Objectives

• The purpose of this training is to teach you about your responsibilities and role in protecting information and information systems

• Understand the importance of safeguards and how and when to apply them

• Understand that everyone is responsible for protecting privacy and security
Who’s Job is it?

It is the job of each associate, physician and volunteer to ensure:

Privacy
And
Security

Winner of the “Not My Job” award
Privacy and Security Defined

**Privacy**: ensuring information is viewed and used only according to Sparrow’s policies; protecting individuals’ right to confidentiality

**Information Security**: putting safeguards in place to protect information

**Confidential Data examples**:

Identifiable patient information such as patient name, address, medical record numbers and any other information that can by itself, identify an individual or be linked with other information sources to identify an individual

Personal identifiable information such as Sparrow Associate, Physician or Volunteer social security numbers, dates of birth and driver’s license number
Why is it Important to Protect Information?

We need patients to trust Sparrow so they will give us complete information.

The more information that a patient gives, the easier it is for clinicians to deliver the right type of medical treatment. If we do not protect information, patients will no longer trust Sparrow.

We need to make sure that information is accurate and available when needed for treatment.
Protected Health Information

Protected Health Information (PHI) is individually identified health information that is transmitted by or maintained in any form – oral, written and electronic. At Sparrow, this could pertain to patient census reports, surgery schedules, patient charts, and electronic directories (such as STAR).

Patient Identifiers

The HIPAA Privacy Rule and Sparrow Privacy Policy define all of the following as patient identifiers whether they are used alone or in combination with one another:

1. Names
2. Street address, city, county, precinct and zip code
3. Birth date, admission date, discharge date and date of death
4. Telephone & fax numbers
5. Social Security numbers
6. Email addresses
7. Full face photographic images and any comparable images

Under HIPAA, a volunteer may not share any PHI with anyone that does not have a NEED TO KNOW.
Need to Know

HIPAA allows patient information to be disclosed for the following purposes:

• **Treatment** – providing care
• **Payment** – for services
• **Operations** – normal business activities

Before disclosing information ask yourself “Does this person meet the TPO test?”
Minimum Necessary

Access only the PHI you need to do your job
AND
Any time you share PHI, provide only the information the person needs to accomplish the purpose of the request

Three Key HIPAA Privacy Questions:
1. Is the patient information I am about to access necessary for me to complete my job?
2. Am I accessing only the minimum amount of information necessary to complete my job? No more and no less?
3. Am I accessing or using this information for Sparrow treatment, payment or health care operations reasons?
Examples of using PHI

**Appropriate use of PHI:** A Patient Ambassador communicates a patient’s concern or complaint to the Nurse Manager for follow-up

**Inappropriate use of PHI:** A volunteer informs the Volunteer Services Department that another volunteer is a patient in the hospital (without their permission). Under HIPAA guidelines, the Volunteer Services staff would not meet the TPO test!
Examples of Protecting PHI

• Never leave a patient list or schedule on a desk unattended. Keep the list with you or turn the list face down.

• When delivering items such as flowers or gifts, make sure the gift card with name and/or address is not visible to others.

• Census sheets or surgery schedules should be disposed of through shredding instead of using a public trash bin.
Technology Concerns

If you are a volunteer with access to a Computer, please use the following guidelines:

• Do not share your password or write your passwords on reminder notes
• Choose passwords that are difficult to guess and add a meaningful number
  Example: ECHASL99 (Every Cloud Has A Silver Lining!)
• Log-off before leaving your workstation unattended – even for just a few minutes. The hospital logs all inquiries into patient records. You are responsible for the activity that occurs under your password.
Technology issues cont.

Cellular phones with picture features create a potential risk to PHI and to both patient and associate privacy. Sparrow strictly prohibits the use of the camera feature in any Sparrow facility.

Cell phone use is limited to hallways, lounges, lobby, break rooms and conference rooms. Restricted areas have notification posted.

As a courtesy to patients and others, please set cell phones to vibrate mode, or turn off while on duty.
Other Privacy Issues

• “Identity Theft” means fraud or attempted fraud using the identifying information of another person without authority. Sparrow takes this very seriously and has protocols in place to help prevent this from occurring.

• Medical advice – Never provide medical advice or opinions. Always refer them back to appropriate caregiver.

• Laws regarding confidentiality of mental health and substance abuse patients are particularly restrictive, the presence of these patients in the hospital is never acknowledged.

• Never ask an acquaintance why they are at the hospital, no matter how well you know them.
Privacy – The End

You have completed the HIPPA section of orientation please remember to complete the orientation quiz.

Thank you!