Flagler Health +
Information Security & Privacy Handbook

Table of Contents

A Message from Information Security

As we continue to move toward an information intensive environment, our goal is to provide "Trusted Access Anywhere, Anytime." This requires the application of good practical information security measures by each individual.

This handbook is designed to heighten awareness about appropriate and prudent security measures. The concepts should not be considered all-inclusive, and each person must apply practical sense in securing confidential patient and sensitive Flagler information in performing their job. Practicing good Information Security helps insure information confidentiality, integrity, and availability in our mission to… "Provide the best patient experience with the best staff."

With Best Regards,

Melissa Cecil
Chief Information Security Officer

A Message from Compliance

We believe that Information Security and Privacy is everyone's responsibility. The protection of the information we work with is important to our patients, employees, and organization. The concepts in this guide will help you to understand the basics of Information Security and Privacy and to develop good work habits. Incorporating these practices into our normal day-to-day operations helps protect against disclosure of information while maintaining our integrity and building public trust.

With Warmest Regards,

Kelly Jenkins
Corporate Compliance Officer

Introduction

Information Security in the healthcare industry means protecting provider and employee information, as well as the patient information that is gathered on behalf of a patient for the purpose of providing treatment. Using good information security practices helps insure the confidentiality, integrity, and availability of the information we use, and helps build public trust.

Healthcare Shares The Same Business Needs as Others To:

- Avoid malicious virus attacks.
- Protect against attempts by "hackers" to affect the system through an interruption of service (e-mail "flood" attack, phishing, ransomware).
- Defend against loss of confidential patient information, employee information, and other sensitive information ("social engineering").

Federal and state laws and regulations make each person responsible for correctly and appropriately using information. These laws and regulations protect the confidentiality of individuals' information and set standards for information security measures.

Flagler Information Security Policies provide details of workforce members' responsibility for the protection of sensitive and confidential information generated and retained as a part of normal day-to-day operations.

Information Security Practices:

Use the guidelines that follow to help you establish good information security practices.

Data Access

- Treat all information as if it were about you or your family.
- Access only those systems you are officially authorized to access.
- Access only the information you need to do your job.
- Only share sensitive and confidential information with others who have a "need to know."
- Keep sensitive and confidential information secured when not in use.

Security Measures

- Use only your assigned User ID and Password to access any system or application.
- Always exit the system before leaving your computer.
- Create a "hard to guess" password.
- Never share your password.
- Change your password frequently (upon system request, or if you believe your password has been compromised).

Questions about Security?

The Chief Information Officer (CIO) is the primary person responsible for information security at Flagler. While there may be multiple individuals who work on information security, the CIO is your first contact for questions or any known or potential security issues.

Security Resource List

- Your first contact for Security questions or issues is your CIO. This person is assigned the responsibility to support security issues. The CIO can be reached by contacting the IS Help Desk at 904-819-4475, if the CIO is not available.
- You may also call the Corporate Compliance Officer, Kelly Jenkins, at 904-819-4221 to report security incidents.
- The Compliance Hotline (1-844-995-4983) may be used if these normal channels of communication have been tried and the problem has not been resolved, or if you would like to submit an anonymous concern.

USER ID and PASSWORD

Your User ID and Password identifies and authenticates you as a valid user of an electronic system or application.

You are responsible for properly "signing on" with your own User ID and Password. Most systems provide documentation of work performed and information reviewed by tracking movement in the system and detailing tasks. You should never give your User ID or Password to anyone else, and you should never use anyone else’s User ID and Password. Using or allowing someone else to use your User ID or Password is like giving a someone your bank card and PIN number. Flagler will hold you responsible for inappropriately sharing your User ID or Password and for inappropriately using another person’s User ID or Password.

Role-Based access and the User ID / Password

Access to applications or systems is based on your job function (role-based) and your "need to know." If your job function changes, your access should be reevaluated to insure that you only have access to the information you need to perform your job, but that the information you do need is available. You or your manager should contact the Helpdesk, if your job function changes.

CREATING QUALITY PASSWORDS

Different electronic systems have different capabilities for password management. When you have the choice, use the guidelines below to create high quality passwords rather than inferior passwords that are easy to guess.

Good Quality Passwords Are:

- Seven (7) characters or more
- Uppercase (A) and lowercase (a) letters
- Combinations of letters and numbers
- Symbols
- Easy to type
- Easy to remember
- Made up of a "pass phrase" (see example)

Think of a phrase that is unique and familiar to you, and easy to remember, but not easy to guess. Read the example used below, then create your own pass phrase. Note that in the example the first letter of each word in the pass phrase is used.

A rancher using the Phrase "All good cows like to eat green grass" might take a capital "A" and the lowercase "gcl" Use the number "2" followed by an "eg" and a "G" This gives you a pass phrase of "Agcl2egG".

This is only an example.
Do not use this as a real password!

Inferior Passwords Include:

- Your User ID or Account Number
- Your Social Security Number
- Birth, death, or anniversary dates
- Family member names (including pets)
- Your name (forward or backwards)
- Your favorite song, artist, author, etc.
- A word or name found in any dictionary

Examples of Inferior Passwords are:

Smithj123
(User account #)

004230019
(Social Security #)

122482suzie
(Child's birth date & name)

fred or fredfred
(Name once or twice)

naillig
(Gillian spelled backwards)

denveranniesong
(favorite artist and song)

Wombat6
(Added random character)

PHISHING

Phishing is the attempt to acquire sensitive information such as usernames, passwords, health information, credit card or bank account details, and other sensitive information for malicious reasons by masquerading as a trustworthy person or organization in an electronic communication. If you receive an email that directs you to either visit another site or click on a link to update personal information this may very well be a fraud or scam. Report any suspicious email to the IS Help Desk at 819-4475 or forward the email to the Help Desk immediately.

VIRUSES

Healthcare organizations have become dependent on computer systems to support their information needs. Interruption of service or corruption of data due to computer viruses is a significant problem, but awareness about viruses and education about how to prevent them can decrease the risk. Some of the more common characteristics of viruses are:

- Viruses are most commonly found in files with the names ending in **.exe**, **.vbs** and **.com**. Use caution with e-mail attachments/files containing these suffixes.
- Many viruses are designed to send, modify, or delete files from the infected computer.
- Many viruses are designed to send themselves to colleagues of the person who opens the infected file.
- Viruses can also be spread by downloading infected Internet files or pictures or by using infected disks or other storage media.
- Multiple e-mail messages with attachments and the same subject line from different senders are often a sign of a virus attack.

Virus Protection

What can you do to help prevent the spread of viruses both at work and at home?

- Use virus protection with the most recent updates.
- Use only licensed software from known and trusted sources.
- Use disks obtained from a known source inside Flagler.
- Remove disks from your computer drive before you start up in the morning.
- Contact Information Services before downloading software from the Internet.
- Only open e-mail or e-mail attachments when you know the source of the email and that you need to perform your job
- If you receive an attachment unexpectedly, or if the title of the attachment does not seem to match the content of the e-mail, check with the sender or contact the **IS Help Desk** at 819-4475 before opening the attachment.
- Do NOT attempt to bypass virus protection on your workstation at any time.
- Notify the **IS Help Desk** at 819-4475 if you suspect that a virus has infected your computer.

SOCIAL ENGINEERING & VERBAL COMMUNICATION

"Social Engineers" are individuals who attempt to gain access to systems or confidential information through the manipulation of others. Using a combination of basic knowledge about a given business with some personal information or details that the "victim" will recognize, the Social Engineer converses with, wins the trust of, and extracts information from an employee. One way they gather knowledge about a business and plan an engineering "attack" is simply by listening to employees who discuss sensitive and confidential information in public places.

Occasionally a social engineer will pretend to be an employee from IS, the Help Desk, the system maintenance employee of one of our outside vendors from an outside company.

Information Services will **never** ask you for your password. Never provide information about the computer system or applications, telephone connections, or network to anyone over the telephone unless you initiated the call and specifically know to whom you are speaking.

You can help combat Social Engineering by:

- Limiting your conversations in public places.
- Being aware of your surroundings and who listens to your conversations.
- Identifying as fully as possible anyone asking you for information.

WORKSTATION SECURITY

A workstation can be a terminal, instrument, device, or location where work is performed. The settings and tools will vary depending on the type of job you perform and the location from which you do it. Protection of your workstation and your equipment is your responsibility. Achieve "workstation security" by controlling your work area fully so that ALL of your information and equipment is kept secure.

Use the following guidelines to help you evaluate locations and equipment wherever you work to help secure your workstation and provide for information confidentiality, integrity, and availability.

Secure Workstations:

- When not in use, hard copy information, portable storage, or hand-held devices are kept in a secured (locked) area.
- Confidential information on any screen or paper is shielded from public view.
- Computers are not left active or unlocked and unattended.
- Computers have short (5-20 minutes) screensaver "time out" settings.
- Be aware and allow Flagler’s approved anti-virus software to actively scan files and documents.
- Only Flagler approved, licensed, and properly installed software is to used.
- Backups of electronic information are performed regularly.
- Surge protectors are used on all equipment containing electronic information.

Un-secure Workstations:

- Information in any form that is left unattended, open, and/or available to anyone that doesn’t have a need to use it to perform their job duties.
- PCs or terminals left unattended and "logged in" to the system and/or application.
- PCs located near exit doors that are not secured to an immovable object.
- Unapproved, downloaded Internet programs or applications.
- User ID and Passwords written down and physically displayed in any location.
- Providing information to another party without requiring the requesting party to authenticate their identity.
- If applicable, screensavers that are disabled.
- Anti-virus programs that are inactivated or not upgraded regularly.

What is your role as a workforce member?

- Exit applications and systems as soon as you complete your work.
- Never intentionally bypass or turn off security measures, including anti-virus software.
- If applicable, activate the screensaver when you leave the workstation.
- Manually scan media, files, and programs for viruses.
- Be aware of your surroundings. Who is able to view information or watch when Passwords are entered?
- Always keep portable equipment and devices with you and in your sight.
- Be sure to "Log off" of your computer before leaving work each day.
- DO NOT “shutdown” or power off your computer.

ELECTRONIC COMMUNICATIONS

The Internet and e-mail provide rapid means of sending and/or receiving information, but the responsibility rests with each individual to do "the right thing" with electronic communications. Some key points listed below will help you protect Flagler, as well as its workforce members, customers, and resources from risks associated with modern means of communication.

You are responsible for:

- Promoting effective and efficient business communication.
- Maintaining and enhancing Flagler’s public image.
- Using e-mail and the Internet in a productive manner.
- Sharing only the minimal amount of relevant information with people that allows them to carry out their job duties (sharing the “minimum necessary”).
- Transmitting information only to individuals who are authorized to see it (they have a "need to know").
- Not using publicly accessible areas of the Internet (e.g. discussion groups, bulletin boards, chat services, unsecured web site, etc.) to transmit or display information.
- Discussing your department's guidelines for acceptable personal use of electronic communications with your manager, employees, and colleagues.
- Only using e-mail and the Internet for limited personal use.
- Not using graphics, clip art, or other elaborate images or backgrounds in your e-mails.
- Using secure methods specifically approved in advance by Information Services to transmit information to appropriate individuals outside of Flagler.
- Using encryption when sending email containing protected health information (PHI) or personally identifiable information (PII). When composing an email, include **[SECURE]** as the lead word including brackets in the subject line.

You must never:

- Automatically forward messages using mailbox rules to Internet email addresses outside of Flagler.
- Transmit unsecured patient identifiable or other sensitive and confidential information outside of the Flagler system, including to external email addresses.
- Impersonate another user, or mislead others about your identity.
- Use electronic communication for any purpose that is illegal, contrary to Flagler policies, or contrary to Flagler’s or its patients’ best interests.
- Use a personal device to text protected health information (PHI) or personally

identifiable information (PII).

Users should have no expectation of privacy when using Flagler information systems. Information Services may log, review, track, and otherwise utilize information stored within or passing through any of the systems it utilizes in order to manage systems, enforce security, or conduct other activities Flagler determines are necessary. Flagler retains the right to monitor and access an employees' use of e-mail, the Internet, or any other of its information systems at any time and without prior notice. There are situations where "private" or "internal distribution" e-mails require public disclosure. A good "rule of thumb" is to never send any communication that you would not want published in the newspaper.

USING THE INTERNET

The Internet is a useful tool for gathering specific information from many sources. Like other computer-based tools, correct or incorrect use depends on the user. Use these basic "rules of the road" for the information superhighway:

- When an Internet site asks you to enter a User ID and Password, create one that is different from your network User ID and Password. (Internet sites requiring a User ID and Password do not always secure these fields.)
- Use only Flagler's e-mail service for messages when connected to the Flagler. (Outside e-mail services such as Yahoo or GMAIL do not provide the same anti-virus protection as Flagler's network.)
- Use secure methods specifically approved in advance by Information Services to transmit information to accounts or destinations outside Flagler, then only to those individuals having a need to know the information. (Appropriate agreements must be in place between involved parties.)

RECORDS MANAGEMENT

Records that have satisfied their required period of retention will be destroyed in an appropriate manner. The approved methods for de destroying Flagler information is based on the format of the information and include, but are not limited to, recycling, shredding, burning, pulping, pulverizing, and magnetizing.

A "record" is recorded information in any physical form that is generated or received in connection with transacting business. Records assume many forms, including x-rays, books, cards, blueprints, photographs, audio/video recordings, etc. Records include both Flagler business records and medical or patient records.

Policy-specific considerations of records management are:

- All records generated/received by Flagler is Flagler property. No workforce member has any personal or property right to Flagler records, even those personally developed or compiled.
- Unauthorized destruction, removal, or use of records is prohibited.
- No one may falsify or inappropriately alter information in any record or document.
- Records containing confidential and proprietary information will be securely maintained, controlled, and protected against unauthorized access.
- Workforce members should report information about unauthorized destruction, removal, use of Flagler records, or the inappropriate alteration or falsification in

records or documents to management or the Compliance Hotline at **1-844-995-4983**.

PATIENT PRIVACY

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires Flagler to protect the privacy of patient information; secure patient health information; adhere to the minimum necessary standard for the use and disclosure of patient health information and specify patients' rights for access, use and disclosure of their health information. Inappropriate use or disclosure of patient's PHI that violates HIPAA can result in civil and criminal penalties to Flagler as well as you as an employee or as an individual.

Notice of Patient Privacy Practices to Patients

The various Flagler entities that are subject to HIPAA publish their *Notice of Privacy Practices* on their respective areas of the Flagler Website. They are also made available to all patients during their registration process. The Notices describes how patient information may be used or disclosed and how patients may gain access to, request amendments to, and request restrictions on their protected health information. Flagler entities must comply with the information they provide to patients in their Notice of Privacy Practices. When patients have specific questions about their protected information, they should be referred to the appropriate Flagler entity's Notice of Privacy Practices or referred to Flagler's Privacy Officer, Cecilia Huffman at 904-819-4410 to obtain additional information.

Key Provisions of Flagler's HIPAA Policies

- Access and use confidential information only when necessary to perform your job duties. If you are not involved in the provision of care to a patient, then you have no right to access, use or disclose protected health information (PHI) related to that patient's care.
- Viewing or accessing the medical records of a family member, friend, or associate for which you are **not** involved in the treatment of is a violation of HIPAA and Flagler policy number *I – HIM - Employees Accessing their Own PHI.* Such violations are subject to disciplinary actions, up to and including termination.
- Minimum necessary - You are permitted to access and use only the minimum amount of patient information necessary to perform your duties
- You must be careful in communication or discussing PHI. Prior to speaking to a patient in the presence of others, ask the patient if it is ok to discuss their patient information in the presence of others. See Flagler Policy *I – HIM - Oral Communications with Patients* for guidelines.
- When mailing or handing documents to patients and family members, verify that each document belongs to that patient.
- Faxing of medical information – refer to policy *I – HIM - Faxing Protected Health Information*, for faxing guidelines.
- Do not leave patient records or other confidential information out and available for anyone to see. Make sure you always leave your workspace free of paper PHI before you leave.
- Do not dispose of PHI in trashcans; place in locked shredder bins in your work area.

- Do not discuss patient information outside of Flagler.

To report a breach of patient privacy or security

In accordance with Flagler policy, *I – HIM Breaches of Protected Health Information*, to report a known or suspected breach of patient privacy or security of information, you can send an email to hipaa@flaglerhospital.org or you can call these Flagler officials:

Flagler's Information Security Officer:
- Melissa Cecil at 904-819-1073

Flagler Hospital's Privacy Officer:
- Cecilia Huffman at 904-819-4410

Flagler's Corporate Compliance Officer
- Kelly Jenkins at 904-819-4221

You can also report anonymously via the Compliance Hotline at:
- 1-844-995-4983

In addition, all potential security breaches must be **immediately** reported to Flagler IS Help Desk at 904-819-4475.

Employees who fail to comply with Flagler privacy and security policies and procedures, or federal and state laws, shall be subject to disciplinary action in accordance with *E – COMP - Sanctions for Privacy and Security Violations.*

References

This *Security & Privacy Handbook* summarizes good user practices but is not a comprehensive document. For additional detailed information about Information Security and Privacy, refer to the Policies and Procedures located on the Flagler's Intranet. You may find them by accessing the Policies and Procedures link on the main page of Flagler's internet at https://flagler.hospitalportal.net/Flagler/main.aspx

Notes: