



Caring. Healing. Leading.

Samaritan

Health

Corporate Compliance Program



Samaritan
Health

Corporate Compliance Program

Samaritan is committed and obligated to comply with all applicable federal and state standards.

The purpose of our Compliance Program is for **everyone to work together** to help Samaritan abide by federal and state laws, rules, regulations, and standards of ethical conduct.

Having a **proactive**, effective program helps us avoid fraud, waste, abuse, and discrimination that could put the organization at risk.

Corporate Compliance Program

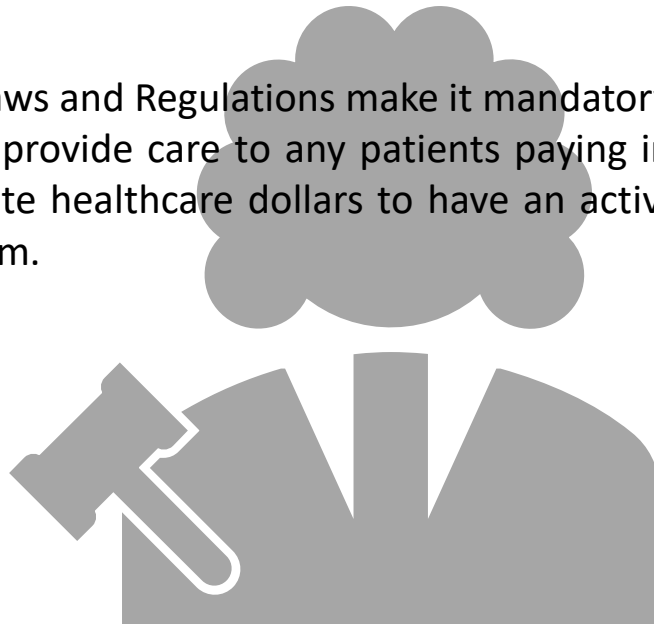
Applicability:

The Program applies to employees, medical staff, volunteers, executives, students, interns, vendors, agents, independent contractors and members of the Board of Trustees (“Representatives”) throughout Samaritan, which includes:

- ❖ Samaritan Medical Center
- ❖ Samaritan Clinics
- ❖ Samaritan Keep Home
- ❖ Samaritan Medical Practice
- ❖ Samaritan Summit Village
- ❖ Samaritan Home Health

Regulators:

Federal and NYS Laws and Regulations make it mandatory for **ALL** health care facilities that provide care to any patients paying in full or in part with federal or state healthcare dollars to have an active and effective compliance program.



Compliance Code of Conduct

Safeguard resources

- Protect the assets of the organization

Appropriately retain, authenticate, & destroy documents/records

- Familiarize yourself with our [Document Management Policy](#) and [Retention Schedule](#)

Maintain confidentiality

- Keep all patient info confidential

Avoid conflicts of interest

- As a charitable organization, we operate for public, charitable purposes and not for the private benefit of any individual. Report any potential conflicts to your supervisor and be familiar with our [Conflict of Interest Policy](#) on Heartbeat.

Report possible violations

- SEE SOMETHING SAY SOMETHING.

Integrity of billing and payer relationships

- All patient records, financial records, timesheets, and other business records must be accurate. You must not alter/falsify information on any record. When signing, only sign your own name; never sign for someone else. Report any suspected falsified information.

Train and educate

- Training is required initially and annually

Avoid inappropriate acceptance of gifts

Non-compliant acts may result in progressive discipline or other corrective action

- Never participate in unethical or illegal conduct. Act in an ethical and honest manner. You are expected to act consistent with our code of conduct, policies & procedures



Elements of an Effective Corporate Compliance Program



POLICIES AND PROCEDURES



COMPLIANCE OFFICER AND COMPLIANCE COMMITTEE



EDUCATION AND TRAINING



LINES OF COMMUNICATION



DISCIPLINARY STANDARDS



AUDITING AND MONITORING



INVESTIGATING/RESPONDING TO COMPLIANCE ISSUES

Element 1

Establish Written Policies/Procedures

Our policies and procedures provide guidance and are based on regulations + Samaritan's requirements.

Policies and Procedures are on Samaritan's Heartbeat page. You're responsible to review and follow them.

You can search & access policies on Heartbeat



Policies  > CORPORATE COMPLIANCE

*For CC policies - Filter Samaritan Dept. to: Corporate Compliance
You can also search for a specific policy in the search bar.*

Policy of Non-Intimidation and Non-Retaliation

'GOOD FAITH'
means with honest
intent & motive

Per our [Non-Intimidation and Non-Retaliation Policy & Procedure](#), affected Individuals will not be subject to intimidation or retaliation by any person affiliated with Samaritan based on reports that he or she reasonably believes to be true, submitted **in good faith**.

Violations of this should be reported to the Chief Compliance Officer or the Director of Human Resources

False Claims Act (FCA) forbids retaliation by Samaritan against an employee who cooperates with investigators regarding potential FCA violations or who commences qui tam actions in good faith.

Samaritan fully complies with applicable whistleblower protections. Per FCA, any employee who is discharged, demoted, suspended, threatened, harassed, or discriminated against in the conditions of employment by their employer because of lawful acts done by the employee per FCA, including initiation of an action filed under FCA, shall be entitled to all relief necessary to make the employee whole.

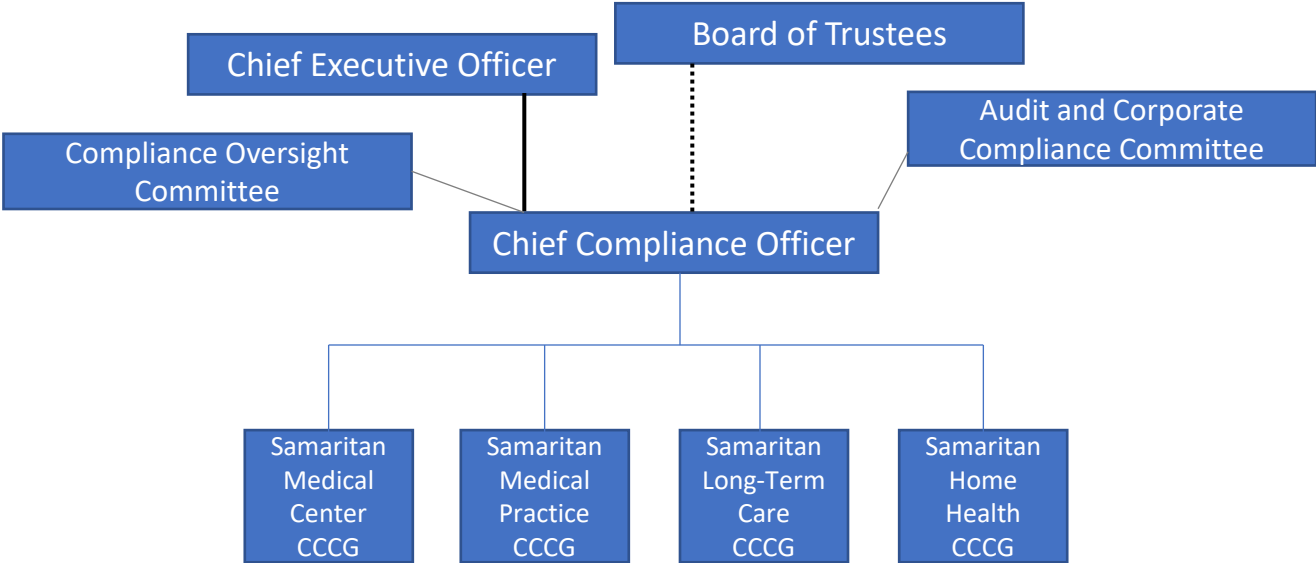
Relief may include reinstatement with the same seniority status the employee would have enjoyed but for the discrimination; two times the amount of back pay; interest on back pay; and compensation for any special damages

Element 2 Chief Compliance Officer (CCO) & Compliance Committee

The CCO is responsible for day-to-day operations and oversight of the Compliance Program, and reports to the Chief Executive Officer with a dotted-line report to the Board.

Each facility has a Corporate Compliance Core Group (CCCG) - they submit reports related to their Work Plan quarterly.

Compliance Officer Reporting Tier



Element 3 - Training & Education






- Required Initially and annually.
- Targeted training provided if/when needed
- Compliance & Ethics Week (*November*)
- Daily briefing

Element 4

Effective Lines of Communication

A person's identity will be kept confidential unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by the Medicaid Fraud Control Unit, Office of Medicaid Inspector General, or law enforcement, or such disclosure is required during a legal procedure or otherwise required by law.

Ways to report:

- Compliance Hotline (anonymous option) 1-877-740-7070
- Online submission form <https://samaritanhealth.com/corporate-compliance/corporate-compliance-concern/>
- Safety Zone
- Email  Compliance@shsny.com
- Phone  315-779-5186
- Face to Face  5 Pratt, by the sleep lab

Element 5 - Disciplinary Policies

Failure to comply with policies, procedures, code of conduct, or laws/regulations will result in disciplinary action. Our Corrective Action Policy/Procedure outlines the process.

Discipline is escalated based on circumstances of the violation.

Intentional/reckless behavior is subject to more significant discipline.

A copy of our Corrective Action Policy is [linked here](#).

Disciplinary Action

- Verbal Warning,
- Written Warning,
- Suspension,
- Termination.

Each representative is required to follow:

- Applicable federal & state regulations;
- Applicable Samaritan policies and procedures;
- Report suspected fraud/ abuse
- Participate in investigations;
- Engage in compliant & ethical behavior;
- Attend required trainings; and
- Assist in resolution of issues

Violations of blatant disregard or with malicious intent-

- could be terminated immediately

Element 6 Auditing and Monitoring

Addressing potential compliance issues as they are reported, including those discovered via auditing.



Corrective actions :

- Thorough and timely;
- Reduce risk of recurrence.
- Reported to OMIG or OIG. Refund Medicaid/ Medicare overpayments if applicable.

Auditing and Monitoring

Audits & Monitoring to identify RISK areas

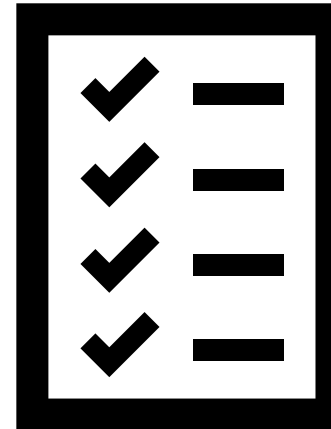
The compliance program MUST apply to risk areas which are areas of operation affected by the Compliance Program and apply to at least: Billings, payments, ordered services, medical necessity, quality of care, governance, mandatory reporting, credentialing, contractor/ subcontractor/agent or independent contract oversight; and other risk areas that should reasonably be identified by Samaritan through its organizational experience.

Monitoring Examples

- Walkthrough audits
- Review of medical record audit trails

Auditing Examples

- Review of OIG and OMIG work plan items
- Facility wide Risk Assessment



Results of risk assessments help determine what will be monitored the upcoming year & on the work plan.

The Work Plan is flexible & ever evolving.

Element 7 - Investigation & response

- Chief Compliance Officer (CCO) or his/her designee will promptly respond and investigate compliance issues raised.
- CCO may work with the appropriate leader to investigate a concern.
- Investigations conducted by Compliance are documented via a standard format. Investigations include a review of all relevant evidence (Ex. data, interviews, etc)
- **Corrective actions:**
 - Thorough, timely;
 - Reduce risk of recurrence.
 - Reported to OMIG or OIG. Refund overpayments if applicable.
 - Corrective Action Plans: Implemented by leadership to avoid recurrence of an issue. Involves a review of the cause of the issue, initial corrections and development of a plan to prevent recurrence that relates to the source of the problem. Person(s) responsible, and date for completion must be indicated.



Government investigations

If approached by an investigator or you receive a non-routine request, notify your supervisor & Chief Compliance Officer (CCO) immediately. Notify CEO/COO if CCO is unavailable.

It's imperative you do not inadvertently waive personal/Samaritan's rights such as attorney-client privilege, right to counsel, and right against self-incrimination.

Always ask to see agent's ID. Document the name, title, agency and phone #. Photocopy all documents presented.

Explain you must notify CCO and your supervisor to await guidance.

CCO will:

- Verify identity & documents
- Notify Director of HR + Risk Manager
- If it's a search warrant, CCO, QI Director, Risk Manager, CEO or AOC will escort the agent.
- **You have the choice to refuse to participate in any interview with government agencies. A court may later compel testimony.**



Gift Policy

- MEALS PROVIDED BY VENDORS with no educational/legitimate business component ARE PROHIBITED.
- Never accept gifts in exchange for prescribing/providing products, services/drugs, or intended to generate business. NO GIFTS ACCEPTED IF THERE'S STRINGS ATTACHED
- NO GIFTS TO GOVERNMENT employees/officials.
- Business courtesies that could influence conducting your duties must be declined. Providers have additional guidelines they need to follow in the policy.
- You're NOT TO GIVE GIFTS TO PATIENTS. This implicates Civil Monetary Penalties Law, Anti-Kickback, & ACO requirements
- You're NOT to ACCEPT GIFTS FROM A PATIENT/resident/family EXCEPT:
 - Those that are perishable items of nominal value given occasionally & shared w/ staff

IT'S OK TO ACCEPT A GIFT FROM A VENDOR, if it:

1. Has no intent to induce/reward referrals or purchase of health care items/services; and,
2. Has educational purpose; and
3. Is not in the form of cash/cash equivalent; and
4. Does not exceed \$100 per-person per-day. All must be met. Cannot exceed \$300 in a year.

- **Offered a gift and not sure if it's ok to accept?**
 - **Reach out to your manager or compliance to assist you**

["Acceptance and/or Solicitation of Gifts" policy](#) is available on Heartbeat.

Fraud, Waste, and Abuse

FRAUD is illegal; it exposes individuals or entities to potential criminal and civil liability, and may lead to imprisonment, fines, and penalties.

Examples of Fraud:

- Billing ins. for appointments the patient failed to keep;
- Knowingly billing for services at a complexity level higher than provided **or** documented (**upcoding**);
- Knowingly billing for services/supplies not furnished, including falsifying records to show delivery
- Paying for referrals (“**kickbacks**”).

Fraud, Waste, and Abuse

Waste is overutilization of services or other practices that, directly or indirectly, result in unnecessary costs to health care, including Medicare and Medicaid.



Examples:

Ordering excessive lab tests when only 1 test is needed.

A prescription for a brand name drug when a generic drug equally effective is available.

Fraud, Waste, and Abuse

Abuse:

Abuse means practices that are inconsistent with sound fiscal, business, medical or professional practices and which result in unnecessary costs to the medical assistance program, payments for services which were not medically necessary, or payments for services which fail to meet recognized standards for health care

Examples of Abuse:

- Billing for unnecessary medical services
- Charging excessively for services/supplies
- Misusing codes on a claim.
Ex. upcoding or unbundling

False Claims Act (FCA)

This law is to deter fraud, waste, and abuse.

Care must be **MEDICALLY NECESSARY**, appropriate, safe and **SUPPORTED BY ACCURATE DOCUMENTATION**.

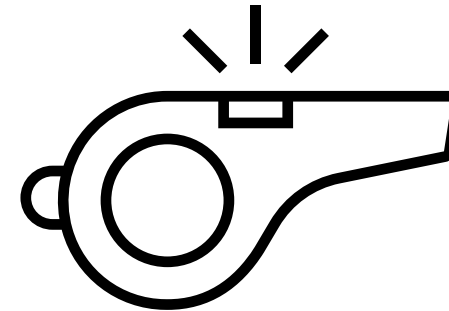
Must have proper credentials, registration, skills & competency. If your credentials are in jeopardy immediately notify Compliance.

Examples of False Claims include billing for services:

- Not provided
- Provided by an unqualified person (Ex. outside of scope, unlicensed, etc.)
- Billed in a manner other than actually provided

There's a Whistleblower provision.

- Allows government to elicit info from employees + offer monetary payments for the info. If determined a false claim was submitted (15% - 25% of money recovered)
- Civil penalties range from \$13,508 to \$27,018 for each false claim, in addition to treble damages and criminal prosecution.



Anti-Kickback Statute (AKS)

AKS makes it a crime to knowingly offer, pay, be involved in, or receive anything of value directly or indirectly to induce or reward referrals of items or services reimbursable by a Federal health care program.

Examples of prohibited kickbacks:

Receiving an extravagant trip or dinner associated with drug/supply company you do business with,

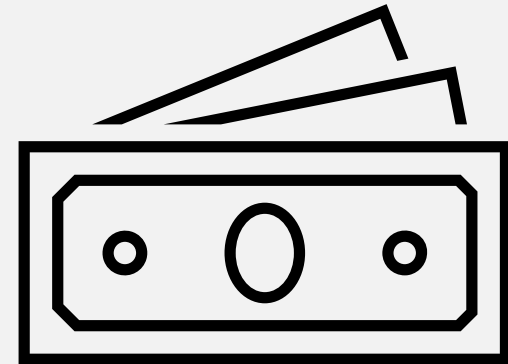
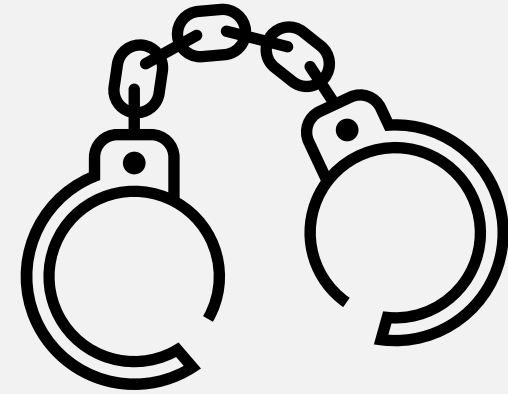
Receiving financial incentives for referrals,

free or very low rent for office space,

excessive compensation for medical directorships,

waiving copays, either routinely or on a selective case-by-case basis.

Possible penalties for violating AKS: fines of up to \$25,000, up to 5 years in jail, and exclusion from Medicare & Medicaid care program business.



Stark Law

Prohibits a physician from making a referral for services where she/he or an immediate family member has an ownership, compensation, or an investment interest.

Penalties may include:

- Civil penalties (up to \$100,000)
- Refund of the money
- Exclusion from Medicare or other health care programs
- Fines up to \$15,000/service provided

Penalties can apply to both the physician & the organization that received referrals. . Penalties may increase if the parties knowingly act together to “circumvent” or avoid Stark Law requirements.



Program Exclusion

Office of Inspector General oversees federal healthcare regulations, and

Office of Medicaid Inspector General oversees state healthcare regulations.

Exclusion lists include individuals/entities not allowed to care for directly/indirectly patients paying in full/part with federal/state healthcare program \$. E.g. Medicare, Medicaid, Tricare, etc.

On list for at least 5yrs; reinstatement is not automatic.

Program Exclusion Authority

Reasons for exclusions:

- Fraud or other health-care related misconduct
- Patient abuse/neglect
- Convictions for unlawful distribution, prescription, dispensing of controlled substances
- Suspension, revocation, or surrender of a license related to professional competence/performance, or financial integrity
- Providing unnecessary or substandard services
- Engaging in unlawful kickback arrangements
- Defaulting on health education loans

You may not provide services paid for by government health care programs such as Medicare/Medicaid if disqualified or excluded.

You must immediately report any exclusion to the Compliance Officer.

In the news...

- **CEO & 4 Physicians Charged in Connection with \$200 Million Health Care Fraud Scheme Involving UNNECESSARY PRESCRIPTIONS OF CONTROLLED SUBSTANCES and Harmful Injections**
- **Allegiance Health Management, Inc., \$1.7 million fine to resolve FCA allegations they submitted, and caused other hospitals to submit, claims for reimbursement from Medicare NOT MEDICALLY REASONABLE AND NECESSARY.**
- **NY doctor sentenced to 4 years in prison FOR TAKING BRIBES In test-referral Scheme With NJ Clinical Lab**
- **\$114 Million Judgement against 3 Individuals for PAYING KICKBACKS for Lab referrals and medically unnecessary Tests**

Accountable Care Organization (ACO) & Medicare Shared Savings Program (MSSP)

ACOs are groups of doctors, hospitals, and other providers, who give coordinated high quality care to Medicare patients. The goal is to ensure patients, especially chronically ill, get the right care at the right time & avoid unnecessary duplication of services. SMC and SMP participate in an ACO

MARKETING - Materials must be CMS's template. See "ACO Marketing and Beneficiary Communications" policy on Sharepoint.

RETENTION - We must maintain ACO records at least 10 years from the ACO agreement/or an audit (whichever is later) unless a longer period applies

NOTICE Medicare fee-for-service beneficiaries must be notified that we participate in MSSP and be given the opportunity to decline claims data sharing. See [FORM - ACO Beneficiary Notice - #402](#). Your supervisor can review this notification process in more detail with you.

SIGNS about our ACO must be in facilities & CMS notices available & provided upon request.

We're prohibited from:

•(1) **INDUCEMENTS TO BENEFICIARIES.**

Civil Monetary Penalties Law prohibits anything of value to Medicare or Medicaid beneficiaries if you know or should know it is likely to influence the beneficiary to order or receive items/services payable by federal or state programs.

•(2) **CONDITIONING PARTICIPATION** on referrals of Federal health care program business that the ACO, its ACO participants, ACO providers/suppliers or others related to the ACO know or should know is being provided to beneficiaries who are not assigned to ACO

•(3) **REQUIRING THAT PATIENTS BE REFERRED ONLY TO ACO** participants, except for referrals made by employees/contractors operating in scope of employment or contract, provided employees and contractors remain free to make referrals without restriction or limitation if the beneficiary expresses a preference for a different provider; the beneficiary's insurer determines a provider/supplier; or the referral is not in patient's best medical interests.

You may contact the ACO Compliance Officer directly: Tonya Gregory tgregory@signifyhealth.com, or:

Report the issue anonymously

844-232-8709, location "ACO"
OR
www.signifyhealth.ethicspoint.com

Subpoena and Summons:



A SUBPOENA is a document that commands the person designated in it to either produce records for court (i.e., subpoena *duces tecum*) or appear/testify in court (i.e., subpoena *ad testificandum*) under a penalty for failure to comply.

A SUMMONS is a form prepared by the plaintiff's counsel & is issued by a court that informs the defendant that they're being sued or are required to appear in Court.

- **If a process server comes to deliver a subpoena or summons, do NOT accept it.**
 - Instead, anyone attempting to serve documents should be directed to appropriate hospital personnel at 830 Washington Street:
 - If related to Samaritan business, it must be directed to Risk Management.
 - If it pertains to a patient/an employee for documents **unrelated** to Samaritan business, the Manager of Emergency Preparedness and Security is the point of contact.
- If a subpoena/summons is delivered by mail, email a copy to Risk Management Director on the day of receipt (Bhusenitza@shsny.com).

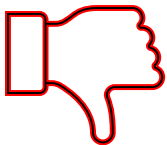
Health Insurance Portability and Accountability Act ("HIPAA")

HIPAA

- To protect the privacy of a person's past, present or future physical/mental health condition & any services associated with their care.
- **PROTECTED HEALTH INFORMATION ('PHI')** is Information which relates to an:
 - Individual's past, present, or future physical/mental health or condition, or
 - the provision of health care to the individual, or
 - past, present, or future payment for the provision of health care to the individual and
- That identifies the individual *or for which there's a reasonable basis to believe can be used to identify them.*
- Includes clinical, demographics, and/or financial info. (examples: Name, birth date, medications, insurance info., etc.)



Example of appropriate access to PHI would be a nurse caring for a patient and needing to enter the patient's vitals into the electronic medical record ('EMR')



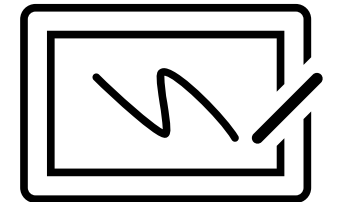
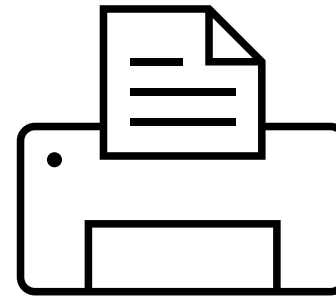
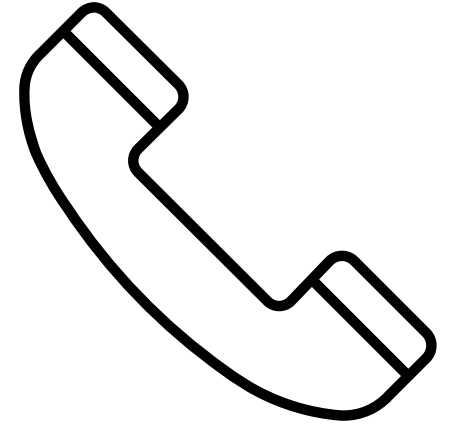
Example of inappropriate access would be a nurse who is NOT caring for a patient, but is curious about the care the patient is being given and accessing their PHI.

HIPAA

- **WHITE BOARDS** – Patients in Confidential status will be signified by initials on the white boards along with the room number. This means they don't want anyone to know they are here. No calls, flowers or visitors are to be directed to them
- **PHONE CALLS** – Aside from the exceptions below, If someone calls and specifically asks about a patient by name, we can only give health condition “**in general terms**” via phone about the patient (I.e., The patient is doing well, not doing well; or, stable/unstable condition). Do not get into test results or specifics.

Exceptions: If a patient is in Behavioral Health, Addiction Services, or in Confidential/Restricted status, no information at all may be given out without the patient's permission; if there is not a proper written consent, you can neither confirm nor deny that the patient is here (I.e. , “I am sorry, they are not in our directory.”)

- **FAXING** – Samaritan fax **COVER SHEETS** must be used for external AND internal faxing. There is a confidentiality disclaimer on them.



👉 Privacy & confidentiality is **everyone's responsibility**. Everyone is accountable.

👉 Keep PHI private and secure at all times

👉 Make sure only SMC personnel who need PHI access it or see it

👉 Use only the **MINIMUM** amount of PHI **NECESSARY** to accomplish a task. Access to a system does not imply you're authorized to view and/or use all information it.

👉 Read and understand SMC privacy policies, procedures, and Notice of Privacy Practices

👉 Know who your Privacy Officer is and consult her as needed

👉 Privacy requirements apply post-employment too

👉 Double check correct content to correct recipient

How to avoid HIPAA Violations

- ✓ **KEEP VOICES DOWN** so others nearby cannot overhear.
- ✓ **DO NOT DISCUSS** patients in hall, elevators, or outside the organization.
- ✓ When entering a patient's room, always **ASK THE PATIENT** if ok to speak openly if they have visitors or if they should step out.
- ✓ **NEVER LEAVE** medical records or any **PHI UNATTENDED**.
- ✓ **PROPER DISPOSAL OF PHI** is in a black bag then in a shredder, never in a trash/recycle bin.
- ✓ Only access patients' info. when caring for them. **“NEED TO KNOW” BASIS ONLY**. Access to a chart is to only be for a legitimate work purpose at that time and must be within the scope of your assigned duties.
- ✓ **DO NOT “SURF” MEDICAL RECORDS FOR POTENTIAL ADMISSIONS.**
- ✓ If there is a permissible, work-related reason for PHI to be **transmitted to an external email account**, the user must utilize their Samaritan email address and type the word encrypt or secure (must be typed using all caps, all lower-case, or capitalized first letter) in the subject line prior to sending.

HIPAA

- ✓ **YOU ARE NOT TO ACCESS A FAMILY MEMBERS' RECORD AT ANY TIME.** A signed release from patient must go to Health Information Management (HIM) or patient can access the info. on portal
- ✓ Do not take home any PHI- this includes daily status lists. PHI must stay on work premises.
- ✓ You're responsible for your password, never share it with anyone.
- ✓ If Law Enforcement or Military question you on a patient, do not give them any info. Direct them to your supervisor, Compliance, or HIM.
- ✓ Do everything you can to respect patients' privacy & report known or suspected violations to the Compliance Officer immediately.
- ✓ **Make sure you're in the correct record. It's *very important* that you verify the identity of the patient by confirming their demos (ex. name, date of birth) to make sure you are in the correct record before you enter information in the EMR. It is critical that you select the correct patient's account.**
- ✓ Verify the identity of the patient; ask *them* to provide their demo information *to you* (not the other way around)



HIPAA – Sanctions Policy

- We have a policy specific to HIPAA violations “[HIPAA Violations – Sanctions](#)”
- For employees, disciplinary action is done by Dept. Leadership on a record of warning within 15 days & given to Compliance & HR.
- HR, Leadership and Compliance Officer are afforded discretion to determine level based on circumstances.
- Violations by medical staff and allied health are reported to VP of Medical Affairs. Reviewed at reappointment.
- Violations by others will be evaluated on a case-by-case basis and may result in Samaritan discontinuing the relationship

Level 1	Unintentional	Remedial action & documented Verbal Warning
Level 2	Intentional/reckless disregard	Remedial action & Written Warning
Level 3	Malicious intent/personal gain	Remedial action & final written; or Termination.



Behavioral Health, Addiction Treatment, HIV/AIDS

- **Afforded a higher level of confidentiality & privacy**
- **It's often difficult for patients needing these services to reach out to obtain services**
- **If you're providing care to a patient receiving any of these services the ONLY time info can be discussed is:**
 - In direct relation to care you're providing at that moment, and ONLY to others also caring for the patient here when that info. is relevant to the care

Some information is kept in a separate database where fewer individuals have access. We factor into discipline inappropriate access or disclosure of this type of info.

Mental/Behavioral Health, Addiction Treatment, HIV/AIDS Permitted Disclosure and Uses

Disclosure of this information is only permitted pursuant to a specific, signed release of information, in accordance with 2782 of the New York State Mental Hygiene Law for confidential HIV-related information, New York Public Health Law Article 27-F, Mental Hygiene Law Article 33, Public Health Law Article 18 for mental health related information, Title 42 of the Code of Federal Regulations, Part 2 and Mental Hygiene Law, Article 22 for alcohol and drug related information, or as otherwise required or permitted by applicable federal or state laws or regulations.

A brief description of HIV Laws, Rules and Regulations are listed on the next page, for further guidance and clarification please see Samaritan's HIV-Confidentiality Policy which is located on the Heartbeat page.

A statement prohibiting re-disclosure must accompany all disclosures, including verbal.

HIV Laws, Rules and Regulations



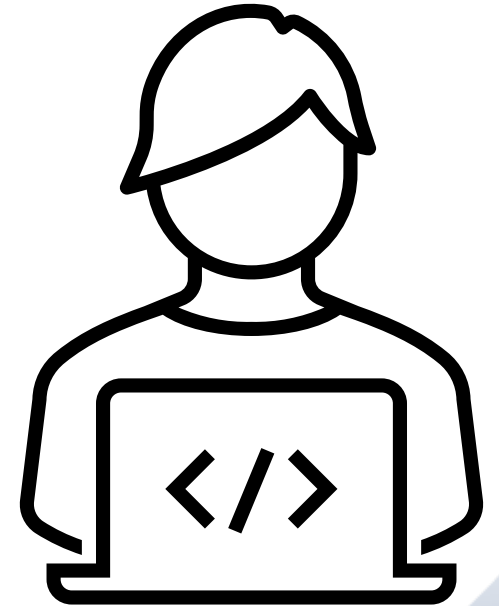
- Testing is voluntary
- Patient counseling is required for pre-testing and post-testing
- NYS specifies the manner and circumstances HIV-related information can be disclosed.
- In specific defined circumstances, a physician can notify a contact who may have been exposed to a patient who has tested positive without the consent of the protected person. In these cases, the physician must not disclose the identity of the protected individual or the identity of any other contact.
- Every time direct patient care is provided via telephone, a re-disclosure notice must be sent to the requesting party.
- An authorization form exclusively dedicated to release of any HIV information, must detail a limited time period, and contain the protected individual's signature.
- Consequences of disclosing confidential HIV-related information in violation of NYS law shall be penalized up to \$5,000 for being guilty of a misdemeanor.

Behavioral Health/Addiction Services

- Behavioral Health/Addiction Treatment service information cannot be released without a specific signed Release of Information (ROI), specific court order, to medical personnel in bona fide medical emergencies when prior written patient consent cannot be obtained, or a situation requiring mandated reporting of child abuse to the appropriate authority.
- Also, crimes on the Alcohol/Drug Treatment program premises or against Alcohol/Drug Treatment program personnel may be reported to law enforcement but the information must be directly related to that crime and must be limited to the circumstances of the incident, including the patient status of the individual committing/threatening to commit the crime, that individual's name and their last known whereabouts.
- Employees are not to speak to anyone on the phone without the client's record and ROI in front of them. Only info. indicated in the ROI may be disclosed.
- A Release of Information form must be completed by the applicable patient(s) in order for any visitors to enter the treatment area.

Confidentiality & Non-Disclosure

- All information in a patient's record is confidential. A properly completed, signed, and dated release of information authorization (ROI) is required for release of patient information. The H.I.M. Dept. handles the ROI requests.
- Access and use of clinical info. must comply with facility and privacy guidelines.
- **ACCESS TO YOUR OWN ELECTRONIC MEDICAL RECORD USING YOUR WORK LOGIN CREDENTIALS IS A VIOLATION OF SAMARITAN'S POLICY AND EASILY DETECTIBLE.**
- **Patient information is not to be shared outside of Samaritan. IT NEVER BELONGS ON SOCIAL MEDIA. Taking/posting a picture or reel on a social media platform like Tik Tok or Instagram captured in a clinical space is a violation.**
- Do not use your device (cell phone, etc.) to capture images, video, or audio, whether native to the device or through a 3rd party application. This is prohibited at work.
- Work business must be on email only, not on or to a personal email. Only use approved information systems and electronic media to store ePHI. Transfer/storage of ePHI on personal/home computers or other media is not authorized.
- ePHI should never be saved to local media (laptops, tablets, phones or other devices, *even if Samaritan-owned*). If necessary, PHI should be saved to network storage under the user's login credentials.
- Public charging ports are a risk for viruses (such as those at airports). Do not use these to charge a device if doing Samaritan business (E.g. SMC email) on that device.



Safeguard confidential information. This also includes business matters.

Confidential Information = In whatever form it exists, related to any person at the clinic, hospital/home & any information not generally available to the public.

Examples:

- Patient/employee demographics, religion, financial status
- Employee health records, medical care program and employment info
- Patient diagnosis, care plan, current & previous medical records + any other type of communication about patient info
- Computer system reports, access, passwords + security codes
- Medical Staff and peer review files
- Institutional business and financial records
- Verbal communication + conversations between patients, physicians, employees and the institution.

While working remotely:



Unplug personal assistants (such as Echos, etc.) while performing work duties.



Remote access to Samaritan systems is only to be offered through a secure Samaritan-provided means of remote access.



You should change default passwords on your wireless routers from existing passwords to a unique, strong password.



Password-protect mobile devices used for work purposes and don't allow others access to that device.



Samaritan's equipment/devices are to be used for Samaritan assignments, not personal reasons. Personal equipment would require approval by our MIS dept.



Only work in your private setting. Never in a public space/on public Wi-Fi, or in an area viewable or heard by others.



What constitutes a HIPAA breach?

A breach is a reportable incident to the patient(s) and the government. The HIPAA Privacy Officer does a Risk Assessment to determine if there's a risk of compromise to the PHI.



Possible consequences:

Consequences include fines, jail time, adverse action to an individual's license, reputational harm, civil suits

In the news...

PRESCENCE HEALTH - \$475,000

- **836 PAPER OR SCHEDULES MISSING.**
- Failed to notify patients, media & Office of Civil Rights within 60 days.

MAPFRE - \$2,200,000

- **USB DEVICE STOLEN. LEFT WITHOUT SAFEGUARDS OVERNIGHT.**
- Names, dates of birth and Social Security # of 2,209 individuals.
- Delayed/failed to implement corrective measures (encryption)

Largest HIPAA breach in history:

ANTHEM, INC.

\$16 MILLION PENALTY

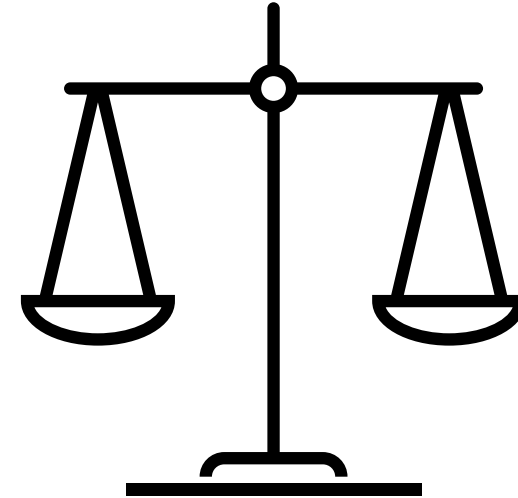
A series of cyberattacks exposed ePHI of **79 MILLION PEOPLE**

Occurred as a result of spear phishing

- These are targeted at specific people who have something in common.
- Spear phishers use information to lure you in & in an attempt to make you think the email is legitimate.

So, what are signs should you look for to help detect it's a scam?:

- A banner at the top of the email will caution you that it originated from outside of Samaritan
- Links and/or attachments in the email.



Samaritan Medical Center Policy on recording/filming

SMC patients/visitors:

- If the person recording is a family/friend of the patient being filmed and the patient is in agreement with the recording, staff will instruct that the scope must be limited to their patient relative/ friend and must not include others, without their prior consent.
- In Mental Health & Addiction Service, patients & visitors are prohibited from taking photos & recordings
- Prior to any recording, the patient must sign form “Filming, Voice Recording and Photography While You are a Patient at SMC” and the staff should confirm this has been signed.
- **When patient/visitor is taking pictures/recording without asking for prior agreement of those included in it, or without first signing the form referenced above, then:**
 - **They should be told they do not have permission, to stop, and asked to delete the photos/videos**
 - **If they refuse, staff should initiate the chain of command and call Security to assist. Visitors who fail to follow this policy may be removed from the premises and/or their recording devices may be confiscated & returned upon departure from the premises.**
- **Patients/visitors are prohibited from recording/photographing deliveries and other procedures.** However, once the infant is stabilized, videos/photos are permitted. All personnel present must be asked & give permission to be in any photos/videos & the patient/patient rep. must be in agreement.
- See our full policy, [linked here](#), for more information.




Brandi Husenitza,
Compliance Officer
(315) 779-5186
Office on 5 Pratt
bhusenitza@shsny.com



Ruth Strickland,
Compliance Specialist
(315) 779-6695
Rstrickla1@shsny.com

www.SamaritanHealth.com/Corporate-Compliance
confidential or anonymous



Hotline: 315-779-5170
or 877-740-7070



REPORT SUSPICIONS OR
CONCERNS.



CONTACT COMPLIANCE

Information Security Awareness Training:

“Good Computing Practices” for Confidential Electronic Information

- MIS Technical Services

Information Systems Security Awareness

After you complete this training you will gain knowledge to protect information systems and sensitive data from internal and external threats.

HIPAA /HITECH and state and federal laws govern the protection of ePHI (electronic protected health information and PII (personally identified information)

Samaritan Health personnel are **critical** to the defense and protection of sensitive information

You will understand our policies and procedures and your individual responsibilities to protect our most private information.

Define privacy and personally identifiable information (PII)

Identify how to respond to a suspected or confirmed security or privacy incident.

This presentation focuses on two types of confidential electronic information:

- **ePHI = Electronic Protected Health Information**
 - Medical record number, account number or SSN
 - Patient demographic data, e.g., address, date of birth, date of death, sex, e-mail / web address
 - Dates of service, e.g., date of admission, discharge
 - Medical records, reports, test results, appointment dates
- **PII = Personally Identified Information**
 - Individual's name + SSN number + Driver's License # and financial credit card account numbers

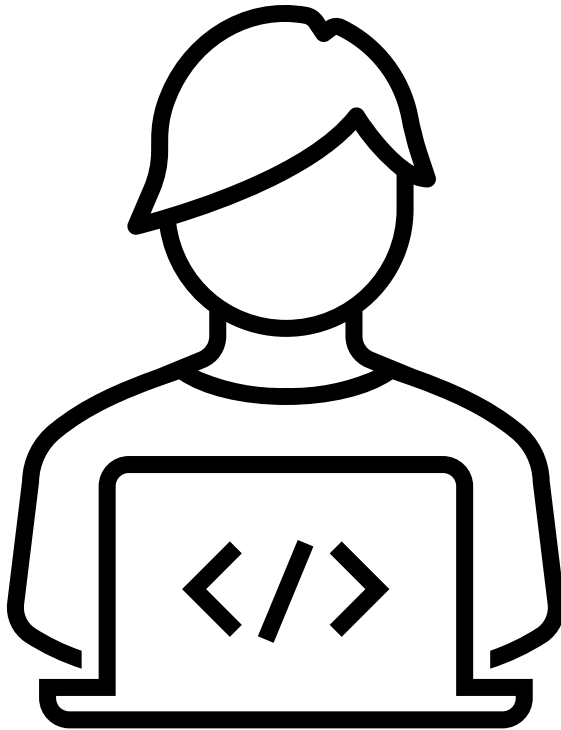
Security Objectives

- Learn and practice “good security computing practices”.
- Incorporate the following **7 security practices** into your everyday routine. Encourage others to do as well.
- Report anything unusual – Notify the appropriate contacts if you become aware of a suspected security incident.
- If it sets off a warning in your mind, it just may be a problem!

“Good Computing Practices” Safeguards for Users

1. **User ID or Log-In Name (aka. User Access Controls)**
2. **Passwords**
3. **Workstation Security**
4. **Portable Device Security**
5. **E-Mail best practices**
6. **Safe Internet Use – Social Engineering/Ransomware**
7. **Reporting Security Incidents / Breach**

HIPAA Security – Access Controls

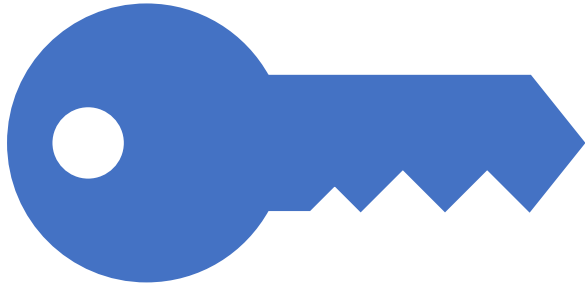


- HIPAA Security = Extension of HIPAA Privacy focused on ePHI
- Access Controls:
 - Users are assigned a unique “User ID” for log-in
 - **Use a UNIQUE password for Samaritan systems, not one used for any personal accounts.**
 - For example, do NOT use the same or similar password for Samaritan systems that you use for your social media account(s).
 - Do not use a password at Samaritan that is easily guessable (Meaning, if you post a lot about your dog Bruno on Facebook... Bruno123! is easily guessable.)
 - Each user’s access to system(s) is appropriate + authorized
 - Access is “role-based”
 - Access = limited to MINIMUM INFORMATION NEEDED to do your job
 - Unauthorized access to ePHI by former employees is prevented by terminating access
 - User access to information systems is logged and audited for inappropriate access/use

Password Protection

When choosing a password:

- Don't use a word that can easily be found in a dictionary or that you use for any other accounts.
- Domain (network) passwords need to be at least 12 Characters (Uppercase, Lowercase, Number and Special Character)
- Other systems such as Meditech have shorter password requirements due to limitations of their system
- Don't share your password. Protect it. After all, it is a "key" to your identity so never write it down.
- Don't let your Web browser remember your passwords. Public or shared computers allow others access to your password.



Workstations: Access Controls

- **Log-off** before leaving a workstation unattended. This will prevent others from accessing ePHI under your ID
- **Lock-up!** – Offices, windows, workstations, papers, PDAs, laptops, mobile devices / media.
- Lock your workstation (Ctrl+Alt+Del and Lock -or-Windows key & L)
- Encryption tools implemented when physical security cannot be provided
- Maintain key control
- Do not leave sensitive info on printers or copier.

Physical Access Controls

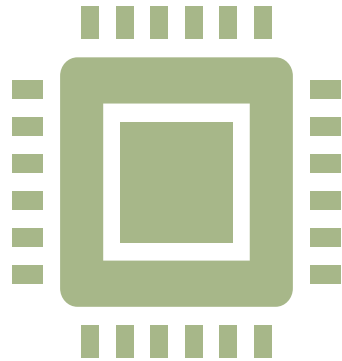
• COMBAT TAILGATING

Limit physical access to information systems & infrastructure to authorized personnel

- ✓ **Never allow** anyone to follow you in the building/secure area without their badge.
- ✓ **Escort visitors to and from your office &** around facility
- ✓ **Do not allow anyone else to use your badge**
- ✓ **Report** any suspicious activity to security.



Security for USB Memory Sticks & Storage Devices



Memory Sticks are devices which pack **big** data in tiny packages, e.g., 1GB, 3GB,8GB, etc..



Safeguards:

Memory sticks (USB thumb drives) are not allowed on the Samaritan Network with only a few exceptions.

NO EMPLOYEE SHOULD USE THEM WITHOUT MANAGER APPROVAL.

Delete ePHI when no longer needed

Protect devices from loss and damage

We only allow USB sticks on campus for very limited purposes.

Social Engineering

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Can be a call, text, in person, e-mail, or someone baiting you (i.e. thumb drives left in parking lot hoping you will plug it in.)
- A social engineer may use phone/internet to trick people into revealing sensitive info or to do something against policies.
- Signs of social engineering attacks to recognize:
 - Refusal to give contact information
 - Name-dropping
 - Intimidation
 - Urgency
 - Small mistakes (misspelling, misnomers, odd ?s)
 - Requesting forbidden or sensitive business or patient information

Social engineers exploit natural tendency to trust another's word, rather than computer security holes

They sometimes try to impersonate someone you trust within the organization, a vendor, or a government agent (DEA, IRS, CMS, etc.).

Never provide them with any information and report social engineering attempts immediately to compliance.

E-Mail Security

Email is like a “postcard”. Email may potentially be viewed in transit by many individuals, since it may pass through several switches enroute to its final destination or never arrive at all.

- Emails containing ePHI need a higher level of security.

-If sending PHI, force encryption by typing either the word encrypt or secure in the subject line prior to sending to manually force encryption of the message. It must be typed using all capitals, all lower-case, or capitalized first letter.

If it's suspicious: Don't open it! Don't click any links or open any attachments.

Ransomware is the new threat in healthcare – Ransomware typically comes in via “phishing” emails from outside sources.

What is suspicious?

- Not work-related
- Attachments not expected
- Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, or *.pif)
- Web link
- Unusual topic lines; “Your car?”; “Oh!”; “Nice Pic!”; “Family Update!”, “Very Funny!”

Email “Phish”

Date Thu 11/2/2017 6:18 PM
From Capital One
To [Redacted]
Subject [Account locked]
View HTML | Text | Header | Raw Content

Potentially dangerous scripts were removed from this message. Allow scripts

1 Caution: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.- Email sent from: "HHS"

Now check the account informations that belongs to you !

Why is my account access is blocked?

Your account access has been blocked for the following reason(s):

- We need to confirm some of your account information.
- We face a problem in the ratification of the real owner of the account. And for that you must follow the following steps :

- 1 Click on the Button Below
- 2 Log In Enter username and password
- 3 Verify Your Information To Activate Your Account

log in

1. Embedded Script
2. Grammatical Errors
3. Strange choice of words
4. Incorrect capitalization.
5. Ratification? I think they met verification!
6. Login link is to a different website

Samaritan Medical Center - Information Security Awareness Training

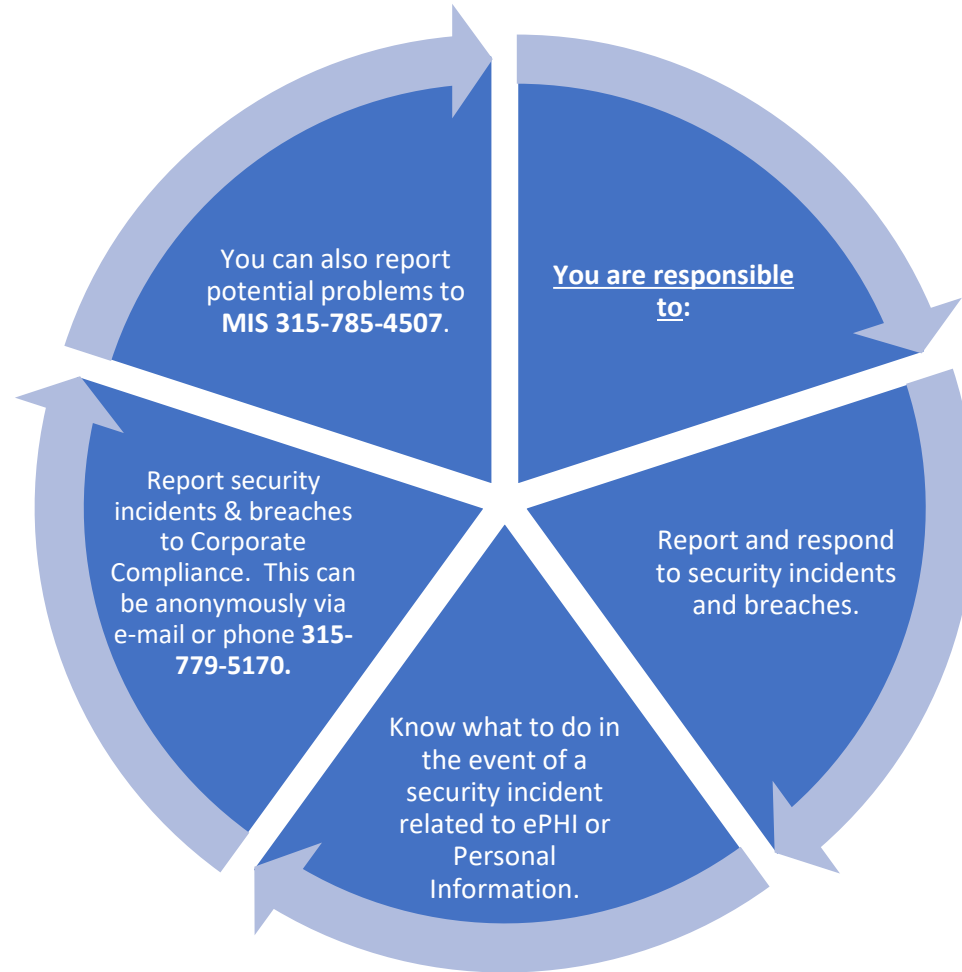
Hovering over a link will reveal the URL, which should be examined and compared with the email’s domain to look for discrepancies.

A decorative graphic on the left side of the slide features a light blue background at the top and an orange background at the bottom, separated by a torn paper edge. Three envelopes are visible: a white one at the top left, a green one in the middle, and a pink one at the bottom right, all appearing to be layered and slightly offset.

E-mails

- ***Remember:*** Emails are the property of Samaritan. They can be subpoenaed and considered admissible evidence in court for litigation or other administrative proceedings.
- As with medical records, all information in e-mails must be truthful & complete.
 - If you don't know an answer, say you do not know.
 - Write objectively.
 - Do not make assumptions.

Report Security Incidents



Security Reminders

- **Password protect your computer**
- **Never share your password or PIN numbers**
- **Backup your electronic information**
- **Watch for tailgaters and social engineering**
- **Practice safe email practices**
- **Keep office secured**
- **Keep disks locked up**
- **Run Anti-virus & Anti-spam software, Anti-spyware**

Resources for Reporting Security Incidents

Your Manager or Supervisor

MIS – Help desk or any MIS manager

Corporate Compliance Office

You are responsible for reading and understanding these policies/documents:

- Information Management Acceptable Use policy:

- https://shsny.sharepoint.com/:w:/r/sites/Policies/_layouts/15/Doc.aspx?sourcedoc=%7B3AE708F4-D4FC-47BF-973F-FD9A05E233E3%7D&file=Acceptable%20Use%20Policy.docx&action=default&mobileredirect=true

Information Management Password policy:

- https://shsny.sharepoint.com/:w:/r/sites/Policies/_layouts/15/Doc.aspx?sourcedoc=%7BC72D6597-EEE3-4DCD-A1A9-919D51A187CD%7D&file=Password%20Policy.docx&action=default&mobileredirect=true

- HIPAA Confidentiality policy:

- https://shsny.sharepoint.com/:w:/r/sites/Policies/_layouts/15/Doc.aspx?sourcedoc=%7B27865713-C533-48B5-8B5B-8688DE516510%7D&file=HIPPA%20Confidentiality.docx&action=default&mobileredirect=true

- IT Data security policy:

- https://shsny.sharepoint.com/:w:/r/sites/Policies/_layouts/15/Doc.aspx?sourcedoc=%7BFC365326-4180-4645-8708-34E7C2540B8B%7D&file=IT%20and%20Data%20Security%20Policy.docx&action=default&mobileredirect=true

- HIPAA Sanctions Policy:

- https://shsny.sharepoint.com/:w:/r/sites/Policies/_layouts/15/Doc.aspx?sourcedoc=%7BE3AC167E-C2DB-41B7-B444-4640E34A1CFD%7D&file=HIPAA%20Violations%20-%20Sanctions.docx&action=default&mobileredirect=true&DefaultItemOpen=1

- Notice of Privacy practices:

- <https://shsny.sharepoint.com/Online%20EForms/Forms/AllItems.aspx?id=%2FOnline%20EForms%2FNotice%20of%20Privacy%20Practices%2Epdf&parent=%2FOnline%20EForms>

By completing this training module, I am attesting to the following:

I acknowledge that I have:

- (1) Received education on Corporate Compliance and Health Insurance Portability and Accountability Act (HIPAA)**
- (2) Received and understand Samaritan's Code of Conduct and Notice of Privacy Practices; and,**
- (3) Reviewed and been educated to Samaritan Health System's Acceptable Use Policy and agree to abide by this policy; and,**
- (4) I acknowledge and agree to the following:**

All medical staff, employees, volunteers, affiliating students, and non-employees who have access to patient information, whether paper record or computer system are required to read and acknowledge understanding of personal responsibilities associated with confidentiality.

The services Samaritan Health System performs for all patients/providers are confidential. The good will of our health system depends, among other things, upon keeping such services and information confidential.

All information contained in the patient record is confidential and I am responsible to ensure the information remains confidential. Access and use of electronic clinical information must be in compliance with guidelines instituted for information systems.

Imprivata Multi Factor Authentication (MFA) is required to access Samaritan resources from an external location, such as an off-site location. New users will be setup with Imprivata MFA prior to accessing the Samaritan network and resources and will be provided documentation on how to setup Imprivata MFA.

Your unique password must be entered each time you access Hospital Information System. This individualized password must not be a common name or your initials, nor a password you use/used for a personal account.

By completing this training module, I am attesting to the following:

- In order to protect the confidentiality of our employees and patients and the integrity of our information system, you must not write down nor share this password with anyone, nor may you access an Application on someone else's behalf or attempt to access the system using another password.
- I understand that I am not to access or attempt to access confidential patient information using work log-in credentials, which is not required in connection with the provision of clinical services or any other authorized use for legitimate work purposes.
- This includes confidential information relating to employees' own and/or their families/significant other's care or treatment.
- I understand I need to follow the proper procedures in order to access my own health record by either Samaritan's Health Information Management Dept. or using the Patient Portal.
- Use of Samaritan's information systems are for business use only. Samaritan reserves the right to filter, monitor, access, or disclose information maintained on, stored in, or transmitted over
- its systems. Unauthorized use, disclosure, or copying of health information may give rise to a cause of action where Samaritan may seek legal remedies against me and result in disciplinary action.
- I understand that I'm expected to promptly report any issues/suspected violations to my supervisor or to the Compliance Department and I will fully comply with all aspects of Samaritan Health System's Corporate Compliance Program.



You've completed your 2024 annual Compliance and MIS Security education.

Click the "Take Test" button to complete your post-test.

If you have questions on this material, contact your supervisor or Compliance.

