

Confidentiality of Student, Medical, and Personnel Records

HR



About This Policy

Effective Date:

Last Updated:

03-01-2003

Responsible University Office:

University Human Resources

Responsible University Administrator:

Vice President and Chief Financial Officer

Policy Contact:

University Human Resources

policy@iu.edu

Related Information

- * [Accessing Human Resources and Departmental Personnel Files](#)
- * [Management of Human Resource Records](#)
- * [Family Educational Rights and Privacy Act \(FERPA\)](#)
- * [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#)

Scope

Policy Statement

Procedure

Definitions

Sanctions

[Back to top](#) ↗

Scope

This policy applies to all Staff and Temporary employees at IU.

[Back to top](#) ↗

Policy Statement

1. Employees cannot use confidential information for personal reasons. For example, employees cannot use someone's address to seek political contributions or to present information about a sales campaign.
2. A federal law, Family Educational Rights and Privacy Act (FERPA), classifies most student record information as private. This information cannot be released to third parties (including parents) without signed consent from the student.
3. Personal health information created or used by employee-sponsored health plans has special protection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
4. Upon request, a university employee or his/her designated representative will have timely access to all information found in the employee's own personnel and medical files.
5. Employees are to follow any additional policies and procedures specific to their position and any work applications used in the position.

[Back to top](#) ↗

Procedure

1. Employees who receive requests for confidential information must follow the specific policy that applies to that request. For policy clarification and details, employees are to consult departmental procedures and an expert in the respective area of information.
2. Proper handling of confidential information includes not releasing such information to anyone unless that person has authorization.

Employee Access to His/Her Own Files

1. If the designated representative of an employee requests access to the employee's personnel and medical files, the representative must present a written authorization signed by the employee that clearly and specifically describes the information the representative may inspect or copy.
2. At no time during the access of an employee's file will the file be out of the direct supervision of the university recordkeeper.

[Back to top ↗](#)

Definitions

Confidential information refers to nonpublic information about students, faculty, and employees. Some examples of confidential information include grades, financial aid, performance evaluations, family data, and medical records.

[Back to top ↗](#)

Sanctions

The consequences of mishandling confidential information (intentionally or unintentionally) range from receiving instruction on proper handling of such information to corrective action or discipline.