Welcome

WHAT YOU NEED TO KNOW TO COMPLETE THIS MODULE:

- There are 24 slides in this module
- To advance to the next slide, select the **NEXT** button
- To review information on a previous slide, select the **BACK** button
- Your exam questions are within this training
  - 2 attempts to answer correctly are allowed per quiz slide
  - Once you have selected your answer(s), select the **SUBMIT** button
  - If you want to change your answer before submitting, select the **CLEAR** button
- To pass the training, you must answer 6 questions correctly

Questions? Contact SHS Professional Development
at 80-5116 or 541-768-5116

Samaritan Health Services
Building healthier communities together

Information Privacy: What Is It?

Establish and maintain the confidentiality and security of our patients' and members' Protected Health Information (information that identifies an individual and relates to their health care, or payment for care) in all forms – paper, verbal, or electronic.

Samaritan Health Services
Building healthier communities together

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

- With the individual's authorization
- When it is part of your work-related duties for:
  - **Treatment**
  - **Payment**
  - **Healthcare Operations**
- When permitted or required by law

Samaritan Health Services
Building healthier communities together

Minimum Necessary Standard

- In general, only access, use or disclose the minimum amount of PHI necessary to do your job or to fulfill a legitimate request

Samaritan Health Services
Building healthier communities together

Monitoring System Activity

- SHS monitors access to patient/member records to ensure access is for a legitimate business purpose (Treatment, Payment, or Operations)
- When potentially inappropriate access is identified – by audit or complaint – the incident is investigated by the Privacy Officer, the workforce member's Manager, and Human Resources.
- Inappropriate or unnecessary access may result in corrective action, up to and including termination of employment.
- See the Information Privacy & Security Investigation and Corrective Action policy for more information.

Samaritan Health Services
Building healthier communities together

Information Security: What Is It?

- 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

Samaritan Health Services
Building healthier communities together

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

Samaritan Health Services
Building healthier communities together

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

Samaritan Health Services
Building healthier communities together

What Are The Greatest Threats to These Valuable Resources?

- Phishing Email Scams
- Computer Viruses
- Revealing Login and Password Information
- Weak Passwords
- Phone-Based Social Engineering
- Mobile Devices
- Improper Disposal of Sensitive Information

Samaritan Health Services
Building healthier communities together

Phishing Email Attacks

- Phishing Emails are after your access to the SHS network
- 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

Samaritan Health Services
Building healthier communities together

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 to anyone, including co-workers**
- **SHS will never contact you and ask you for your network password**
- Call the IS Service Desk if you receive a suspicious email

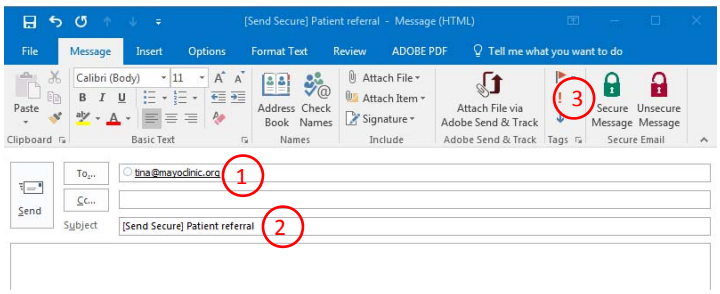
Samaritan Health Services
Building healthier communities together

Email Security

- Unless an exception has been made by the Information Security Officer, emails that contain PHI sent to an external recipient must be sent using “Send Secure” (Click the *Secure Message* button in Outlook; or enter the text “Send Secure” in the email subject line)
  - “Send Secure” only needs to be entered once – not on every reply email – so long as the phrase “Send Secure” remains in the subject line
- Double check email addresses when sending PHI or other sensitive information – ensure names and email addresses belong to the intended recipient prior to sending.

Samaritan Health Services
Building healthier communities together

Email Security



1. Confirm external recipient’s email address is correct
2. If email will contain PHI, enter a subject line, then:
3. Click “Secure Message” button OR type “Send Secure” in subject line

Samaritan Health Services
Building healthier communities together

Computer Viruses and Other Malware

- "Malware" is short for malicious software and refers to software that causes damage to computers or networks. Malware includes viruses, spyware, trojan horses, and internet worms.
- Malware is introduced to the SHS network most frequently when employees:
  - Open an email attachment that contains a virus
  - Download a file from a website
  - Visit a compromised website

Samaritan Health Services
Building healthier communities together

Protecting Yourself from Malware

- When logged onto the SHS Network, use of the Internet should be limited to business-related purposes
- SHS Workforce Members should use personal devices to conduct personal Internet activity. Any 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
- 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 Service Desk if you are uncertain about an email attachment or a website

Samaritan Health Services
Building healthier communities together

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 or email address
  - navigate to a website
  - download a document

Samaritan Health Services
Building healthier communities together

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 password to anyone, including co-workers**
- **SHS will never contact you and ask you for your network password**
- 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.
- SHS policy prohibits the use of Siri or other "virtual assistants" to dictate and transcribe PHI. Workforce members may only use Dragon or other approved dictation tools.
- When in doubt, contact the SHS Privacy or Information Security Officer

Samaritan Health Services
Building healthier communities together

How to Prevent Loss or Theft

- Secure mobile devices (laptops, tablets, smart phones, and USB drives) at all times
- Do not leave mobile devices unattended in your car
- Do not store sensitive information on your mobile device unless it is part of an approved business process
- Lock or log off your workstation when not in use
- Know and enforce your site's visitor policies

Samaritan Health Services
Building healthier communities together

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
- Rapid response minimizes the damage done in an information security incident
- 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

In Conclusion

- Only access, use and disclose the minimum information necessary to do your job
- Never text or use Siri to transcribe PHI
- Protect valuable SHS Assets
- Identify and understand threats to security
- Protect yourself from Phishing Attacks and Malware
- Safeguard your passwords
- Secure mobile devices
- Report anything suspicious

Samaritan Health Services
Building healthier communities together

Compliance Team

Colleen Fair, VP Corporate Compliance Officer
cfair@samhealth.org
(541) 451-7928

Erick Edtl, Privacy Officer
eedtl@samhealth.org
(541) 768-4948

Tyler Jacobsen, General Counsel
tjacobsen@samhealth.org
(541) 768-4478

Jim Kelly, Information Security Officer
jkelly@samhealth.org
(541) 768-4507

Altove (Tovee) Rowley Esch, Assistant General Counsel
alrowley@samhealth.org
(541) 768-4691

SHS Anonymous Hotline: 866-297-0489 or at www.ethicspoint.com

Samaritan Health Services
Building healthier communities together