

**NORTHEAST HOSPITAL CORPORATION  
HUMAN RESOURCES POLICIES AND PROCEDURES**

**Policy #:** 5.13  
**Subject:** Confidentiality of Patient Information  
**Applies to:** All Hospital Colleagues

**I. Statement of Purpose**

It is Northeast Hospital Corporations (NHC) intent to establish policies on the confidentiality of patient-related information and to provide guidelines for the security and appropriately controlled release of such information.

Northeast Hospital Corporation supports a patient's right to confidentiality (that is, the right to keep information about himself/herself inaccessible to others) and accepts responsibility to keep secure and confidential the information collected about our patients during their encounters with us. Northeast Hospital Corporations also understands that releasing parts or all of that information is appropriate under certain circumstances, such as providing for continuity of care, participating in approved research and educational activities, complying with the law and assuring reimbursement for services provided, and that such releases provide benefit to the patient or to society.

**II. Scope and Definition of Terms**

This policy statement applies to all personnel of NHC, as well as anyone participating in medical educational programs within its organizations.

This policy statement applies to all patient-related information: any item containing information about a patient that reasonably could directly or indirectly identify the patient, whether in electronic or hard copy format, whether original or copied, any electronic data base, whether free-standing or networked, any medical records, whether maintained by the Health Information Management Department or any other department, section, or provider. This policy statement also covers items regardless of storage medium or location. Also covered are operating schedules, registration forms, financial documents, patient conference notes, provider's personal notes, photographs or videos, information in registries, room assignments, radiology films, cine films, computer-generated microfilm, electronic mail correspondence, and all other media now known or later invented.

Types of release covered by this policy statement include (but are not limited to) written, verbal, telephonic, or electronic, transmitted intentionally or unintentionally, in public or in private, inside or outside the walls of our organizations. Also included is information released to regional health data networks, insurance companies, managed care providers, medical data banks, and other data repositories.

This document provides philosophy and direction for decision making and procedure development throughout our organization. Health Information Management Departments will develop implementation policies to provide mechanisms for appropriate protection and release of information. These implementation policies will define the circumstances under which an unauthorized access to or release of patient-related information will

constitute a breach of confidentiality. At a minimum, any disclosure of personal computer password (s) which risks unauthorized access to confidential patient information will be construed as a breach of confidentiality. If you have any questions about this policy statement or release of any patient-related information, contact the Health Information Management Department.

### **III. General Principles**

- a. Patients own their personal healthcare information, and with the exception of mental health notes, have a reasonable right to access their own healthcare information and to correct or comment on information contained in the medical record. Northeast Hospital Corporations owns the medium on which the information is kept: paper records, videos, photographs, electronic storage media, etc. As patients must be informed of their rights and obligations regarding their own information whenever possible.
- b. Whenever possible, we will release patient information only with patient authorization, but we will proceed without consent for uses and disclosures for treatment, payment, health care operations, or when required by law.
- c. Individual NHC employees are accountable to read, know, and understand this policy statement, to adhere to approved specific policies and procedure for confidentiality of patient-related information, and to exercise care and good judgment in accessing, using, or disclosing such information.
- d. In all circumstances, only the minimum necessary amount of information will be released to those individuals or entities with a need or right to access such information. This “minimum necessary” required would not apply to information used or disclosed for treatment, authorized by the patient, or required by law.

### **IV. Statement on Patient Authorization**

- a. Federal law permits us to use or disclose patient information without patient consent for treatment, payment, or health care operations. Permission for access to or release of a patient’s information may be granted only by a competent patient, the parent or guardian of a minor child, the patient's attorney, or by a court order.

### **V. Statements on Specific Situations**

#### **a. Treatment**

Medical information shared for the patient's ongoing care is assumed to be in the patient's best interest. To facilitate a patient's treatment, disclosure of information may occur among providers. Patient information will be released to non – NHC healthcare providers without written consent when appropriate to do so, such as, in a medical emergency and when providing test results and/or reports to referring physicians. We direct the patient to the Notice of Privacy Rights which sets forth their rights under the Health Insurance Portability and Accountability Act of 1996.

#### **b. Payment**

When possible, as patients must be informed about the following:

- that their medical records data may be released to primary and secondary payers;
- that payers maintain claims databases on their clients;
- that payers may contribute patient data to the Medical Information Bureau;
- that third-party reviewers may request and receive patient information over the telephone for utilization review purposes, or may review the medical record on the premises.

c. Health Care Operation

Patient Information is essential to many corporate functions. These functions include administrative activities such as surveys by accrediting bodies and evaluations of clinical outcomes. We recommend that non-patient specific and non-diagnostic information be used whenever possible. In all cases, we recommend that only the minimal amount of information be accessed and only by those with a need to know the information.

Quality assurance functions are used to evaluate the adequacy and appropriateness of care rendered. Documentation generated during the process is confidential and is protected by state statutes from disclosure. When disseminating information from these reviews at section or department meetings, patient specific identifiers are to be deleted whenever possible.

- d. Release of Information to News Media. Requests from the news media for patient information should be referred to the public affairs department in Burlington, regardless of the site.
- e. Release Under Law or State Regulation. In accordance with state law. Certain diagnoses and circumstances require disclosure without patient consent. Each regional Health Information Management Department policy will explicitly describe these situations with references to the applicable statutes and regulations.
- f. Release and Use of Information for Medical Research. The release and use of information for medical research must be approved by the appropriate Institutional Review Board (IRB). Articles, papers, copies of records, x-rays, photographs and/or other artifacts of research must not divulge patient identity without authorization of the patient or his/her legal representative, unless de-identified or otherwise approved by the IRB.
- g. Release of Sensitive Information. State and Federal laws contain special confidentiality provisions regarding sensitive diagnosis. These include, but are not limited to, HIV test results, mental health records and records of patients who have been diagnosed or treated for drug or alcohol abuse. These laws require special authorizations or court orders for release of information. Each regional Medical Records Department policy will describe how to handle these situations.
- h. Release and Use of Information for Education. We recognize the necessity of sharing patient-related information to fulfill our educational mission. This may be consistent with applicable law and standards of ethical conduct use or disclose PHI (patient health information), if NHC, in good faith believes the use or disclosure is valid and approved by appropriate entities (HIM, IRB).
- i. Release of Information in Crisis Situations
1. Information may be released when deemed necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is reasonably able to prevent or lessen the threat to others, including the target of the threat; or

2. is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that NHC reasonably believes may have caused serious physical harm to the victim; or where it appears from all the circumstances that the patient has escaped from a correctional institution or from lawful custody.
- j. **Release of Information of Patients who are Armed Forces Personnel**  
NHC may use and disclose information of patients who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the *Federal Register* appropriate military command authorities and the purposes for which the information may be used or disclosed. This rule applies to disclosure of information of foreign military personnel to their appropriate foreign military authority.
  - k. **Release of Information to Federal Officials**  
NHC may disclose information to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security act. Furthermore, NHC may disclose information to authorized federal officials for the provision of protective services to the President or other authorized persons or to a foreign head of state or for the conduct of federal investigations.
  - l. **Release of Information During a Disaster**  
NHC may use or disclose information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

## **VI. Computerized Patient Records**

We support the concept of the computerized patient record and believe that it enhances the effectiveness and efficiency of medical care.

A computerized patient record should be structured so that patient records created and stored on the system can also be admitted as evidence in court. This means, in general, that the computerized patient record must:

- be kept during the ordinary course of business
- be created contemporaneously with the event being documented
- include documentation dates, times, and the identity of every individual making or modifying any entry (maintaining the original plus the modified entry)
- be protected by publicized and enforced rules against unauthorized access and disclosure of patient-related information.

Information on the computer or in hard copy will be considered part of the medical record, so that by definition the NHC Clinic hospital record contains information in both paper and electronic formats. All confidentiality rules and security precautions set up for the paper record also apply to the computerized patient record.

## **VII. Regional Health Data Networks**

We support the development of regional health data networks if those organizations promote public health and provided that they enforce explicit policies for the protection of data against unauthorized access or release.

## **VIII. Communications by Electronic Mail, Cellular Telephone, Modem or Fax**

Our intention is not to discourage the appropriate use of electronic media for patient care, but to draw attention to the need to manage the different security issues arising from the use of new technologies.

Technologies such as electronic mail ("e-mail") and cellular or cordless telephones which are used to communicate patient information between providers or between providers and patients are less secure than the computerized patient record because of the nature of the technology or the place in which they are used.

- Cellular and cordless telephones communicate by broadcasting radio signals, which can be overheard through various electronic means, such as scanners, without the user's knowledge.
- E-mail messages can be inadvertently sent to the wrong party, forwarded by the recipient, or accessed through computers left logged-on and unattended. In addition, "trash" messages remain retrievable by third parties under certain circumstances. It is possible for e-mail messages to be forwarded or printed without the sender's or recipient's knowledge or permission. Furthermore, e-mail messages may be used as evidence in court.
- Access by modem makes the information available in remote environments. Screens must not be left logged-on in unsecured areas. Passwords must be **kept** secure. When in the company of others, in an airport or in private homes for example, care must be taken to protect the information from unsecured viewing.
- Facsimile (fax) transmissions can be inadvertently sent to the wrong party and or left unattended for long periods at unsecured locations.

Therefore, when these technologies are used, extra precautions must be taken.

## **IX. Review and Amendment of this Document and the Implementation Policies**

Specific policies will be adopted that implement this policy statement. Because of the rapidly changing health care environment and technologies, we anticipate that this policy statement as well as the implementation policies can represent only the current thinking and law at any point in time and, therefore, will need periodic reviewing and updating. This review will be coordinated by the appropriate governing bodies or their designees.

DATE ISSUED: January 2011  
DATE REVIEWED: May 2017  
DATE REVISED: May 2017

**BEVERLY HOSPITAL AND ADDISON GILBERT HOSPITAL**  
**CONFIDENTIALITY STATEMENT**

Beverly and Addison Gilbert Hospitals (BH/AGH) is committed to a patient's quality care, safety, dignity and well-being. As part of this, Beverly and Addison Gilbert Hospital expect and require its colleagues to keep patient information confidential and secure. Beverly and Addison Gilbert Hospitals also expects its colleagues to keep confidential any and all confidential financial data and other non-public proprietary information (as defined below) not otherwise available to persons or entities outside of Beverly and Addison Gilbert Hospitals.

**Confidentiality of Patient Information**

I hereby acknowledge and agree that I have received and read the **Confidentiality of Patient Information** and understand that, as defined in this policy, I must hold in strict confidence all information relating to BH/AGH patients (including but not limited to the confidential patient information of BH/AGH colleagues). I understand that I have a legal and ethical responsibility to prevent access to and disclosure of confidential patient information without proper authorization or for unauthorized purposes.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_

**Confidentiality of Non-Public Business Information**

I hereby acknowledge and agree that, to the extent I have access to confidential financial data and other non-public proprietary business information (as defined below), I must maintain the confidentiality of such information and prevent the access and disclosure of such information without proper authorization or for unauthorized purposes. Confidential financial data and other non-public proprietary business information includes, but is not limited to, information regarding BH/AGH financial goals and performance, budgetary information, and non-public information regarding BH/AGH business partners, vendors and customers/patients.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_

*\*Nothing in this Confidentiality Statement is intended to restrict a colleague's right to engage in protected activities with other colleagues, including discussing wages, hours, and working conditions with fellow colleagues or others.*

***Check appropriate category:***

Colleague \_\_\_\_\_ Student \_\_\_\_\_ Volunteer \_\_\_\_\_ Contract Personnel (non-colleague) \_\_\_\_\_

DATE ISSUE: November 2016

DATE REVISED: May 2017

# Document Information

## Document Title

5.13 Confidentiality of Patient Information

## Document Description

N/A

## Approval Information

**Approved On:** 05/04/2017

**Approved By:** Human Resources [Gail Tsoukalas (gtsoukal)]

**Approval Expires:** 07/03/2020

**Approval Type:** Process

**Document Location:** / Human Resources / Section V: Work Rules & Schedules

**Keywords:** N/A

**Printed By:** Guest User

**Standard References:** N/A

**Note:** The most recent version of this policy is online.