

## **Data Privacy and Protection of Personal and Confidential Information Policy**

Bethsaida Community, Inc. (“BCI”) is dedicated to protecting the security and confidentiality of the Personal and Confidential Information (as defined below) that we collect, use and maintain. Laws and regulations in the United States and other countries require that organizations safeguard Personal Information and certain Confidential Information.

During the course of your association with BCI, you may create, discover, use, access, receive or otherwise handle Personal and Confidential Information. No matter what your position or role at BCI, you have an obligation to safeguard Personal and Confidential Information. This policy applies to all BCI employees, agents, contractors and associates. In addition, BCI maintains other policies that may protect a broader class of information beyond that covered in this policy.

### **(1) Types of Information Covered by this Policy**

This policy is designed to protect information that BCI collects, uses and maintains that can be used to identify any individual (“Personal Information”), including:

- an individual’s government identification numbers (e.g., Social Security number (“SSN”), Driver’s License identification number, etc.);
- an individual’s financial information, such as an individual’s financial account number, credit card number, debit card number and credit history;
- an individual’s medical or health information, such as an individual’s health insurance identification number; and
- an individual’s name, home address, personal e-mail address, personal telephone or facsimile number, birth date, employment information and background information.

Personal Information may relate to any individual about whom BCI maintains information, including BCI’s employees, officers, directors, owners, consultants, prescribing physicians and patients and individuals associated with employees, consultants, vendors, prescribing physicians, patients and other third parties.

This policy also is designed to protect information that BCI collects, uses and maintains that is proprietary (“Confidential Information”), including but not limited to information related to BCI’s services or business plans, such as:

- technical data, trade secrets and know-how;
- customer and vendor lists;
- marketing strategies;
- patent applications and inventions;
- regulatory data or plans;
- finance and capitalization.

## **(2) Protection of Personal Information**

All BCI employees, contractors and associates must properly handle the Personal and Confidential Information that we collect, use or maintain in the course of business. You have an obligation to safeguard Personal and Confidential Information, regardless of its form (e.g., paper and electronic records containing Personal Information). Your obligations to safeguard Personal and Confidential Information include:

- precluding unauthorized access to, and protecting the security and confidentiality of, Personal and Confidential Information;
- only collecting, accessing, using, maintaining, transporting or disclosing the minimum amount of Personal and Confidential Information that is necessary and relevant in the course of your job responsibilities;
- only disclosing Personal and Confidential Information to individuals who are authorized to access and need such access to perform their job duties and only where such disclosure is permitted by applicable law;
- holding Personal and Confidential Information in strict confidence, both during and after your employment at the Company;
- only removing Personal and Confidential Information from BCI's offices that is required to perform your job responsibilities and returning it immediately after such use;
- not using Personal or Confidential Information for unauthorized purposes and not permitting Personal or Confidential Information to be used for unauthorized purposes; and
- properly disposing of Personal and Confidential Information (where permitted by the Company's Record Retention Policy) in a manner that is commensurate with the degree of risk posed by such Information (e.g., ensuring that SSNs are disposed of so as to make them unreadable, such as by shredding paper documents that contain SSNs or wiping or shredding electronic media that contains SSNs).

You may not use Personal or Confidential Information for your own personal benefit or for the benefit of any third party. Personal and Confidential Information only should be copied to the extent necessary to perform your job responsibilities for BCI, and you must properly maintain, destroy or otherwise dispose of such copies once they are no longer needed so that the Personal or Confidential Information is unreadable. If your employment or association with BCI ends, you may not divulge or use Personal or Confidential Information, and must immediately return to BCI any records containing such Personal or Confidential Information.

The obligation to safeguard Personal and Confidential Information extends to all situations in which Personal or Confidential Information is collected, accessed, used, maintained, transported or disclosed, including when an employee is away from work or working remotely. Measures to safeguard this information may include, but are not limited to, authorization procedures, access limitations and audit controls, such as:

- not discussing another individual's Personal Information or BCI's Confidential Information where you might be overheard;
- utilizing appropriate security measures that are provided, such as encryption, password protection or other technical measures;
- redacting Personal and Confidential Information in documentation so that it may not be viewed by others;
- filing documents and media with Personal or Confidential Information in secured locations with limited access and key or monitored badge access; and
- limiting electronic access to records containing Personal or Confidential Information by saving them to your personal drive.

If the performance of your duties for BCI requires you to disclose Personal or Confidential Information to a third party, prior to such disclosure you should review whether such disclosure is permitted and appropriate. If disclosure is permitted, then prior to transfer of information measures should be taken to safeguard the transfer of such Personal or Confidential Information, including the following:

- request a statement from the vendor or third party regarding the vendor's data security provisions; and
- obtain the third party's agreement to maintain confidentiality of Personal and Confidential Information and to use, maintain and/or dispose of such information in a manner designed to protect such confidentiality.

### **(3) Notification of Potential Breach**

If you become aware of any unauthorized disclosure, access, loss or other misuse or suspect any breach of the confidentiality or security of Personal or Confidential Information, you must immediately inform Claire Silva at (860) 886-7511 x 201 or ClaireS@BethsaidaCT.org BCI will investigate all reported incidents where a breach of Personal or Confidential Information may have occurred and take appropriate action to address any breaches.

**(4) Compliance with Company Policies**

Employees and associates are required to sign an agreement relating to confidentiality and assignment to the Company of rights to inventions as a condition of employment and may be required to re-execute such agreements throughout their employment.

Employees and associates who fail to comply with BCI's policies relating to Personal and Confidential Information, including those who obtain unauthorized access to, or improperly use or disclose, Personal or Confidential Information, will be subject to disciplinary action up to and including termination of employment.