Confidentiality/HIPAA

This information is review of important Health Insurance Portability and Accountability Act (HIPAA) requirements. Many of these requirements are included in our Code of Conduct and our Ethics and Compliance policies and procedures.

- We have always endeavored to deliver healthcare compassionately and to maintain our strong ideals.

- Our Mission and Values Statement is the cornerstone of our organization. It recognizes our commitment to deliver high quality, cost-effective healthcare in the communities we serve. It provides the value statements that we consider essential and timeless. The words selected from our Mission and Values Statement exemplify the type of conduct that all of us strive for.

Reporting Concerns

There will be no retribution for asking questions, raising concerns about the Code of Conduct or for reporting possible improper conduct that are done in good faith. Any colleague who deliberately makes a false accusation with the purpose of harming or retaliating against another colleague will be subject to punishment.

We encourage the resolution of issues at the local level whenever possible. To obtain guidance on an ethics or compliance issue or to report a potential violation, you may choose from several options:

- Consult your instructor.
- Consult your Facility ECO or another member of management at your facility.
- Call the Ethics Line at 1-800-455-1996.

The Ethics Line is an easy and anonymous way to report possible violations or obtain guidance on an ethics or compliance issue. You are encouraged to use the Line anytime, especially when it is inappropriate or uncomfortable to use one of the other methods. In order to properly investigate reports, it is important to provide enough information about your concern.

Information Security

HIPAA requires healthcare entities to appoint a facility information security official (FISO). The FISO leads the facility's Information Security Program. This program establishes standards and other requirements to safeguard the confidentiality, availability, and integrity of electronic protected health information (EPHI).

IDs and Passwords
Patient Financial Information, Clinical Information, and User Passwords are all examples of confidential information. A User ID without a password is not confidential and is frequently included in directories and other tools widely available. The person granting access to a system or application typically assigns a User ID to the end user, and the User ID is sometimes used for identification, tracking and other maintenance procedures within IT&S.

If you have access to information systems, please keep in mind that your password acts as an individual key to our network and to critical patient care and business applications, and it must be kept confidential. It is part of your job to learn about and practice the many ways that you can help protect the confidentiality, integrity and availability of electronic information assets.

Confidential Information
A patient's diagnosis, the Company's marketing strategy, and computer network configurations are all considered confidential information. The Confidentiality and Security Agreement states that individuals with access to confidential information will not disclose or discuss any confidential information even after termination of their relationship with HCA.

No HCA colleague, affiliated physician, or other healthcare partner has a right to any patient information other than that **necessary to perform his or her job**.

Examples of Appropriate Access:
- Viewing patients' information when you are involved in their care/treatment
- Signing-on to the computer with your own password.

Examples of Inappropriate Access:
- Viewing a relatives information…including a spouse or child
- Viewing a co-workers information…even if they request you do so
- Allowing someone to use your password
- Leaving a computer terminal unattended with patient information displayed on the screen
- Viewing your own record

Although you may use confidential information to perform your function, it must not be shared with others unless the individuals have the need to know this information and have agreed to maintain the confidentiality of the information.

Patient or Confidential information should not be sent through our intranet or the Internet until such time that its confidentiality can be assured. If it is necessary to send patient information to a business associate (*i.e*. someone outside HCA), arrangements other than e-mail must be made.

Privacy

HIPAA and its implementing regulations set forth a number of requirements regarding ensuring the privacy of protected health information (PHI).

HIPAA requires healthcare entities to appoint a Facility Privacy Official (FPO). The FPO in our facility oversees and implements the Privacy Program and works to ensure the facility's compliance with the requirements of the HIPAA Standards for Privacy of Individually Identifiable Health Information. The FPO is also responsible for receiving complaints about matters of patient privacy. The Facility Privacy Officer at Palms West Hospital is Donna Scheffler, Director of Health Information Management.

HIPAA regulations do not prevent medical records from being maintained at the patient's bedside or outside the patient's room; however, they do encourage reasonable safeguards be put in place to protect the patient's information from inappropriate uses or disclosures.

The HIPAA regulations contain a number of restrictions on the transmission of PHI; however, they do not prevent faxing or mailing health information as long as certain precautions are taken. The regulations mandate that health information may not be sold by a facility.

The Notice of Privacy Practices must be made available to all patients and posted on the facility's Internet site (unless the facility does not have a site). Any facility consent form language must reference the notice. Patients need to sign an acknowledgement form confirming receipt of the notice.

Patients have the right to access any health information that has been used to make decisions about their healthcare at our facility. They can also access billing information. They may review the paper chart (supervised) or be provided a hard copy. Access to the Clinical Patient Care System (CPCS) is not a recommended method of providing access to PHI.

A patient may have access to all of the records in the designated record set. This record set includes any information that is maintained, collected, used or disseminated by a facility to make decisions about individuals. The paper record is the legal medical record and a copy should be provided upon request (electronic access is not appropriate with our current systems.) A patient may be denied access under certain circumstances *(e.g.,* when a person may cause harm to him or herself or others, or when protected by peer review). Our FPO has more information on the right to access.

A patient may add an amendment to any accessible record for as long as the record is maintained by the facility. The request for amendment should be made in writing to the facility. The amendment may be approved or denied. Our FPO and the HIM department have more information on the right to amend.

While patients have a right to amend their record that does not mean that health information can be deleted from the record. The patient may submit an addendum correcting or offering commentary on the record, but no information may be deleted from the record.

In order for the HIM department to track releases of patient information, patients (including employees) should be directed to the appropriate personnel at your facility for access to any health information.

Everyone is responsible for protecting patients' individually identifiable health information. Any piece of paper that has individually identifiable health information on it must be disposed of in appropriate receptacles. The paper must be handled and destroyed securely. The elements that make information individually identifiable include: name, zip or other geographic codes, birth date, admission date, discharge date, date of death, e-mail address, Social Security Number, medical record/account number, health plan id, license number, vehicle identification number and any other unique number or image.

Any member of the workforce with a legitimate need to know to perform his/her job responsibilities may access a patient's health information. However, the amount of information accessed should be limited to the minimum amount necessary to perform his/her job responsibilities.

Policies prohibit employees/students from accessing their own records in CPCS (also known as Meditech). Typically, employees do not have a "need to know" for the performance of their job. Employees may, however, fill out the appropriate authorization in HIM and can obtain a copy of their records.

The hospital directory or listing of patients used by the PBX operator, information desk or volunteers should contain only patient name, room/location and condition in general terms. Patient diagnosis or procedures should not be released. Also, this information may not be released about confidential patients or patients who ask not to be listed in the directory or have their whereabouts known.

Lists of patients may be provided to clergy. The current Conditions of Admission form explains that the patient name may be released to local religious organizations. The lists should consist of the patient name, room/location, and may include the condition in general terms. This list should be restricted by religion. Confidential patients and patients who opt out of the directory should not be included.