

**TERMINATION OR MODIFICATION OF ACCESS TO  
PROTECTED HEALTH INFORMATION: ELECTRONIC  
SYSTEMS POLICY**

**RESPONSIBILITY:** Director of Information Systems, Security Official, Human Resources Director, and all Department Managers

**BACKGROUND:**

When an employee ends his/her employment, or when an internal or external information systems user's access to certain types of data is withdrawn, appropriate security measures must be taken to minimize the possibility of unauthorized access to secure data by those who are no longer authorized to have access to that information. This may include business associates, such as systems maintenance contractors, as well as employees and other members of the workforce. Examples of procedures that may be appropriate upon the termination of access privileges include:

- Changing locks
- Removal from access lists
- Removal of user account(s)
- Turning in keys, tokens, or cards that allow access

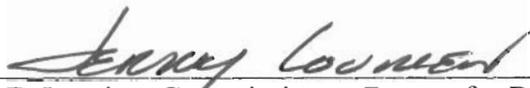
**POLICY:**

Behavioral Health and Health Facilities (BHHF) will terminate access to information systems and other sources of protected health information (PHI), including access to rooms or buildings where PHI is located, when a BHHF employee, agent or contractor ends his/her employment or engagement. BHHF will terminate access to specific types of PHI when the status of any business associate or member of the workforce no longer requires access to those types of information.

It is the duty of the Security Official to receive all notices of termination or modification of access authorization, and to document that all required procedures have been followed to accomplish termination of access in a timely fashion. The Security Official will coordinate these actions with the Director of Information Systems, the Director of Human Resources (or a designee), and the relevant department manager(s).

Effective Date: 4/14/03

Dates Revised:



---

Jerome E. Lovrien, Commissioner, Bureau for Behavioral Health and Health Facilities