

UNIVERSITY OF PITTSBURGH

POLICY

SUBJECT: Control of Physical Access to Confidential Information

DATE: April 14, 2003

I. POLICY

It is University policy to appropriately limit access to areas containing confidential information. This includes the ability to monitor the movement of people, equipment, and supplies into or out of those areas. Only those individuals who need access to private and confidential information in order to perform their work related job responsibilities should have access to it, and they should only access the minimum amount necessary.

Additionally, it is the policy of the University to comply with the Health Insurance Portability and Accountability Act (HIPAA) rule and any applicable related state laws that are not preempted by HIPAA. The privacy regulation addressing this can be found at 45 CFR Parts 160 and 164 or at <http://aspe.hhs.gov/admsimp/final/PvsTxt01.htm>.

II. PURPOSE

1. To ensure that access to University areas containing confidential information is appropriately secured.
2. To prevent unauthorized access to confidential information.

III. DEFINITIONS

1. **Need To Know Principle:** Only those individuals who need access to private and confidential information should have access to it, and they should only access information that they need to see. Need is based on a user's demonstrated business requirement for performing duties and responsibilities of a job function.

IV. GUIDELINES

1. Each University unit/department or School is responsible for coordinating access to its facility(ies). Responsibilities include, but are not limited to, the authorization, issuance and review of physical and electronic access privileges.
2. Individuals shall not provide access to confidential information unless authorized to do so in accordance with the appropriate University policies and/or procedures. Failure to adhere to such policy(ies) may be grounds for dismissal.
3. All University areas possessing confidential medical information, clinical and non-clinical, shall be appropriately secured. This includes appropriately managing and safeguarding information within these areas.

V. RESPONSIBILITIES

It shall be the responsibility of each University unit/department or School to implement processes and procedures to meet the requirements set forth in this policy based on the facilities' unique systems and processes.

VI. NON-COMPLIANCE

An employee's failure to abide by this policy may result in the disciplinary action up to and including termination.