BARBADOS FAMILY PLANNING ASSOCIATION
BFPA
CONFIDENTIALITY POLICY

First Approval Date: December 2017	Next Review Due: November 2024
Dates Reviewed: January 2023	Dates Revised:

Purpose:	To maintain confidentiality of (BFPA) corporate and programmatic information.
Mandated by:	Board of Directors and the Executive Director
Applies to:	All (ORGANIZATION) staff, volunteers, Board members, interns

SCOPE OF THE POLICY

All corporate information is confidential. BFPA's Employees are prohibited from discussing corporate information with persons other than those directly involved. Employees are responsible for storing confidential information (whether paper copies or electronic) in the appropriate location to maintain confidentiality of the document(s).

Confidentiality of all records must be maintained. No information obtained in connection with the provision of programs or services to any person served by or through BFPA shall not be disclosed without the Executive Director's consent, except as may be necessary to provide services, or as may be required by law. Information may be disclosed in statistical or another summary form.

All employees, Board members, volunteers, and interns will be required to sign the Employee / Contractor Confidentiality Agreement assuring compliance with the rules and regulations, and a fundamental core value of the BFPA. As well, any representative of an outside entity who would have access to confidential information through an event such as an audit or site review must sign the Non-Employee Confidentiality Agreement. It is the responsibility of the employee who is the primary contact for the visitor to secure the signed Non-Employee Confidentiality Agreement.

Stringent policies and procedures regarding confidentiality are in place for (BFPA's) staff who have access to Protected Health Information (PHI) and the levels of Accountability. At (BFPA) the only staff who routinely have access to PHI are Health Network staff, but all staff should be aware of the policies and procedures.

The BFPA's Health Information and Technology Program sets forth specific requirements to protect the privacy and security of individuals' protected health information, in compliance with national legislation. Employees and other authorized users with access to the BFPA's records and computer systems are also required to comply with the Health Information Security and Privacy Program and its related policies and procedures.

Confidentiality of information extends beyond employment. All levels of staff, including contractors, are prohibited in divulging, discussing, contacting or otherwise using information, for any reason, regarding all programs served by the (BFPA).

Any employee who violates the acceptable rules of confidentiality or other codes of professional ethics may be subject to terms of progressive discipline, which may include termination by the Executive Director, where there are situation(s) of Gross Misconduct and breaches.
Examples of gross misconduct which will not be tolerated: 1) ***Clients personal information being photographed and circulated to an unauthorized person.***
2) Client and company private and confidential files not being securely stored, and there is a leak.

Reference is made to the following supporting values and policies:

- ***BFPA's Core Values***
- **BFPA's Code of Conduct**
- **BFPA's Communications Policy**

DEFINITIONS

"The BFPA's Confidential Information" - Information, records and data that are subject to this policy include, but are not limited to:

- Individually identifiable health information, including, but not limited to, patient medical records, demographic information, medical, personal or financial identifiers, and financial or payment-related information.
- Research information and processes.
- Personal information about employees, physicians, nurses, and other caregivers, and other individuals affiliated with the BFPA.
- Information and processes related to medical, administrative and professional staff credentialing and privileging and peer review.
- Employment records of others, including but not limited to, competency and performance evaluations, disciplinary actions, and Employee Health records.
- Information about relationships with payers and other third parties.
- Business records and proprietary information including, but not limited to, financial records, audit and accounting records, risk management and
- compliance activities, quality assurance information, operations, policies and procedures, business development and strategic plans, and similar information.
- Computer software and information technology processes.
- Products/devices protected by intellectual property or proprietary rights of any party.
- Fundraising data and individual donor information held by the BFPA.
- Data related to community members and non-patient participants of other BFPA Programs.

THE BFPA Confidential Information includes information in any format, including, without limitation, computerized records, manually generated records, paper copies, electronic records, digital records, audio or video recordings, and information obtained orally.

Confidentiality is the act of limiting access to and disclosure of protected information to authorized persons or parties.

Security is the act of preventing unauthorized access, use, disclosure, modification and destruction of BFPA confidential information.

Authorised User means any individual or entity that is given access to BFPA records, data and/or information technology systems that may contain confidential or proprietary information. This includes, but is not limited to, employees, medical staff members, health care professionals, residents, fellows, students, volunteers, governing board members of any BFPA affiliate, committee members, and other individuals or entities carrying out authorized functions or responsibilities.

PROCEDURE

1. Access to the BFPA's Confidential Information is restricted to authorized users on a need-to-know basis, as determined by their job-related or service-related responsibilities and obligations. Business, financial and corporate records may be accessed and used by authorized business, financial, external auditing, and corporate consultants within the scope of their responsibilities.

2. Any third party granted access to the BFPA confidential information shall be restricted to those records and information necessary for the purpose(s) set forth in the service agreement. Appropriate confidentiality provisions will be set forth in the service agreement. Any third party that will be accessing the BFPA's patient protected health information and meets the definition of a Business Associate and must enter into a Business Associate Agreement.

3. It shall be the responsibility of each BFPA employee to report any suspected breaches of this policy to BFPA management.

4. It is the responsibility of each BFPA employee and authorized user to comply with the Information Technology Handbook with respect to individually identifiable health information of the BFPA patients.

5. It is the responsibility of the BFPA employees and authorized users to take reasonable precautions to protect the BFPA confidential information from unauthorized access, use, disclosure, modification and destruction. This includes reasonable steps to ensure the physical and technical security of paper records, as well as all types of files and data, electronic mail, and computing devices, portable devices and or remote access to the BFPA information systems that may be used to access, store or transmit confidential information electronically.

6. Any BFPA employee will be subject to disciplinary action, in accordance with applicable employment policies and procedures, up to and including termination, if he or she: Accesses or misuses confidential information other than on a need-to know basis as determined by his/her job-related or service-related responsibilities and obligations;

6.1 Fails to protect the confidentiality or security of BFPA confidential information;

6.2 Fails to prevent disclosure of BFPA confidential information to any unauthorized third party;

6.3 Fails to report any suspected breaches of this Policy, BFPA policies related to information security, or BFPA policies governing health information security or privacy;

6.4 Fails to abide by the BFPA Health Information Security and Privacy Program or The BFPA policies and procedures related to confidentiality, privacy or security of electronic protected health information; or

6.5 Shares computer passwords or permits another person to inappropriately access, alter, delete or use confidential information using his/her unique username and/or password or other token or authentication method assigned to the individual.

7. Any authorized third party who violates this policy may be denied continued access to BFPA systems, records and information, may be subject to the termination provisions in the service agreement or Business Associate agreement, and/or may be subject to legal action for breaching the duty of confidentiality, breach of contractual obligations, or breach of any covenants, express or implied, contained in the service agreement, or applicable legal obligations.

8. With specific regard to patient medical records, the medical record is the property of the entity in which it is created and is used by practitioners in the management and evaluation of patient care. It is maintained for the benefit of the patient, the physician and other caregivers, and the operations of the BFPA entities. Disclosure of medical record information is allowed in accordance with established policies only and is the responsibility of the BFPA Management.

9. Upon hire, all new employees must sign any Employment Agreement/Contract with a respective Confidentiality clause to be given access to any BFPA records or computer systems.

9.1 An IT User Access request via email must be submitted by the person's Manager before any employee or authorized user can be granted privileges to access. The BFPA's information technology resources. Privileges will be granted only as necessary to carry out his/her duties or job responsibilities.

10. In addition to employees, certain other individuals must sign a Confidentiality Agreement prior to being given access to the BFPA records or systems, including but not limited to the following:

    - Applicants to the Medical Staff for membership or clinical
    - privileges
    - Faith based Leaders
    - Consultants and Individual Clinical Contractors
    - Residents, Fellows and Medical Students
    - Trainees/Students
    - Volunteers

    Signed Confidentiality Agreements for non-employees will be retained in the Medical Staff credentialing files, or with the department/manager responsible overseeing the functions and activities of such individual, as applicable.

11. This policy is not intended to invalidate confidentiality protections established in law or other applicable BFPA policies, including, but not limited to, employment policies, Medical Staff By-laws or Rules and Regulations, quality improvement procedures, or other policies providing specific protection of confidential information.