SHS Annual Information Privacy and Security Training

Samaritan Health Services

HIPAA Overview

- Sets the ground rules for how we use and share health information, with whom, and for what purposes
- Provides privacy protections (rights) to patients and members
- Balances need to protect patient/member privacy with our need to have information so we can provide the best possible patient care
- Establishes standards for the security of the health information we hold

Samaritan Health Services

Building healthier communities together

What information is subject to HIPAA?

- HIPAA applies to Protected Health Information (PHI), which is information maintained by SHS that:
  1. Directly identifies a person (e.g. their name, address or MRN) OR that may identify a person with added context (e.g. their date of service plus their unique diagnosis); AND
  2. Includes 'health information' – information that relates to the person's past, present or future health condition, provisioning of care, or payment for care.

When Should You Access, Use or Share Patient/Member PHI?

- With the patient or legal guardian's authorization;
- For Treatment, Payment, or Healthcare Operations:
  - Treatment: Patient care, or care coordination efforts by healthcare providers
  - Payment: To obtain reimbursement for care, or to pay for health care services
  - Healthcare Operations: Specific functions necessary to run the organization (quality assessment/improvement, responding to grievances, business/financial management, etc.)
- For certain public health activities
- When otherwise permitted or required to by law

Social Media

1. **Don't post**. Unless you work in the Marketing/PR Department AND have the patient's authorization, NEVER discuss or share patient information on Social Media platforms such as Facebook, Twitter, SnapChat, Instagram, etc.
2. **Don't try to de-identify**. Do not post information about patients even if you think you've removed all possible identifiers, as information can sometimes be identified from the additional context or other details in the post.
3. **Don't acknowledge or respond**. Even if a patient complains about their care, or about you as a care provider, on their own Social Media platform, DO NOT REPLY. Instead, contact Marketing/PR for guidance.

Access to reports, lists, and schedules

- Access to patient lists, schedules, reports, or other similar resources should only occur when necessary for a legitimate business purpose – i.e. for treatment, payment, or health care operations.
- Example: Do not access patient lists within Epic simply to see who is visiting the hospital and for what reason.

Accessing your own record

- In general, do not access your own medical record via Epic, Facets or other electronic medical record system.
- Instead, sign up for MyChart or request your record via the Health Information Management department.

Samaritan Health Services

Building healthier communities together

Accessing friends, family members and co-worker records

- In general, only access the record of friends, family members or co-workers when:
  1. Necessary for a legitimate business purpose (i.e. a permissible or required purpose under HIPAA, such as Treatment, Payment, or Healthcare Operations), AND
  2. No one else is available to complete that task.
- If a family member, friend or co-worker requests that you enter their record to obtain information on their behalf:
  - Only provide them with the requested information if that is something you would normally do for other patients making the same request. Otherwise, refer them to the appropriate department for assistance (e.g. Health Information Management, their PCP office, etc.).

Accessing friends, family members and co-worker records continued

- As an employee, while you may have the right to access a parent, spouse, or minor child's information, SHS policy still requires you to obtain that information through appropriate channels.
- For example, accessing a minor child's medical record via Epic, Facets, or similar system for personal reasons is not appropriate. Instead, please request MyChart proxy access, contact the patient's primary care physician, or contact the Health Information Management department to request records.

Securing Workstations

- SHS employees must lock their workstations when leaving their computer unattended. This is true regardless of setting: home office, exam room, secured building/office, etc.
- SHS has a responsibility to safeguard patient data. Leaving a workstation unlocked and unattended exposes SHS and our patients/members to unnecessary risk.

What is “Information Security?”

- Information Security is the preventing of unauthorized access, use, or destruction of SHS information
- The mission of the SHS Information Security Program is to **protect valuable SHS resources**
- Information Security is everyone’s responsibility

What Valuable Resources are We Protecting?

- Protected Health Information (PHI)
- Other Sensitive Information, including:
  - Social Security Numbers
  - Credit Card Numbers
  - HR Data
  - SHS Financial Data
- Laptops, Computers, Mobile Devices
- SHS Reputation in the Community
- SHS Legal Position
- Employees

Why You Need to Know About Information Security

- Without information security, SHS cannot protect PHI, other sensitive information, and other valuable SHS resources
- The Health Insurance Portability and Accountability Act (HIPAA) requires SHS to provide for the physical and electronic security of PHI
- Our customers expect us to protect their privacy
- Major cybersecurity attacks pose a major threat to SHS

What Are The Most Common Cybersecurity Incidents?

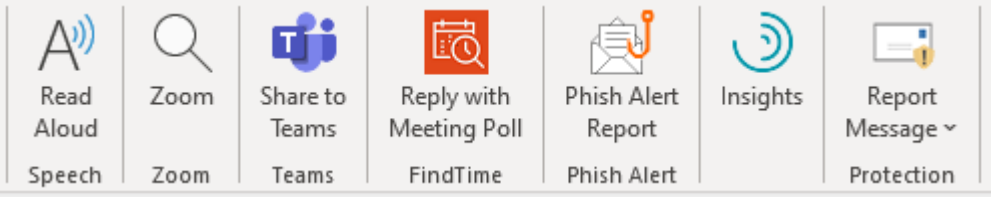
- Phishing Emails
- Computer Viruses (especially Ransomware)
- Stolen or cracked passwords and passcodes
- Phone-Based Social Engineering
- Loss, theft or compromise of Mobile Devices
- Improper Disposal of Sensitive Information

Phishing Email Attacks

- Phishing Emails are attempts to deceive you
- Phishing Emails often contain:
  - Promises, offers, or threats
  - A link that takes you outside the SHS network
  - Requests for your user name and password
  - An attachment that contains a computer virus
- Phishing Emails are the #1 cause of data breaches

How to Protect Yourself from Phishing Email Attacks

- Check the sender – is it from an external source?
- Verify the email sender before responding
- Hover over links to check web addresses
- **Never reveal your SHS network password or one-time passcode to anyone, including co-workers**
- **SHS will never contact you and ask you for your network password or a one-time passcode**
- Report phishing emails using the “Phish Alert Report” button



Samaritan Health Services

Building healthier communities together

Computer Malware (especially Ransomware)

- “Malware" is short for malicious software and refers to software that causes damage to computers or networks. Ransomware is a type of malware.
- Malware can be introduced to the SHS network if employees:
    - Share their username and password or passcode with a cyber criminal
    - Open an email attachment that contains a virus
    - Download and open a malicious file from a website
    - Insert an unauthorized USB device and copy an infected file to an SHS computer

Protecting Yourself from Malware

- Internet use on the SHS network should be limited to business-related purposes
- Use personal devices to conduct personal Internet activity. Personal use of the Internet must be conducted on the Workforce Member's own time, i.e., during rest breaks and meal periods
- Visit only trusted websites – avoid "surfing the web"
- Do not open attachments from unexpected or untrusted external email sources
- Maintain anti-virus protection on personal computers and mobile devices that you use to connect to the SHS network
- Contact the IS Service Desk if you are uncertain about the trustworthiness of an email or a website

Choosing and Protecting Your Passwords

- Longer and more complex passwords are generally more secure
- Passphrases can be easier to remember and are often harder to crack
- Never share your SHS Network password with anyone
- Do not reuse your SHS Network password on any other program or website
- Do not write your password down and store it in an unsecured place, especially on your desk or on or next to your computer

Samaritan Health Services

Building healthier communities together

Phone-Based Social Engineering

- Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
- External callers might ask you to:
  - share your password, your onetime passcode, or your email address
  - navigate to a website and download a document
  - Make changes to your SHS computer

How to Protect Yourself from Phone-Based Social Engineering Attacks

- Don’t trust caller ID. Caller ID spoofing is easy and widespread
- Verify external callers
  - Ask for their name and telephone number
  - Offer to call them back at their number
- **Never reveal your SHS network username, password, or one-time to anyone, including co-workers**
- **SHS will never contact you and ask you for your network password or one-time passcode**
- Call the IS Service Desk if you receive a suspicious phone call

Samaritan Health Services

Building healthier communities together

Mobile Device Security

- Do not text PHI or other sensitive information using the text messaging apps on your phone.
- Secure laptops, tablets, smart phones, and USB drives at all times
- Do not leave mobile devices, including SHS laptops, unattended in your car
- SHS policy prohibits the use of Siri, Alexa, or other “smart speakers” to dictate and transcribe PHI. Workforce members may only use Dragon or other approved dictation tools.
- When in doubt, contact the SHS Privacy Officer or Information Security Officer

Security when Working from Home

- Secure your home office
  - Use a strong password on your home wireless router
  - Maintain a secure and private workspace
  - Do not allow family or household members to use your SHS-issued device or to use your personal device while it is connected to the SHS network
- Make sure that the personal computers that you use to telecommute are:
  - Running up-to-date software
  - Protected from malware with an update Anti-Virus tool
  - Configured to auto-lock when you step away from them

Proper Disposal of Sensitive Information

- Dispose of all papers in designated Confidential Shred bins.
- All CDs, DVDs, or USB devices that contain sensitive information and are no longer needed should be sent via SHS courier to the IS Security Team at Samaritan Square.

Samaritan Health Services

Building healthier communities together

If You See Something, Say Something

- Report anything suspicious or out of the ordinary ASAP
- Rapid response minimizes the damage done
- Report lost or stolen devices or equipment to the IS Service Desk immediately at:
  - (541) 768-4911
  - SHSISServiceDesk@samhealth.org

Samaritan Health Services

Building healthier communities together

Reporting Concerns

Report Concerns Through your Chain of Command ASAP: *Supervisor > Manager > Director > AVP > VP > Site COO > Site CEO > CEO*		
Compliance Team: Colleen Fair, VP, Compliance & Privacy Officer James Kelly, Information Security Officer Brooklyn (Brooke) Mills, Privacy Program Manager Tyler Jacobsen, VP, General Counsel Altove (Tovee) Rowley-Esch, Sr. Asst. General Counsel	 541-451-7928 541-768-4507 541-768-2165 541-768-4478 541-768-4691	 cfair@samhealth.org jkelly@samhealth.org brmills@samhealth.org tjacobsen@samhealth.org alrowley@samhealth.org
Anonymous Hotline: 1-866-297-0489 or www.ethicspoint.com and search for "Samaritan Health Services"		
Oversight Agencies: Department of Health & Human Services (HHS), Oregon Health Authority (OHA), Centers for Medicare & Medicaid Services (CMS), etc.		

Samaritan Health Services

Building healthier communities together

Non-retaliation

- SHS does not tolerate retaliation for good faith complaints
- SHS policy takes retaliation extremely seriously
- If you feel like you've experienced retaliation, report your concern immediately to HR or the Compliance & Privacy Officer, or via the anonymous hotline