

Bethany Life Communities	Date Written: 2-24-2003	Date Revised: 5-1-2009
<i>Installation/Removal of Hardware and Software (HIPAA Security)</i>	Page 1 of 1	

***Policy Statement***

The HIPAA Compliance Officer and/or HIPAA Security Officer will over any installation or removal of hardware or software to the Bethany Life Communities computer system/server/network.

***Policy Interpretation and Implementation***

1. Should an outside vendor be needed to install/remove Bethany Life Communities' computer or server hardware or software, the following protocols must be implemented by the HIPAA Compliance Officer and/or HIPAA Security Officer:
  - a. A complete backup of all data must be performed prior to any installation or removal of hardware or software;
  - b. If the vendor does not have a signed business associate agreement, the vendor must sign a Confidentiality and Non-Disclosure Agreement prior to beginning such installation/removal process;
  - c. If the hardware is being replaced/upgraded, the device must be reformatted to ensure that all data is erased;
  - d. If the hardware is being added, such software must contain appropriate password and user ID protection devices to prevent unauthorized access; and
  - e. If new software is being added, such software must contain appropriate password and use ID protection devices to prevent unauthorized access; and
  - f. If the work is being completed on premises, our HIPAA Compliance and/or HIPAA Security Officer must remain with the vendor until the repair/installation/removal process has been completed.
2. Any CDs or diskettes used for making backup data must be erased, reformatted, or destroyed upon reinstalling the information onto our computer system/server.
3. The HIPAA Security Officer maintains the original copy of software/hardware applications, devices, programs, etc. used by Bethany Life Communities. No other copies are permitted. Only the HIPAA Security Officer or the HIPAA Compliance Officer shall have access to this data.
4. Any suspected or known violations of this policy must be reported promptly to the HIPAA Compliance Officer or the CEO/President.