Health Insurance Portability and Accountability Act (HIPAA)

CONFIDENTIALITY OF PATIENT AND HEALTH SYSTEM INFORMATION

Students of St. Luke's College will comply with the confidentiality of Patient and Health System Information policy of UnityPoint Health- St. Luke's which states:

All information regarding patients is legally and ethically considered privileged information. This information is not to be disclosed or used in any way other than as needed for treatment of the patient. Accidental or intentional disclosure, modification or destruction of patient information can result in legal action and/or loss of community credibility, reputation and business or as directed by HIPAA regulations. This confidentiality of patient information continues to exist when the patient also happens to be a co-worker or physician.

Information related to patient and health care is to be treated in a confidential manner. Employees, who are contacted by representatives of the media concerning any proprietary, technological, health care and/or patient information, must refer such calls to the Director of Community Relations who shall then be responsible for coordinating appropriate responses to such inquiries.

Failure to maintain security procedures for handling confidential information is considered misconduct and gross violation can result in immediate termination.

As part of our ongoing compliance program random audits for appropriate access to patient information will be conducted by the Privacy Officer. Potential inappropriate access will be reviewed by the manager and department director for employee or student involved in potential inappropriate access. Such inappropriate access can involve disciplinary action including verbal or written warning, suspension or immediate termination.

The following procedures are to be followed when a violation of confidentiality is discovered:

- When a violation of confidentiality is discovered, it is to be reported to the appropriate department director/manager. The department director/manager will notify the Human Resources Department if this involves and employee.
- The department director/manager is responsible for investigating the circumstances surrounding the violation. Areas to be investigated shall include, but not be limited to, the following:
- Determining whether the violation was intentional or accidental.
- The impact upon the Health System (includes public confidence as well as financial impact).
- The employee's or student's history of previous violations.
- The department director/manager will review the results of the investigation with a representative of the Human Resources Department prior to any disciplinary action being taken.

Privacy Audits

- Random privacy audits will be conducted on a routine basis by the Privacy Officer and results reported quarterly to the Compliance Officer.
- Potential inappropriate access identified on the audits will be reported to the Manager and Department Director of the employee involved in the access and investigation of the access will be conducted.
- Manager and Department Director will report back to Privacy Officer the findings of their investigation.
- In the event inappropriate access is confirmed, the manager and/or Department Director will involve Human Resource Director in plan for disciplinary action. Privacy Officer will also notify Human Resource Director of confirmed Privacy violation.
- Employees and students are responsible for all accesses made under their respective computer codes. In the event the employee or student denies entering the record, they will be held accountable for the entries made under their code.
- Disciplinary action will be determined with the assistance of Human Resources General guidelines for disciplinary action could include:
  - Confirmed inappropriate access- written warning to include possible immediate termination for future inappropriate access AND one to three day suspension.
  - Probably inappropriate access- (this may include access made with employee code but employee denies access & no previous incidents of inappropriate access.) Written warning to include possible immediate termination for future inappropriate access.
  - Repeat inappropriate access- termination.