FORT HEALTHCARE

STATEMENT OF CONFIDENTIALITY & SECURITY – EXTERNAL USERS

Date:_____

Last Name:_____ First Name_____MI_____

Position_____E-mail_____

Facility:_____ Business Phone _____

Access Time Frame: □ 1 year □ Other_____ Start Date_____

Manager:_____ Phone:_____E-mail_____

Purpose of Access:_____

Confidentiality

In the performance of your normal job duties, Fort HealthCare has granted you access to information that is confidential in nature. This information includes protected health information on our patients accessible through our electronic medical record.

Your use and/or access to this type of information may be required by the nature of your job duties and assignments. To the extent that you use or access this information as a result of your job duties and assignments, you are required to protect this information and maintain the highest degree of confidentiality regarding its use at your facility and outside your environment.

Your use and or access to confidential material as a result of your job duties and assignments is limited to only the information required by those job duties and assignments. If you use your job position or responsibilities to access information not required for your job, it will constitute a misuse. Deliberate efforts to use the privileges accompanying your official duties to gain access to data you are not authorized for, by breaching installed security provisions or getting around them, will constitute an abuse of your job responsibilities. This will include accessing information under someone else's log on and password or requesting that another employee access information that you do not have a need or right to access. This will include any information regarding yourself, family members, friends, coworkers, etc.

Even though your personal medical records or those of your family members may be maintained by Fort HealthCare facilities, you must follow the same rules as any patient would when accessing these records for personal reasons. Accessing your own medical records or those of your family members without your/their signed authorization is not allowed unless necessary to perform your job duties. To access these records, contact the Medical Record Department at the site where the documentation originated. Any unauthorized electronic access will be identified by an audit report.

Any abuse, misuse or dissemination of any confidential information (whether listed above or not) will result in minimally termination of access privileges and further action depending upon nature of the violation. By signing this agreement you are stating that you will follow all policies regarding access of protected health information set forth by Fort HealthCare in concurrence with State and Federal confidentiality and privacy laws.

Security of Information

It is imperative that all confidential information be maintained in a secure environment. Systems utilized by Fort HealthCare are equipped with security measures such as unique logins, passwords, etc that prevent unauthorized access. Your access is determined by your role within the organization. All users are expected to abide by the following guidelines:

STATEMENT OF CONFIDENTIALITY & SECURITY – EXTERNAL USERS

- Login IDs are assigned to authorized users to identify them within the systems they access. The user is responsible for all entries, activities and accesses to accounts made with their login ID. Passwords are not to be shared with others.

- Users may not manipulate software or hardware configurations, or load executable software on the hospital's workstations.

Fort HealthCare will monitor appropriateness of access of organizational protected health information. Users should be aware that:

- Monitoring of usage, access, and activity can and will occur, without notification or request for authorization.

Fort HealthCare will monitor access to the electronic medical record per organizational policy. All violations of external users will be reported to the employee's manager by the Fort HealthCare Privacy Officer. The manager will investigate the violation, complete an investigation form and return to the Privacy Officer. All confirmed violations will result in immediate termination of access rights for the employee. Further action will be determined by nature of violation.

It is expected that all employees review and comply with the Fort HealthCare Information Management Security policy. All violations or suspected violations should be reported to management or administration. Failure to abide by Fort HealthCare security guidelines and polices will result in minimally termination of access rights and further action depending upon nature of the violation.

It is the manager's responsibility to notify the Fort HealthCare Human Resources department within 24 hours of an employee's termination so that all access rights can be terminated.

Access to Fort HealthCare systems will be granted for one (1) year. At the end of one (1) year, the manager must contact the Fort HealthCare Human Resources department to notify them of the employees who will continue to need access to our system and this form must be signed and returned to the Fort HealthCare Privacy Officer.

For the Fort HealthCare Privacy and Security Officer contact (920) 568-6558

Your signature indicates that you have reviewed this statement of confidentiality & security and that you understand your responsibilities and consequences of misuse of access.

Your access to Fort HealthCare protected health information is limited to one (1) year

Print Name_____ **Date**_____

Signature:_____ **Date**:_____

Print Manager Name_____ **Date**_____

Manager Signature:_____ **Date:**_____