

Bethany Life Communities	Date Written: 2-24-2003	Date Revised: 5-1-2009
<i>Reporting Unauthorized Access, Use, and Disclosures of PHI (HIPAA Privacy & Security)</i>	Page 1 of 2	

Policy Statement

The protection of resident and Bethany Life Communities information is the responsibility of all Bethany Life Communities team members including business associates. Unauthorized access, use, and/or disclosure of protected information must be reported.

Policy Interpretation and Implementation

1. Team members who suspect or have knowledge of any unauthorized access, use, or disclosure of protected information must promptly report such data to the HIPAA Compliance Officer or the CEO/President.
2. Incidents of unauthorized access, use, and/or disclosure of protected information must be promptly reported, but in no case later than twenty-four (24) hours of observance or discovery of such incidents. Incidents include, but are not limited to, the unauthorized access, use, or disclosure of the following information:
 - a. Financial information;
 - b. Resident names or other identifying information;
 - c. Resident personal and medical information;
 - d. Resident billing information;
 - e. Employee salaries, employment information, etc;
 - f. Marketing and general business strategies; and
 - g. Any other resident or Bethany Life Communities information that has not been publicly disclosed or has been de-identified according to established Bethany Life Communities policy.
3. When reporting unauthorized access, use, or disclosure of protected health or Bethany Life Communities' information, the following data should be included:
 - a. The name of the person(s) involved in the incident;
 - b. The date and time such incident occurred;
 - c. The location used to access the information (e.g., which terminal, workstation, records room, etc.);
 - d. A description of the information accessed, used, or disclosed (e.g. treatment and payment records, account numbers, etc.);
 - e. If know, the identity of the individual(s) or agency(ies) to which information was released;
 - f. The identity of any witnesses to the incident; and
 - g. Any other information deemed appropriate and relative to the incident.
4. Insofar as permitted by law, person reporting unauthorized access incidents will remain anonymous.
5. Persons reporting unauthorized access may not be subject to any form of retaliation. Substantiated findings of any form of retaliation will be grounds for termination of employment.

Bethany Life Communities	Date Written: 2-24-2003	Date Revised: 5-1-2009
<i>Reporting Unauthorized Access, Use, and Disclosures of PHI (HIPAA Privacy & Security)</i>	Page 2 of 2	

6. Team members who have a reasonable basis to suspect that unauthorized access, use, or disclosure of protected health information has occurred, but do not report such incident, are subject to disciplinary action.
7. False reports of unauthorized access may result in disciplinary action up to and including termination of employment and/or civil action.