SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

1. SECURITY POLICY FOR DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION .......................................................... 2
   1.1. Certification .................................................................................................................................................. 2
   1.2. Chain of trust business associate agreement ......................................................................................... 2
   1.3. Contingency plan ......................................................................................................................................... 4
   1.4. Formal mechanism for processing records ............................................................................................. 6
   1.5. Information access control ...................................................................................................................... 9
   1.6. Internal audit and Security Incident Policy .............................................................................................. 13
   1.7. Personnel security ........................................................................................................................................ 15
   1.8. Security configuration management ....................................................................................................... 15
   1.9. Security management process .................................................................................................................. 16

2. PRIVACY POLICY FOR DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION .......................................................... 17
   2.1. Medical Record ........................................................................................................................................ 17
   2.2. Business Data: .......................................................................................................................................... 17
   2.3. Record Retention: .................................................................................................................................... 18
   2.4. Employment Records ............................................................................................................................ 18
   2.5. Medical Staff Records ........................................................................................................................... 18
   2.6. Electronic Medical Records Privacy Policy ............................................................................................. 18
   2.7. Training ...................................................................................................................................................... 20
   2.8. Press Releases .......................................................................................................................................... 20
   2.9. Disciplinary Measures ............................................................................................................................ 21
   2.10. Review of Medical Records ................................................................................................................ 21

3. DEFINITIONS ..................................................................................................................................................... 22
   3.1. Health Care Operations: ......................................................................................................................... 22
   3.2. Sensitive Data: ......................................................................................................................................... 22
   3.3. Protected Health Information: ................................................................................................................. 22
   3.4. Payment: .................................................................................................................................................. 22
   3.5. Treatment: .............................................................................................................................................. 23
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

The purpose of this policy is to define the philosophy and practice for maintaining reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of patient and employee identifiable health information.

1. Security Policy for Data Integrity, Confidentiality, and Availability of Patient and Employee Identifiable Health Information

1.1. Certification

Each organization is required to evaluate its computer systems or network design to certify that the appropriate security has been implemented. The Information Services Department has a security consultant under contract to perform security and confidentiality reviews of all network configurations and application systems. In addition, the security consultant performs spot security audits of user departments and/or specific application systems. The Information Services Department is audited yearly by an outside auditing firm, as a part of the overall Hospital annual audit.

1.2. Chain of trust business associate agreement

All contracts negotiated and approved by XYZ Hospital which include the transfer of protected information will include the following Business Associate contract terms as stated in the privacy regulations as required by the Health Insurance Portability and Accountability Act.

1.2.1. Require that the Business Associate comply with privacy standards as defined by the Health Care Financing Administration and/or federal statute (implementing Sections 261-264 of the Health Insurance Portability and Accountability Act of 1996) (the “Privacy Rules”).

1.2.2. State that the terms “Business Associate”, “Use”, “Disclosure” and Protected Health Information” have the meanings stated in the Privacy Rules.

1.2.3. Specifically define the Privacy Rules as those standards set forth in a final rule by HCFA with implementation Sections 261 – 264 of HIPAA.

1.2.4. Require that the Business Associate will:
• Not use or further disclose the Protected Health Information received from XYZ Hospital other than as permitted or required by the contract.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

- Not use or further disclose the Protected Health Information in a manner that would violate the requirements of the Privacy Rules.
- Use appropriate safeguards to prevent use of disclosure of the Protected Health Information other than as provided for by the terms of the contract.
- Report to XYZ any use or disclosure of the information not provided for by the contract of which it becomes aware.
- Insure that any subcontractors or agents to whom the Business Associate provides Protected Health Information received from XYZ agree to the same restrictions and conditions that apply to the Business Associate with respect to such information.
- Make available Protected Health Information in accordance with proposed 42 C.F.R. 164.514(a), i.e., access of individuals to Protected Health Information.
- Make the Business Associate’s internal practices, books, and records relating to the use and disclosure of Protected Health Information received from XYZ available to the Secretary of the Department of Health and Human Services for purposes of determining XYZ’s compliance with privacy regulations.
- After termination of the contract, return or destroy all Protected Health Information received from XYZ that the Business Associate still maintains in any form and retain no copies of such information.
- Incorporate any amendments or corrections to Protected Health Information when notified by XYZ in accordance with the Privacy Rules.

1.2.5. Include in the Business Associate agreement language stating that:
- XYZ may terminate the contract if it determines that the Business Associate has violated a material term of the contract required by the Privacy Rules.

1.2.6. Additional contract provisions not required by the Rule:
- Add language which would require the Business Associate to make its practices, books, and records available in the event the Business Associate breaches its agreement with XYZ.
- Require the Business Associate to indemnify XYZ from any loss resulting from an improper use or disclosure of Protected Health Information by the Business Associate. If insurance coverage is available, XYZ should require the Business Associate to obtain insurance against improper uses and
disclosures of Protected Health Information, naming XYZ as an additional insured.

- In the event of a Business Associate’s breach, XYZ should be able to require the Business Associate to retrieve improperly disclosed information, to adopt new practices to assure Protected Health Information is appropriately handled; to subject the Business Associate to audits or require it to submit reports to demonstrate compliance, and to terminate the Business Associate contract if the associate cannot be relied upon to maintain privacy of Protected Health Information.

1.3. Contingency plan

Disaster recovery plans exist to address potential damage of data/information or interruption of normal operations.

1.3.1. The computer operator on duty must monitor the XYZ system to check for hardware/software problems with any of the XYZ Avion processors. Each hour the operator should login to the XYZ system, then take the JOB MONITOR selection and review the processor status screen. In order for the operators to have a point of reference a document is provided for their records. This system monitor record is stored and logged by the XYZ Hospital Information Services Operations Mgr. All problems, resolutions and notes are logged on this form. This document should include calls made to XYZ with times and details of conversations, all calls received from XYZ with times and details of conversations. Total downtime should be documented.

In the event of a processor dropping out of the sequence the FGH Information Services operator should contact XYZ technologies at 909-888-3282 and report the problem.

With any other errors occurring please call 1-909-888-3282 report the problem then call the Information Services Systems person on call. During the outage or process of the correction of the error the Information Services person on call should be kept up-to-date as to the status. If the error occurs after regular hours and the error affects the user population the house supervisor should also be notified. At this time the downtime system should be started in the capacity specified in the DART procedures.
In the event the problem is with PROD3 through PROD9 the urgency is not as great. If the problem is on PROD1 or PROD2 the problem should be reported as an emergency. At this time the operator should start an unscheduled full backup on the processor remaining (PROD1 or PROD2).

With all contacts made to XYZ company the computer operator should record all details and time conversations and notify a supervisor.

1.3.2. The XYZ ULITCARE CLINICAL system is made up of multiple XYZ computer processors. These processors are directly connected through a FDDI (Fiber Distributed Data Interface) ring. The production processors designed to be the ARCHIVE and the MIRROR. These 2 processors have complete control over the entire ring. The processor acting as the Mirror is an identical copy of the ARCHIVE. In the event the ARCHIVE machine fails the MIRROR machine becomes the ARCHIVE and at this point no users are affected with any data lost. After the problem is corrected the failed machine is brought back online as the MIRROR machine. All of the above procedures are handled through the XYZ technical staff.

In the event a problem occurs with Processors PROD3 through PROD9 the problem is corrected and the processor is brought back online, no users are affected and no data is lost.

To assist in disaster recovery the ARCHIVE and the MIRROR machines are housed in separate computer rooms in 2 different buildings. Each controlling processor (PROD1 and PROD2) has 3 applications processors located with them. This allows each computer room with equipment that the hospital could function with. In the event of loss of either site no data should be lost and the affect on response time should be minimal.

FGH will place on order the equipment necessary to replace destroyed hardware requesting delivery over-night or ASAP. When equipment arrives, this hardware will be installed in the stable computer room. XYZ will be contacted to load software onto hardware.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

After the system software has been loaded and the processors are ready for the tape restores to be started the restore procedure will be followed as specified previously in this manual.

At this point data verification should take place. This is done by comparing like reports from the DART system and XYZ reports. After data verification the system will be turned over to the EPICS Clinical Analyst. The EPICS Analyst will verify stabilization of the system and the validity of the data. The Director of Clinical Information Systems (EPICS) will determine at what time the system will be released to users. At this time the appropriate flags will be set to signify a recent downtime and hospital communications will announce over intercom that the system is back in operation.

1.3.3. The guidelines for database restore on the Clinical XYZ system should be a joint decision and effort of the XYZ Hospital Information Services Staff and the XYZ Technologies technical staff. The most current backup tapes should be received from the FGH Information Services Operator on duty and loaded per instructions from the XYZ staff.

XYZ technical staff will perform the restore and verify the data according to their standard procedures. After XYZ staff restores the data FGH will run several reports from the restored database. Then they will run similar reports from the DART system (Data Archive Retrieval Technology) and verify the reports match. The reports from XYZ should have the same patient and medical record information as the DART system. At this time the system will be released to the users.

1.4. Formal mechanism for processing records

1.4.1. The medical record is the property of XYZ Hospital, and is maintained for the benefit of the patient, physician, and hospital. It is the responsibility of the Health Information Management Department and all XYZ Hospital personnel to safeguard the information in the record against loss, tampering, or use by unauthorized persons. Disclosure of patient information requires the patient’s authorization or that of a legal representative except where authorized by legal or regulatory provisions. The patient
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

negley, otto & associates, inc.

form #5 – him policy/procedure

3/17/2005

copyright & patent pending

1.4.2. The Hospital is responsible for safeguarding both the record and its

expects and XYZ Hospital strives to provide confidentiality. The hospital has the obligation to safeguard the records against unauthorized disclosure.

All information is regarded as confidential and made available only to authorized users based on a need-to-know basis. On line computer access is controlled via an Information Systems Access Request. All system security access I.D.'s and passwords will be issued only after execution of a security/confidentiality agreement by the practitioner, staff, or other authorized user of the system. Any breach of confidentiality, misuse of the computer system at XYZ Hospital, and/or unauthorized release of information may result in disciplinary action, including immediate discontinuation of the practitioner's use of the Health Information system, and termination of other appropriate privileges up to and including termination.

Hospital personnel shall be specifically informed of their responsibility to protect patient data, and of the penalty for violation of this trust. Proven violation of the confidentiality of information shall be cause for immediate disciplinary action up to and including termination. This policy shall be made known to all employees at the time of employment. Personnel having access to patient identifiable health information shall be required to abide by all applicable Federal, State, and local laws, rules and regulations. Policies on confidentiality of records shall also conform to the Alcohol and Drug Abuse Confidentiality Regulations published in Part IV of the July 1, 1976 Federal Register as well as HIPAA or related state laws.

Medical records being transported (to or from) Pine Grove Recovery Center will be placed in an attaché case that is locked to ensure confidentiality. Data will be delivered to Pine Grove Recovery center routinely at 10:00 a.m. and 4:00 p.m. in the locked attaché case. Pine Grove will return their data to Health Information Management in a locked attaché case. A STAT pick-up or delivery requires only a telephone call to Pine Grove.

All requests for medical record information on discharged records shall be directed to the Health Information Management Department for processing. It is the policy of XYZ Hospital to require authorization for the release of information. The proper authorization shall be signed by the patient (or guardian, if a minor), giving XYZ Hospital permission to release information. Doubtful consents or authorizations should be referred to Administration or to the Hospital attorney.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

informational content against error, loss, defacing, and tampering; the Hospital also safeguards these records against use by unauthorized individuals.

1.4.3. Particular emphasis is given to protection from damage or loss by fire or water. Specific policies regarding these records are as follows:

1.4.3.1. Security: The Hospital provides security measures that reasonably safeguard both the medical record and its contents (information, whether in hard copy, on film, or in computerized form), against loss, defacement, tampering, fire or water damage, unauthorized disclosure, and use by unauthorized persons.

1.4.3.1.1. XYZ Hospital provides adequate facilities for the storage, processing and handling of medical records for patients admitted to XYZ Hospital and Pine Grove Recovery Center, including suitably locked and secured rooms. All employees of the Health Information Management Department are made aware of their responsibility in maintaining the confidentiality of medical record information, and the disciplinary actions that will be taken for unauthorized disclosure of patient identifiable information.

1.4.3.1.2. To assure the accuracy and protect the integrity of computer-based patient records, health care providers are given an opportunity to review their entries for completeness and accuracy prior to electronically signing them. Once an entry has been signed electronically, the computer system prevents it from being deleted or altered. If the signed entry is converted to another format, the electronic signature applies only to the original format. If errors are later found in the entry or if information must be added, this is done by means of an addendum to the original entry. The new entry is labeled a corrected copy and is signed electronically and the new date and time identified.

1.4.3.1.3. Passwords are carefully controlled to assure that only the authorized practitioner can use a specific electronic signature. Each practitioner must sign a statement that he/she alone will use the electronic signature.

1.4.3.2. Information Management: The development of the Health Information Management Department’s information management processes have taken into consideration the following factors:

1.4.3.2.1. XYZ Hospital’s complexity, enhancement of workflow, and support for clinical decision making. The Health
1.4.3.2.2. The information managed shall have controls to ensure that XYZ Hospital's policy identifies who may access information; what information can be accessed; XYZ Hospital's policy for the individuals confidentiality obligation, release of information and removal of records; and that the information is secure against corruption, damage, or errors.

1.4.3.2.3. XYZ Hospital is responsible for safeguarding records and health information against unauthorized access or tampering.

1.4.3.2.4. Uniformity of data is accomplished through the creation of data definitions, the use of common terminology throughout the Hospital and establishing quality control methods to make sure the data is accurate.

1.4.3.2.5. The key Health Information Management Department personnel who generate, collect, and analyze data remain knowledgeable and competent in information management on an ongoing basis through educational activities.

1.4.3.2.6. The transmission of data shall be timely and accurate. Medical records are accessible 24 hours a day.

1.4.3.2.7. Patient and non-patient data is coordinated; capable of being linked, organized, analyzed and interpreted; and provides longitudinal information in accordance with the policy of XYZ Hospital.

1.4.3.2.8. The data collected shall be gathered timely, efficiently, and accurately. Regular verification of the accuracy and consistency of data shall occur.

1.4.3.2.9. The hard copy portion of the Hospital records will be retired at the time the records have been reproduced, inspected, and found to be in good condition. In accordance with Mississippi Code Annotated Section 41-9-77 (1972, as amended provides that “Any hospital may, in its discretion, cause any hospital record or part thereof to be reproduced on film or in any other acceptable form of medium, as determined by the licensing agency, which shall include, but not be limited to, microfilming, photographing, Photostatting, or storage on optical disks. After the records have been reproduced, the hospital may retire the original documents so reproduced.”)

1.5. Information access control

1.5.1. The confidentiality, security, and integrity of all patient health information is assured through controlled access of data. Access to information must be on a need to know basis. “Need to know” is
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

defined as providing access to protected health information only to those employees who need access to carry out their duties. Access will be governed by security levels established based upon job specific responsibilities or by exception approval through the Data Security Committee. Patients and employees expect and XYZ Hospital strives to provide confidentiality of all records and communications. All information is regarded as confidential and made available only to authorized users who will be determined based on job responsibilities. The facility will ensure the physical protection of records by persons receiving, processing, storing, or handling such records to prevent tampering, theft, destruction, loss, or unauthorized access. Individually identifiable health information that is or has been electronically transmitted or maintained, including such information in any other form will be managed appropriately to assure confidentiality. All individuals engaged in the collection, handling, or dissemination of patient health information, employee information, or medical staff information are specifically informed of their responsibility to protect the data through verbal or written communication at all times and will be informed of the consequences of a breach of confidentiality. All employees are instructed on the implications of HIPAA or related privacy practices.

1.5.2. Secondary health information and computer processed patient/provider treatment information should be protected with the same diligence as the original medical record. On line computer access is controlled via an I.S. System Access Request which must be requested by the user, and approved by their department head. Routine requests for system access associated with an employee’s normal job duties will be handled in conjunction with their orientation process upon being hired. Users are limited to specific menus and functions within menus as designated by the appropriate supervisor. Unusual or non-routine requests will require additional management approval by both the data sponsor and the Data Security Committee. Security of computer reports is maintained by an authorized distribution lists and limitation to specific menus depending on a need to know in order to perform job duties. I.S. reports are distributed through hand delivery, interoffice mail or picked up by the user. Reports and sensitive data are protected from accidental disclosure. I.S. will be notified when distribution lists should be changed. Patient account
numbers, medical record numbers, and physician ID numbers are used to protect confidentiality in reporting processes. The above practices will also be emulated as appropriate for non-patient information of a sensitive nature, i.e. employee or medical staff records.

1.5.3. XYZ Hospital has developed extensive decision support system capabilities that provide the ability of different departments and individuals to analyze data from an operational and clinical perspective. The information is considered Confidential in nature and should only be provided to individuals or groups that meet specific criteria. All requests should be formal and treated as Confidential.

The Administrative Staff, Department Directors, Managers, and Program Coordinators request data on a frequent basis to address issues regarding different projects/programs and initiatives. Timely and accurate information is necessary.

Requests will be made via specific departments who have representatives that have access to information including, but not limited to the following: Quality Management, Health Information Management, Management Systems, Marketing, and Behavioral Health. Requests will be submitted on a FGH Information/Data Request Form. All requests will be reviewed and logged into an Information/Data Request System that resides on the FGH network. This system provides the departments listed above the ability to view and monitor all data requests made. The Information/Data Request System will categorize the type of information needed, i.e. clinical, operational, or financial.

Data requests will be logged in order of priority based on urgency and date needed. Requests will be reviewed to ensure there is no duplication of requests/resources. This policy is to assure that safeguards are in place to provide accurate and timely responses to requests.

1.5.3.1. This policy applies to requests from internal/external customers for data to support FGH sanctioned programs, projects and official queries for information.

1.5.3.2. Electronic mail via the Internet cannot be considered
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

Confidential and secure without approved encryption tools. However, analysis distributed internally can be sent via the FGH email system to the approved data requestor. Information should only be given to the approved data requestor.

Prior to generating reports, files, etc. from a data request, the logging resource will communicate to the DWH/CDR User Group EMAIL-ID Team in order to convey the request and determine duplicity of request or solicit advice on producing the report. The log-in resource will complete the request in accordance with legal authorities, including HIPAA. Concerns will be forwarded to the Data Security Committee.

All written, verbal, or electronic confidential hospital or patient information must be protected. Requests from an internal FGH entity should be handled with discretion on a need-to-know basis. “Need-to-know” is defined as limiting the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. No data shall be supplied to outside/external (Non-FGH) entities without approval of the Data Security Administrator (DSA). Any requests of a questionable nature shall be referred to the Vice President/CIO for final approval or the Security Committee, depending on timing constraints. Such information must be destroyed or disposed of, after a six-year period, in such a way that protects confidentiality of the information. Visit Numbers/Medical Record numbers should not be included in the analysis file unless it is deemed necessary and the proper safeguards are taken. All hardcopy reports should be marked Confidential and only provided to the requestor of the data. All information/data analysis (both diskettes and hardcopy) will be signed for by the receiver to acknowledge that they are accountable for the use/further distribution of information.

Vendors requesting information to assist in analysis for specific projects must have signed Confidentiality Statements and Business Partner Agreements prior to the release of information. If the information releases are not for treatment, payment, or health care operations purposes, then patient authorization is also required for these releases to vendors if
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

there is individually identifiable information contained in the report.

1.6. Internal audit and Security Incident Policy

Each organization is required to maintain an ongoing internal audit process, which is the in-house review of the records of system activity. XYZ Hospital has implemented guidelines for auditing breach of patient and employee confidentiality. These guidelines are developed to address issues that may occur in maintaining confidentiality of patient/employee information in electronic health care information. These guidelines are applicable to all employees of XYZ Hospital and its entities, physicians who practice at XYZ Hospital, contractors, and volunteers. Related policies that support confidentiality are in the Employee Handbook.

1.6.1. Each person accessing information in the patient/employee data base is responsible for their own actions.

1.6.2. No patient or employee information is to be obtained from the system except for the purpose of continuing care, follow up care, quality assessment and improvement, business or legal requirements and/or external regulatory reporting requirements. All other accesses should be based on an approved business partnership with legal agreements including a chain of trust agreement.

1.6.3. All access privileges are assigned on the need-to-know basis.

1.6.4. The following tracking mechanism will be conducted by the Quality Improvement Department to assess the confidentiality of information and ensure compliance with XYZ Hospital policy.

1.6.4.1. Quality Improvement regularly audits access to patient care information.

1.6.4.1.1. Quality Improvement Department will perform a random quarterly audit of patient care/employee information users in designated areas.

1.6.4.1.2. The selection of the area to be audited will primarily be high risk, high volume and/or problem areas. However, all areas will be subject to audit at least annually.

1.6.4.1.3. Quality Improvement Opportunities and audit reports will be reported to Administration through the Vice President of Information Technology and/or the I.T. Security Committee.

1.6.4.1.4. Quality Improvement Opportunities and audit reports will be reported to Administration and the Quality Management Committee.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

1.6.4.1.5. Action will be taken by the appropriate Vice President upon being notified by the Vice President /CIO of Information Technology and/or the I.T. Security Committee.

1.6.4.2. Reports of suspected or confirmed breach of confidentiality (verbal, Quality Control Care Report, auditing, etc.) will be guided by the following:

1.6.4.2.1. Quality Improvement Department will perform an individual audit of the suspected user or record in question.

1.6.4.2.2. Quality Improvement Opportunities and audit reports will be submitted to the President and/or Vice President/CIO who will involve the appropriate Vice President as needed.

1.6.4.2.3. The Risk Manager will notify the insurance company of confirmed breach of confidentiality.

1.6.4.3. The following inquiries will be made whenever there is a suspected or confirmed breach of confidentiality in order to determine the appropriate corrective action:

1.6.4.3.1. Did the employee know they were accessing information they were not authorized for?

1.6.4.3.2. Was there a FGH business “need to know” reason for the access?

1.6.4.3.3. If the reason for access was based on a perceived FGH operational/management need, was the channel of accessing the information inappropriate? (i.e.: Via EPICS System or accessing physical record rather than through the designated channel such as Human Resource Department, employee assistance programs, etc.)

1.6.4.3.4. Once the information was obtained, what was it used for?

1.6.4.3.5. Did the employee use the information for personal gain or other unethical reason?

1.6.4.3.6. Was the information further breached via conveyance, etc.?

1.6.4.3.7. Is the patient or employee aware that there was a confidentiality breach?

1.6.4.3.8. Was there an adverse impact on the patient or employee as a result of the breach? (i.e. clinical outcome, social stigma, gainful employment, etc.).

1.6.5. All circumstances will be taken into consideration when investigating violations of this policy. The Hospital reserves the right to take disciplinary action, up to and including termination or suspension of privileges, for any violations of this policy.
1.7. Personnel security

1.7.1. Administrative responsibility for managing access to patient information is a shared role between the data sponsor(s) and the Data Base Administrator. The Security Officer and Privacy Officer play an integral role in monitoring access. The Data Sponsor is the recognized management resource of a department and will be determined based on where the data is stored. The following are defined as the primary data sponsors for the designated data:

1.7.1.1. Director of Health Information Management (Clinical Patient Chart Information on Discharged Patients)
1.7.1.2. Nurse Manager/Director (Clinical Patient Chart Information on In House or Active Patients)
1.7.1.3. Director of Patient Financial Services (Patient Specific Financial Information)
1.7.1.4. Director of Finance (Employee Payroll Information)
1.7.1.5. Director of Human Resources (Employment Related Information)
1.7.1.6. Director of Physician Support Services (Credentialing Related Information)

1.7.2. Other data sponsorship will be determined on a case-by-case basis by the security committee based on the scope of a request. The ultimate decision on all new requests will be based on a “need-to-know basis”.

1.7.3. The Data Security Committee will be comprised of the above Data Sponsors, Security Officer, Privacy Officer, and chaired by the Data Base Administrator within the I.S. department. The committee will meet periodically in response to non-routine requests which are outside of the scope of job related requests for either reports, files or computerized access levels. Additional management personnel will be invited to participate in the committee’s evaluation of a request based on the type of information being considered. Minutes of all meetings will be maintained by the chair of the committee and available for retrospective audit. Requests for sensitive information will be reviewed by the Vice President/Chief Information Officer subsequent to determination by the committee for final approval.

1.8. Security configuration management

1.8.1. Basic confidentiality & security procedures should be practiced in
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

accordance with the following standards:

1.8.1.1. Passwords and security codes will not be shared with anyone.
1.8.1.2. Work stations will not be left unattended while a user is logged on.
1.8.1.3. Screen saver applications and system time outs will be utilized to minimize risks of unattended viewing/access where appropriate.
1.8.1.4. Passwords for access to the patient’s electronic medical record will be changed periodically.
1.8.1.5. Work stations will be logged off when not in active use.
1.8.1.6. Sensitive information will not be displayed where it can be viewed by unauthorized personnel.
1.8.1.7. Every department will be responsible for providing immediate notification to Information Services in conjunction with Human Resources upon implementing a position change or termination of personnel.
1.8.1.8. Discussion or consultation involving privileged information will be conducted discreetly and individuals not directly involved will not be present without the patient’s or other authorizing approval.
1.8.1.9. There will be periodic changing of remote access passwords for systems support vendors.
1.8.1.10 Access to the EPICS system by non-FGH clinical R.N. personnel must be in conjunction with medical staff sponsorship of access. The I.T. Security Committee or CIO must approve exceptions.

1.9. Security management process

1.9.1. The confidentiality, security and integrity of patient and employee information are a legal and ethical matter. Management of this access must be conducted in a formalized manner in compliance with all traditional codes of conduct associated with data security. In this regard, all system (computerized) security access passwords will be issued only after execution of a security/confidentiality agreement by either the employee or non-employee entity (physician/consultant).

NOTE: This portion of the policy was instituted in conjunction with the EPICS project in 1997. Prior to that time the prevailing practice was limited to securing a written acknowledgment statement from
the employee during orientation that they have received the handbook which covered confidentiality guidelines.

2. Privacy Policy for Data Integrity, Confidentiality, and Availability of Patient and Employee Identifiable Health Information

2.1. Medical Record

2.1.1. The medical record is the property of the facility and is maintained to serve the patient, health provider and the facility in accordance with legal, accrediting and regulatory requirements. Any data collection or conveyance on a patient whether by interview, observation, review of documents or systems, will be conducted in a manner that provides maximum privacy and protects the information from unauthorized access. The storage and handling of this information will be afforded maximum privacy protection as well. The types and amount of patient information gathered for the medical record is limited to that information needed for patient treatment. All medical records are housed in physically secure areas.

2.1.2. Patient information released to authorized individuals/agencies is strictly limited to that information required fulfilling the purpose stated on the authorization. Every reasonable attempt is made to verify the authenticity of the signature on any authorization. A properly completed and signed authorization to release patient information will be required. Patient authorization generally will not be required for uses or disclosures of protected health information for treatment, payment, and health care operations purposes, or in accordance with other legal and regulatory exceptions found in HIPAA and/or other federal and state authorities.

2.2. Business Data:

All hard copy billing records containing discharge diagnoses or coded data are maintained securely by the Business Services Department with the same principals as noted above for management of the patient's medical record.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

2.3. Record Retention:

Primary and secondary health records are retained according to approved institutional retention policies and per legal, accrediting or regulatory requirements specific to the data type and content. (Refer to Health Information Management policy, Confidentiality and Security of Medical Records, section 2,B2,i.)

2.4. Employment Records

All personnel records on all employees are maintained in the Human Resources Department in lockable file cabinets. A separate medical file is maintained on each employee in separate lockable file cabinets in the Epidemiology Department. These records are highly confidential and access is given only on a need-to-know basis authorized by the Director of Human Resources. The employee personnel file is the property of XYZ Hospital.

Terminated employees’ personnel and health records are maintained in the Human Resources Department for one year after terminating then are sent to the Service Center to be microfilmed. The records are maintained on microfilm indefinitely.

2.5. Medical Staff Records

Recognizing the importance of preserving the confidentiality of all Medical Staff records, the staff designated by Administration shall handle in strictest confidence all information obtained in connection with fulfilling the responsibilities of the Medical Staff Office. This confidentiality extends to all practitioner’s professional and credentials files, Medical Staff minutes, and all Quality Assessment activities, as well as to the discussions and deliberations which take place within the confines of the Medical Staff Department/Committee meetings. All professional and credentials files (both current and inactive) shall be maintained in the Medical Staff Coordinator’s office in locked file cabinets.

2.6. Electronic Medical Records Privacy Policy

2.6.1. Electronic medical records are strictly confidential under state law and may be accessed or released only by consent of the patient or the patient’s authorized legal representative, or by court order, or
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

pursuant to a state or federal statutory exception if access is for purposes unrelated to patient care or hospital operations.

2.6.2. Physicians are authorized to access the medical records of hospital patients whom they are presently treating or as reasonably necessary to provide follow-up care, including review to determine medical protocol of prior patients. Every access shall be by physician access code and password and shall be permanently recorded for audit purposes. Physicians may not access the medical records (electronic or hard copy) of non-patients (including the medical records of relatives or employees) for any reason without a signed release, which shall become part of the permanent record. Physician office access shall restrict the ability to print an original hard copy of EPICS unless otherwise approved by the I.T. Security Committee or CIO.

2.6.3. Request to access a patient medical record by a physician or person acting as the physician’s agent (i.e., employed nurse, office Coder, office manager), constitutes a legal representation by the physician and the agent is legally entitled to access the record contingent upon a proper valid patient consent being obtained plus a confidentiality agreement executed for business partners.

2.6.4. A grant of access or release of a written medical record does not authorize any re-release or further dissemination of the record to any other person unless authorized in writing by the patient.

2.6.5. Medical Coders, medical office nurses, and allied health personnel acting under the authority of a physician may access electronic patient medical records as reasonable necessary for the provision of medical care for the period during which the employing physician has the right to access the particular record, consistent with the signed consent or legal exception. Exceptions must be approved in advance by the I.T. Security Committee or CIO.

2.6.6. Electronic or hard copy access for purposes other than patient care will be arranged as appropriate via the Data Security Committee. Such access will be limited to information needed to perform one’s job and not based on a full access privilege to the entire on-line or hard copy chart. All access will be on a need-to-know basis and limited to information required to perform job related duties. Access shall be by unique patient identifier, and personal code. All such accesses shall be permanently recorded.

2.6.7. Consents to release shall be maintained as part of the medical record. Records of persons who have accessed a medical record shall be maintained as the property of XYZ Hospital and shall not be part of the medical record. Release of access information shall be at
the discretion of XYZ Hospital unless otherwise required under state or federal requirements.

2.6.8. Duly established hospital medical review or quality assessment committees may access patient medical records as reasonable necessary to evaluate or review the diagnosis or treatment or the performance or rendition of medical or hospital services, to evaluate or improve the quality of health care rendered, to determine the health care services rendered were professionally indicated or were performed in compliance with the applicable standard of care, and to determine that the cost of health care rendered was considered reasonable under the circumstances. All said access is protected under state laws not subject to discoverability.

2.6.9. An order in the medical record for a consult shall constitute a legal representation by the ordering physician that the patient has consented to the consult. The consulting physician shall have access to the patient’s medical records to the extent reasonably necessary for the purposes of the consult.

2.6.10. Emergency Department physicians and support personnel treating patients under conditions of implied consent or where obtaining written consent is not practical, and hospital staff physicians treating patients in emergency situations, shall be allowed access to the patient’s medical records as reasonably necessary to provide treatment.

2.6.11. Allied health personnel performing procedures or tests ordered by a physician shall have access to the patient’s medical records as reasonably necessary in the furtherance of treatment or testing.

2.7. Training

All employees are provided security training regarding the vulnerabilities of the health information to ensure the protection of that information. Employees are trained to understand their privacy and security responsibilities and make security a part of their day-to-day activities. Privacy and security of health information is provided as a part of general orientation with periodic user reminders. Employees are educated regarding confidentiality policies and password management.

2.8. Press Releases

Information to newspaper, radio or television station representatives, the press or any other news media representative, shall be given only by authorized personnel, in accordance with approved news media policy.
2.9. Disciplinary Measures

An employee found to be in violation of this policy, whether inadvertent or intentional, is subject to disciplinary action, which may include separation. Non-employees may be subject to loss of computerized access or loss of other privileges granted by the hospital.

2.10. Review of Medical Records

A patient may request review of their medical records. The patient will be informed that the record will be available in the Health Information Management Department on a specified day at a given time convenient to both the patient and the Health Information Management Department. A designated hospital employee will be present during the review. The hospital employee will not offer an opinion or judgment of the patient’s treatment. Before review of HIV/AIDS, psychiatric or substance abuse records, the attending physician will be notified to express permission for the patient to review the record. If the attending physician states that access to HIV/AIDS records, psychiatric records, or substance abuse records will in some way endanger the life or physical safety of the individual, then access will be denied.

If the individual requests the Hospital to amend or correct his medical record, the Patient Advocate/Risk Manager will be contacted and risk management procedures will be initiated. The Patient Advocate/Risk Manager will follow the procedures and standards for the amendment and correction of patient health information at the patient’s request as outlined in HIPAA regulation (164.516).
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

3. Definitions

3.1. Health Care Operations:

The activities considered to be compatible with and directly related to treatment, payment, or other core hospital operational process such as quality assurance, etc., and therefore would not require authorization from the individual for use or disclosure of protected health information.

3.2. Sensitive Data:

Sensitive data includes patient information, payroll and personnel data, physician data, and patient accounting records, as well as medical staff records. Any reports, records, or systems containing sensitive data will be managed appropriately to assure confidentiality.

3.3. Protected Health Information:

Individually identifiable health information that is or has been electronically transmitted or maintained, including such information in any other form.

3.4. Payment:

Activities undertaken by a health plan (or by a business partner on behalf of a health plan) to determine its responsibilities for coverage under the health plan policy or contract including the actual payment under the policy or contract, or by a health care provider (or by a business partner on behalf of a provider) to obtain reimbursement for the provision of health care including:

- Determinations of coverage, improving payment methodologies, or coverage policies, or adjudication or subrogation of claims;
- Risk adjusting payments based on enrollee health status and demographic characteristics;
- Billing, claims management, medical review, medical data processing;
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

- Review of health care services with respect to medical necessity, coverage under a health plan policy or contract, appropriateness of care, or justification of charges; and,
- Utilization review activities, including precertification and preauthorization of services.

3.5. Treatment:

The provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers, or the referral of an individual from one provider to another, or coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual.
SECTION: HIPAA POLICY REGARDING PRIVACY AND SECURITY OF PATIENT AND EMPLOYEE IDENTIFIABLE HEALTH INFORMATION

APPROVED BY EXECUTIVE COMMITTEE: 01/01
APPROVED BY BOARD OF TRUSTEES: 01/01