UNIVERSITY HOSPITAL
Newark, New Jersey

UNIVERSITY HOSPITAL POLICY

SUBJECT:	COMPLIANCE AND PRIVACY	**TITLE:**	STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION		
CODING:	831-200-963	**ADOPTED:**	July 1, 2013	**AMENDED/ REVIEWED:**	

I. PURPOSE

To ensure University Hospital's (UH) compliance with the Health Insurance Portability and Accountability Act (HIPAA) and to establish standards for Privacy of Individually Identifiable Health Information (IIHI).

II. ACCOUNTABILITY

Under the direction of the President/CEO, General Counsel and the Chief Compliance and Privacy Officer, all Department Heads shall ensure compliance with this policy.

III. APPLICABILITY

This policy shall apply to health information that is generated during the provision of health care services to patients in any of UH's departments.

IV. REFERENCES

A. 45 CFR, 160, Code of Federal Regulations, Title 45, Part 160, Subpart C, General Administrative Requirements, Compliance and Enforcement

B. 45 CFR, 164.514(e), Code of Federal Regulations, Title 45, Part 164, Subpart E, Security and Privacy, Privacy of Individually Identifiable Health Information

C. 45 CFR, 164.530, Code of Federal Regulation, Security and Privacy, Administrative Requirements

D. Accounting of Disclosures of Health Information — Policy #831-200-957

E. Disclosures of Personally Identifiable Health Information to Business Associates — Policy #831-200-958

F. Protected Health Information Breach Notification Policy — Policy #831-200-847

V. POLICY

UH will implement and maintain a Privacy Program to assure compliance with state and federal laws and UH policies protecting the confidentiality of individually identifiable health information of its patients and/or Human Subjects in research. The Privacy Program will complement the Information Security policies of UH.

All UH employees, and individuals working on behalf of UH in any capacity (including Board members, medical staff, business associates, independent contractors, and volunteers) will conduct themselves and their activities in a manner so as to protect the confidentiality of patients' individually identifiable health information as required by state and federal laws and regulations and in conformance with UH policies.

A. Requirements:

1. UH's Privacy Program will consist of the following elements:

a. UH Privacy

i. The Chief Compliance and Privacy Officer, will oversee the development, implementation and maintenance of UH's Privacy Program. The Privacy Program will complement the Information Security policies of UH.

ii. The Institutional Review Board (IRB) will assure that informed consents include appropriate authorizations for disclosure or that authorization has been appropriately waived for research subjects.

b. Director of Medical Records

i. The President/CEO or designee, will appoint a Director of Medical Records.

ii. It will be the responsibility of the Custodian of Medical Records to assure that processes are in place to implement and monitor compliance with the elements detailed in Section V.A.1.c., below.

c. The Chief Compliance and Privacy Officer, with the assistance of the Director of Medical Records, will direct that the following elements are developed, implemented and maintained in conformance with state and federal requirements, and are reflected in UH policies and procedures accordingly:

i. Providing notice to patients of UH's privacy practices for Protected Health Information (PHI);

ii. Protecting the confidentiality of uses and disclosures of PHI, including requiring appropriate authorizations, and/or an opportunity to agree or object when mandated by law for uses and disclosures of PHI;

iii. Implementing appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of PHI from unauthorized use or disclosure in collaboration with Chief Security Information Officer;

iv. Assuring that a written process is in place that allows individuals to restrict uses and disclosures of their health information. UH, however, is not required to agree to such requests.

v. Assuring that patients can receive communications of their health information by alternate means or alternate locations, if requested.

vi. Implementing a written process for maintaining and providing an accounting of UH uses and disclosures of PHI to requesting individuals to whom the information pertains;

vii. Assuring that a written process is in place that allows individuals to access, inspect and/or obtain a copy their health information;

viii. Assuring that a process is in place that allows individuals to request to amend their health information UH however, may deny requests under specified circumstances;

ix. The Chief Compliance and Privacy Officer will be the contact person for individuals seeking further information or clarification to privacy and patient rights requirements covered under the notice. He/she will be to receive complaints concerning UH and its compliance with health information privacy and patient rights requirements.

d. All existing or new policies and procedures addressing any of the items in section V.A.1.c. above, or that concern the use or disclosure of PHI, and all consent/authorization forms for the disclosure of PHI, must be presented to the UH Chief Compliance and Privacy Officer for review to assure compliance with UH- policies, as well as state and federal requirements.

e. The Chief Compliance and Privacy Officer will communicate periodically, with all Department Heads on the status of all policies and procedures concerning PHI, the Privacy Program, including its implementation, training, any recommended changes or amendments, complaints or issues of non-compliance.

f. UH will promptly revise its policies and procedures related to the Privacy Program as discussed above as necessary and appropriate to comply with changes in law and or regulation. All policies and procedures will be reviewed periodically by the Chief Compliance and Privacy Officer, to assure compliance with the laws and regulations as well as for operational effectiveness. If the changes in the law and regulation also materially affect privacy practices stated in UH's notice to patients regarding privacy practices, the notice must also be revised in a timely manner.

g. All notices to patients concerning UH's privacy practices must state that UH reserves the right to make changes in its privacy practices at any time.

2. Education and Training

a. The Chief Compliance and Privacy Officer will develop training to refresh the UH workforce regarding the Privacy Program, policies and procedures and the regulatory requirements, as appropriate.

b. The Chief Compliance and Privacy Officer will take necessary efforts to offer new members of the workforce privacy training within 30 days of hire.

c. The Chief Compliance and Privacy Officer will coordinate additional training of the workforce whose functions are affected by a material change in the policies and procedures within a reasonable period of time after the change becomes effective.

d. Training provided will be appropriately documented and the documentation will be maintained by the Office of the Chief Compliance and Privacy Officer for a minimum of six (6) years or as specified by the New Jersey State Retention Schedule.

3. Non-retaliation for exercise of Patient Rights

UH will maintain in the Code of Conduct and other applicable policies and procedures that state intimidating, threatening, coercing, discriminating or taking other retaliatory action against the following is prohibited as outlined in the Notice of UH Privacy Practices for Protected Health Information:

a. Patients for exercising any right established by HIPAA privacy guidelines, 45 CFR 164, subpart E;

b. Individuals and others for filing a complaint with the Secretary of Health and Human Services under 45 CFR 160, subpart C;

c. Individuals and others for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

d. Individuals or others for opposing any act or practice made unlawful by 45 CFR 164, subpart E, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of 45 CFR 164, subpart E.

B. Responsibilities:

1. The Chief Compliance and Privacy Officer shall be responsible for communicating and enforcing the above policy as it relates to all UH employees.

2. The Chief Compliance and Privacy Officer and President/CEO or shall be responsible for communicating and enforcing the above policy as it relates to persons involved in patient and human subject research contact.

3. The Supply Chain Management Executive or his or her designee shall be responsible for communicating and enforcing the above policy as it relates to vendors, independent contractors, business associates, etc.

4. UH may not require individuals to waive their rights to file a complaint with the Secretary of Health and Human Services or any other right under CFR 164, subpart E, including 164.500 through 164.530, as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.

5. Monitoring and Evaluation

a. The Compliance Committee is the governing body for the evaluation and monitoring of the Privacy Program and will review compliance issues as appropriate.

b. The IRBs and the Chief Compliance and Privacy Officer will monitor compliance with requirements for research related disclosures.

c. The Chief Compliance and Privacy Officer will periodically request external or internal audits to be conducted to ensure compliance with this policy.

d. The Chief Compliance and Privacy Officer, is responsible for investigating and reporting on allegations of non-compliance with UH privacy policies.

6. Sanctions for Non-Compliance

a. UH will apply appropriate sanctions, against any member of the workforce who fails to comply with UH's privacy policies and procedures.

b. The President/CEO or designee, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently.

c. UH will document all sanctions that are applied.

7. Documentation

Documentation evidencing implementation of the Privacy program, including complaints, training, sanctions, auditing, etc., will be maintained for a minimum of six (6) years or the time period specified by the New Jersey State Retention Schedule, whichever is longer.

APPROVALS BY:	**NAME:**	**SIGNATURE:**
President/CEO	James R. Gonzalez	
Interim Chief Compliance and Audit Officer	John W. Ras	
Chief Human Resources Officer	Gerard Garcia	