



## Confidentiality of Patient, Personnel, and Hospital Information

### Policy

- Employees with access to confidential patient, employee, and/or business information may only access it on a "need to know" basis.
- Examples of confidential information include but are not limited to:
  - Patient medical, social, financial and demographic information.
  - Employment information, occupational health records, and employee personal information.
  - Hospital business information, such as financial and payor information, strategic planning, fundraising and reporting information and internal memoranda.
  - Research information, including information describing or relating to inventions and discoveries.
  - Information concerning outside companies, with which the hospital does business, including information the Hospital is contractually obligated to keep confidential.
- Employees must:
  - Keep patient, personnel, data/access codes, and other proprietary and sensitive information confidential.
  - Access or use confidential information only as required to perform their job.
  - Provide the minimum information necessary when responding to information requests.
  - Not discuss this information with others unless it is administratively or clinically necessary and you have been authorized to do so.
  - Not disclose, release, or distribute confidential information unless authorized to do so.
  - Not use any electronic media to copy and/or transmit confidential information unless specifically authorized to do so.

### Standards

#### Responding to Requests for Information

When responding to requests for information:

- **Refer requests from a legal entity**, such as a judge, lawyer, or social service officer, to the Office of General Counsel. Such requests may include subpoenas or court orders.
- **Refer requests from the media** to Marketing and Communications.

## Patient Information

All patient information is considered confidential and sensitive. This includes patient demographic, registration, financial, and clinical information. Hospital policies and procedures, and state and federal statutes protect the internal use and external disclosure of patient information. In general, releases and disclosures of patient information via any media require a completed and [signed written authorization](#) by the patient/family or guardian.

When responding to requests for patient information:

- Refer questions about releasing information and appropriate authorizations to the Medical Records Department or Privacy Officer.
- Refer requests for patient information that do not seem appropriate to your supervisor or chief.
- Refer requests for a copy of any portion of a patient's Hospital medical record to the Medical Records Department. They will obtain the necessary authorization prior to the release of the medical record. Do not release any Hospital medical record information without approval from the Medical Records Department

## Personnel and Hospital Information

Never access personnel and Hospital information for personal reasons or private gain. Examples of this information include:

- Personnel profile information such as demographics, performance review, and salary information.
- Hospital information such as financial data, contract negotiations, business strategies and practices, research discoveries.

## Electronic Information Access

The Information Security Manual: [Acceptable Use of Computer and Network Resources](#) describe the employee's obligation to protect information that is stored or accessed electronically.

Computer and telecommunication accounts require passwords for access. The following are forbidden under any circumstances.

- Disclosing your computer access password(s) to another employee.

Refer an employee requesting another employee's password or password to the ISD [Help Desk](#).

- Disclosing your telephone, voicemail, or beeper authorization code to another employee.

Refer an employee requesting another employee's authorization code to the [Telecommunications Comrequest](#).

## Misconduct

Unauthorized disclosure of confidential patient, employee or Hospital information is serious misconduct. Such action by a person affiliated with the Hospital may necessitate immediate

investigation, investigatory suspension, discipline, or dismissal. See Human Resources Manual: [Discipline, Discharge, and Standards of Conduct Discipline](#) for further information about standards of conduct.

## Related Content

- Compliance Manual: [Confidentiality of Patient Information](#)
- Human Resources Manual: [Discipline, Discharge, and Standards of Conduct Discipline](#)
- Information Security Manual: [Acceptable Use of Computer and Network Resources](#)
- Patient Health Information Manual: [HIPAA Content](#)

## Document Attributes

<b>Title</b>	Confidentiality of Patient, Personnel, and Hospital Information		
<b>Author</b>	Gerald Ellis Director of Human Resources Information Services	<b>Date of Origin</b>	06/98,
<b>Reviewed/ Revised by</b>	Carolyn T. Stetson Director, Employee Relations Julie Dardano Director, Human Resources Compliance and Operations	<b>Dates Reviewed/ Revised</b>	10/00; 05/07/03 09/15/11
<b>Copyright</b>	© Boston Children's Hospital, 2025	<b>Last Modified</b>	07/31/15
<b>Approved</b>	Signature on File  Inez Stewart Vice President for Human Resources		