior approval from their manager access to the Avery Square building outside of normal business hours (6:00 am to 6:00 pm)
- All SHPO staff are given the combination to the locked SHPO exterior doors. SHPO staff are prohibited from sharing this number with any non-SHPO employees. SHPO are also prohibited from allowing non-SHS individuals from entering the employee-only locked entrances. All visitors should be directed or escorted to the appropriate visitor entrances (suites 101 and 103).

Use of Electronic Mail

- SHPO staff shall use the SHS secure email capability when sending PHI to external (non-SHS) email addresses. Generally speaking, SHPO staff may only disclose PHI for the purposes of treatment, payment, or operations. For additional information, SHPO staff should refer to *HP-20 HIPAA Operations*.
- SHPO staff may use “non-secured” email (i.e., Outlook) to disclose PHI for the purposes of payment or operations to SHS internal email recipients. For additional information, SHPO staff should refer to *HP-20 HIPAA Operations*.

Use of Facsimiles

- SHPO staff shall use the secure fax machines when sending or receiving PHI. For additional information, SHPO staff should refer to *HP-20 HIPAA Operations*.

Access to and use of Facets

- SHPO staff may only access Facets using the network user name and password that was issued to them by SHS Information Services (IS).
- SHPO staff may only access Facets applications for which they have been authorized by their manager.
- SHPO staff may only access lines of business for which they have been authorized by

their manager.

Access to and use of other applications and electronic storage media

- Application access: SHPO staff may only access applications made available by SHS IS for which they have been authorized by their manager.
- Shared Folder Access: SHPO staff may only access shared folders made available by SHS IS for which they have been authorized by their manager.
- Portable Electronic Storage Media:
 - SHPO staff are responsible for safeguarding PHI against loss, destruction, tampering, and unauthorized copying, access, or use.
 - SHPO staff shall not store PHI on mobile devices (including laptops and PDAs).
 - SHPO staff shall take measures to ensure the security of Personal Digital Assistants (PDAs), laptops, thumb drives, other mobile devices, compact discs (CDs), and other electronic storage media. SHPO staff may not leave these devices and storage media unattended outside of the secured office environment.
 - If possible, SHPO staff shall enable the security features on the device (user names, passwords, etc.).
 - SHPO staff shall password protect CDs and other electronic storage media when transporting these items outside of the secure SHPO space.
- Access to Facets and other application via Virtual Private Network (VPN)
 - SHPO staff must have a manager's approval to access PHI via VPN
 - SHPO staff must use a computer that has been configured by SHS IS for that purpose.
 - SHPO staff must take appropriate steps (consistent with in-office policy) to safeguard PHI when accessing Facets and other application or databases via VPN, including, but not limited to:
 - Covering work when stepping away from the computer
 - Using screensavers, privacy screens, etc.
 - Being aware of surroundings and the potential for unauthorized observation

Access to and use of Facets, applications, and databases by third parties

- Managers must approve access by a third party to any applications or databases that contain PHI.
- SHPO must have a signed, current Business Associate Agreement (BAA) in place prior to the granting of access.

Monitoring

The SHPO Compliance Department will monitor adherence to HIPAA Privacy and Security regulations through periodic HIPAA Privacy and Security evaluations and risk assessments and through the HIPAA incident reporting process.