

Bethany Life Communities	Date Written: 2-24-2003	Date Revised: 5-1-2009
<b><i>Passwords and User ID Codes (HIPAA Security)</i></b>	Page 1 of 1	

### ***Policy Statement***

It is the policy of Bethany Life Communities to ensure that only authorized team members gain access to or retrieve information from our computer systems, databases, or system applications. This policy applies to all employees of Bethany Life Communities, any subsidiaries, contractors, consultants, business partners, or temporary employees.

### ***Policy Interpretation and Implementation***

1. Passwords and user ID codes shall be required in order to gain access to or retrieve information from any of Bethany Life Communities' operating systems, databases, or system applications.
2. All team members authorized to gain access to or retrieve information from Bethany Life Communities' computer operating system, databases, or system applications will be assigned an individual user ID code and password by the HIPAA Security Officer.
3. A listing of user ID codes, passwords, and levels of access will be stored in a locked file in the HIPAA Security Officer's office. Only the HIPAA Security Officer and the HIPAA Privacy Officer will have access to this file.
4. All programs, software, applications, resident care databases, clinical and financial records, employment records, or other records or databases developed internally will be password protected.
5. All passwords and user ID codes will be assigned by the HIPAA Security Officer or designee. Passwords may not include the user's date of birth, social security number, name, family names, initials, phone number or commonly used words. Random changes of passwords will be made in order to control or manage access to protected information.
6. Passwords will be changed immediately if they are suspected of being disclosed or are shared with another user or unauthorized person.
7. Passwords may not be displayed on the system or maintained at the user's workstation.
8. Users will only be granted access to information, system software, and applications as required for performing their jobs.
9. The HIPAA Security Officer or designee will immediately revoke access privileges when an authorized user is terminated.
10. User privileges will be appropriately changed if the user is transferred or another position.
11. Only the HIPAA Security Officer or designee will shall have access to Bethany Life Communities' system operating files, utility programs, etc., that affect the overall systems operation and management of programs and applications.
12. Users who have access to Bethany Life Communities' information system will be required to sign a compliance agreement prior to issuance of a user ID and password.