INFORMATION SECURITY & TECHNOLOGY POLICIES

Part I: Employee Responsibilities

Effective Date: _____

Last Approved by Board: _____

Last Revised : **March 2013**

Table of Contents

Introduction: Why do we have an Information Security & Technology Policy?

It makes sense: Bread for the City users, guests, volunteers, contractors, and other visitors interact with private information all the time. It isn't our information to share with anyone else, and this document describes how we can protect the information we are trusted with.

HIPAA Compliance: We'll discuss this shortly, but the Health Information Portability and Accountability Act (and the other assorted rules and regulations) require us to take certain steps to protect information. This document outlines all of those steps.

This policy describes how to:

- Secure protected client information.
- Provide privacy training for our employees.
- Provide information for our patients about their rights - Bread for the City will only share their personal information for the purpose of treatment, clinic operations, public health, or research
- Have some written information and security policies and procedures.
    - Have a Privacy Officer to ensure HIPAA compliance: Jeannine Sanford for all of BFTC, and Julia Eddy for Medical.

What does the Information and Security Policy Cover?
The policies outlined here apply to all departments of Bread for the City and the confidential information with which they interact.

This document defines security procedures for all Bread for the City personnel (staff, volunteers, contractors, etc) and for all of the systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of Bread for the City, entities in the private sector, and in cases where Bread for the City has a legal, contractual or fiduciary duty to protect said resources while in Bread for the City custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Bread for the City network system of various hardware, software, communication equipment and other devices designed to assist Bread for the City in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Bread for the City domain, either hardwired or wirelessly, and includes all equipment that is deployed by Bread for the City inside and outside of our offices.

Related Laws/Regulations
The following is a list of the various agencies/organizations whose laws, mandates, and regulations guide this document.

DC Mental Health Information Act of 1978:
The Act makes it unlawful for a mental health professional, facility, or its employees to disclose or permit the disclosure of mental health information unless permission is granted, or a specific exception in the law applies (such as an emergency situation). The Act addresses such issues as personal notes, general rules governing disclosures and the prescribed form of authorization, amongst other interactions.

Health Information Portability and Accountability Act (HIPAA) of 1996:
The main objective of HIPAA is to protect health information by establishing standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information. HIPAA applies to health care providers and employer group health plans. HIPAA is a complex statute that affects Bread for the City in several ways, including operations, policies, IT systems, training, contractual relationships and relationships with long–standing partners.

In 2009, the HITECH Act added an additional requirements around information security and notifying patients in the event of a breach of their health information.

Who do I talk to when there are issues?
Issues and questions regarding security concerns should be sent to privacy@breadforthecity.org. The Confidentiality and Security Team (see below) will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will address security issues as they arise and will identify areas where staff training may be necessary.

Privacy Officer
Bread for the City has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee everything related to the development, implementation, and maintenance of Bread for the City privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for Bread for the City is:

Jeannine Sanford, Esq. COO. She can be reached at privacy@breadforthecity.org.

Confidentiality / Security Team (CST)
Bread for the City has a Confidentiality / Security Team made up of staff who are responsible for identifying and planning for possible security concerns and for being the first line of defense for our confidential information. The members of the CST as of March 2013 are:

Chief Operating Officer - Jeannine Sanford
Network Administrator - Andre Saliba

Information Management Specialist - Jessie Posilkin
Medical Clinic Operations Manager - Julia Eddy

What is confidential information?
Bread for the City staff, interns, volunteers, and contractors have access to a lot of information that could reveal a person's identify or provide someone with access to our systems. The following is a list of information that should be protected:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images
- Usernames and Passwords

Confidentiality Agreement
As a condition for employment/contract, all users of Bread for the City information resources sign a confidentiality agreement.

Temporary workers and contractors not already covered by a confidentiality agreement must sign the confidentiality statement prior to accessing Bread for the City information resources.

Compliance and Enforcement of these Policies & Procedures
All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to disciplinary action, up to and including termination, in accordance with Bread for the City's Sanction Policy.

Employee Responsibilities

Employees have three major responsibilities:

- Only access information if you need it to do your job.

- Ask for consent before sharing information.

- Only share information with others who need it to do their jobs.

Below we have detailed exactly how you can meet these responsibilities. Each of us are the first line of defense in protecting the personal information we work with daily. We are responsible for the security of all data, in any format. Each of us is responsible for staying up to date with Bread for the City's ongoing training programs, and Bread for the City is responsible for planning and implementing those ongoing trainings. Staff can protect data by observing the following policies and procedures.

Sharing Client Information

All staff and volunteers are reminded that client/patient confidentiality is to be respected at all times. While each program area has somewhat differing requirements regarding confidentiality, some basic standards apply in all cases.

First and foremost, the fact that an individual is a client/patient of the organization is, in and of itself, confidential information. Occasionally, a caller or visitor to the clinic will ask if an individual is a patient or client of our clinic. Under no circumstances should this information be revealed without the express consent of the client/patient. **The fact that an individual is being seen in our medical clinic, working with an attorney or caseworker, or getting a bag of groceries is confidential information and is not to be revealed to anyone making a general inquiry.**

The most common scenario occurs when "Joe Smith" comes to the clinic or calls to find out whether "Jane Smith" is here. Usually, they are simply trying to arrange transportation. But, unless "Jane" has told you that she is expecting a call from "Joe," it is <u>not</u> appropriate to tell Joe that she is here or that she is being seen or that she should be done in an hour. The appropriate response is to ask for his name, call a staff person in the program area where you believe Jane is being seen, and state that there is a Joe Smith here or on the phone for Jane Smith. The staff person then can ask Jane if she wants to talk to Joe or give Joe any information. This provides Jane an opportunity to say "I don't want him to know I'm here – please tell him I'm not here." Then, the staff can relate an appropriate response to Joe. Pretending the patient or client is not here until she expresses a willingness to let her presence be known can be awkward, but it is nonetheless important. Please remember that there are any number of reasons a patient or client may not want someone else to know that they are seeing someone here. (Think domestic violence, personal legal matters, medical condition, pride . . .)

Even if a police officer or other badge flashing authority figure shows up and asks whether an individual

comes here or is here, we cannot answer that question. Politely explain to the officer that the information is confidential, but if he or she returns with a subpoena, we may be able to provide the requested information.

Any time someone can view your computer screen, when you send a fax, call someone on the phone, or use the Internet in a public place, personal information is at risk. Even if you do not anticipate someone using the information for nefarious purposes (e.g. your trusted roommate is not likely to commit identity theft or sell BFC client information to scam artists), someone could intercept confidential information and you have an obligation to protect the very personal and private information you have been entrusted with.

Any purposeful and unauthorized release of Bread for the City data is a violation of Bread for the City policy and will result in personnel action, and may result in legal action.

Release of Information (ROI) forms

Each of Bread for the City's programs may have specific policies and procedures around sharing client information, and clients should be informed about basic use and disclosure of their information at intake. The Medical Clinic has a Release of Information form (ROI) that clients must sign for release of their medical records beyond the normal scope of information sharing that is done for Treatment, Payment, and Operations; the Legal and Social Services departments have similar forms. These forms are designed to reinforce the client's control over their information.

When medical records are requested, written consent is obtained from a client before releasing records for any reason other than for Treatment, Payment, or Operations as outlined in Bread for the City's HIPAA Notice of Privacy Practices. Copies will be made only for the information and dates of service indicated. Records from outside clinics and hospitalizations will not be released. Please see Bread for the City's Consent for Release of Information form and HIPAA Notice of Privacy Practices for more info about Medical Clinic procedures.

Photo Release

Bread for the City uses social media for all kinds of communication and fundraising work. If you are helping a client tell a story, or are taking photos or videos of clients, you must obtain a release of information using the Photo Release Form (available on the Development Drive and in the All Staff Information Folder). You must inform them that Bread for the City can use the information we obtain at any time for any reason - and allow the client to adapt the release as they wish. (For instance, someone might allow their photo to be used in one blog post, but not want their photo used again without express permission).

Electronic Information Security

Document Storage

Most departments have guidelines for where documents should be saved (eCW, Box, different specific

files on the server). *Nothing should ever be saved to the local computer.* If you are in doubt about where to save something, please ask your manager. Generally, H Drives are deleted when employment is terminated, so supervisors and staff should be cognizant of where important documents live.

Storing & Locking Computers

Unattended computers should be screen-locked (or logged off) by the user when leaving the work area. Remember that anyone who uses your computer when you are logged on can go anywhere you can go. Bread for the City requires that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Laptop computers are unfortunately easy to steal. Cable locks are not foolproof, but do provide an additional level of security. An unattended laptop or tablet should also be locked with a cable lock.

At the conclusion of your work day, you must log off and **shut down** your computer.

De-identification / Re-identification of Confidential Information

Confidential or personal identifying information, especially Protected Health Information (PHI), should be de-identified (removed or scrambled) any time it is shared or stored.

For instance, the legal clinic or social services program might share information about a public benefits application with a colleague at another organization. In this case, the documents should not contain Social Security numbers, birth dates, or names. Should it need to contain that personal information, the email must be encrypted.

> *Data Analysts/Tech Team take note*: If you have any information that you are transferring and have a code you are using to de-identify and re-identify that information, do not derive that code from or related to information about the individual. For instance, birth dates should not be scrambled and then used as a "unique identifier" for the client. The code should not be disclosed for any other purpose nor should the mechanism for re-identification be disclosed.

Encrypting Email to send outside of Bread for the City

Any user wanting to exchange confidential information with a specific person outside of Bread for the City (for instance, to share HIPAA protected information with a patient or Doctor) can use our Postini encryption software, which is built into our Google Accounts. This applies across departments at Bread for the City. Bread for the City Technology staff will train all staff as soon as this tool is live - please stay tuned for updates.

User Login IDs & Passwords

User IDs and passwords are required in order to gain access to all Bread for the City network, workstations, and information systems.

Individual users must have unique login IDs and passwords. Users are responsible for the use and

misuse of their individual login ID.

Those who manage generic logins (the Intake login, for instance) are responsible for the use and misuse of those login IDs, and for properly training those who use any generic login.

Your login ID will be locked after a maximum of five (5) sequential unsuccessful login attempts. Contact TechSupport to have your password reset.

When a new user is set to begin, their supervisor should contact TechSupport@breadforthecity.org, who will reply with the Network Access form to be completed.

All user login IDs are audited at least twice yearly and all inactive logon IDs are revoked. Bread for the City HR notifies TechSupport@breadforthecity.org, at the time of departure of all employees and contractors, at which time login IDs are revoked.

All passwords need to be "Strong", which means they must conform to restrictions and limitations that are designed to make the password difficult to guess. When setting a password, please note the following:

> Password Length – Passwords are required to be a minimum of eight characters.
> Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
> Change Frequency – Passwords must be changed every 180 days[16]. Compromised passwords shall be changed immediately.
> Reuse - The previous ten[17] passwords cannot be reused.
> Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Use of Transportable Media

Transportable media includes anything that you might use to move information between computers, such as DVDs, CD-ROMs, USB key devices and SD cards.

The purpose of this policy is to guide Bread for the City in the proper use of transportable media. First, transportable media can only be used when there is an organizational need to transfer data to and from Bread for the City networks. Because transportable media are easily lost, we must be extra careful with these devices.

Because any transportable media that comes from somewhere else or is connected to a non-BFTC computer can have a virus, please bring the device to the Network Administrator before using it. For example, do not copy a work spreadsheet to your USB key and take it home to work on your home PC. We have trusted relationships with certain organizations (for instance, DCPCA) and you are allowed to use devices from those organizations without permission from the Network Administrator.

When using a USB/transportable media with sensitive information, you must:

- Get the device from the Network Administrator, that's Andre.
- Encrypt the device (need help on this? Ask the Network Administrator)
- Non-sensitive data may be transferred to the non-encrypted space on the media.

While no USB keys should be necessary for internal BFTC use, occasionally we will have to use them internally for necessary data exchange - for instance, providing Data to auditors via USB key during the course of the audit.

- Report all lost transportable media to your supervisor or department head and Privacy@breadforthecity.org. You must report immediately, so Tech and Privacy staff can identify the severity of a potential breach of confidential information.

- When a device is no longer needed, or an employee ends employment at Bread for the City, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for proper disposal.

Disposal of Transportable Media

It must be assumed that any external media device (USBs, CDs, etc.) in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Therefore, please take the following steps to destroy those devices:

- It is the responsibility of each employee to identify items to be shred or cleaned.
- When no longer needed, all external media devices are to be sent to Information Management Specialist for proper disposal with information about who sent it and why. External media should **never** be thrown in the trash.

Before disposing, equipment will be wiped of all data, and factory defaults restored. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Personal Use of Bread for the City's Technology:

Technology resources are intended for organizational business. However, personal use is permissible as long as:

1. it does not consume more than a trivial amount of your time or resources,
2. it does not interfere with your job responsibilities,
3. it does not preempt any organizational activity,
4. it does not involve any of the following:

   a. Copyright violations – This includes the act of pirating software, music, books and/or

videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
b. Illegal activities – Use of Bread for the City's information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
c. Commercial use – Use of Bread for the City's information resources for personal or commercial profit is strictly prohibited.
d. Political Activities – Bread for the City is a 501(c)3 organization. Bread for the City encourages all of its employees to vote and participate in the political process. However, Bread for the City resources may not be used in specific candidate campaign activities.
e. Harassment – Bread for the City does not tolerate any form of discrimination of or by its employees. Therefore, Bread prohibits the use of any technology in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but are not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
f**. Junk E-mail** - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited.

Generally, while it is **NOT** the policy of Bread to monitor the content of any electronic communication, Bread for the City is responsible for servicing and protecting our equipment, networks, data, and resource availability and therefore may access and/or monitor electronic communications. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

Bread for the City reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Bread for the City policies.

Please use all technology and communications tools with the knowledge that the content could be seen by others, and that any electronic communications can be forwarded, intercepted, printed or stored by others.

Prohibited Activities
Personnel are prohibited from the following activities. The list is not exhaustive. Other prohibited activities are referenced elsewhere in this document.

- Do not crash or significantly slow down any of BFC's information systems. If you are made aware that something you are doing on the computer has crashed or significantly compromised BFC's systems and you continue to engage in that activity, your action will be considered a

deliberate act and Bread for the City may take disciplinary action.

- Do not attempt to "break in" or to bypass security features that protect an information system.
- Do not infect or attempt to introduce a computer virus, Trojan horse, peer-to-peer ("P2P") or other malicious code into an information system.
- Do not go browsing in our databases. Bread for the City has access to a lot of confidential and sensitive information which is protected by various federal, local, and professional regulations (ie. HIPAA) which stipulate a "need to know" or other requirement before approval is granted to view the information. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited.
- Do not use personal or unauthorized software on one of Bread for the City's protected networks. Use of personal software is prohibited. All software installed on Bread for the City computers must be approved by Bread for the City.
- Do not violate or attempt to violate the terms of use or license agreement of any software product used by Bread for the City.
- Do not engage in any activity that is illegal or contrary to the policies, procedures or business interests of Bread for the City.

Appropriate Use of Organizational Hardware

Only computer hardware and software owned by and installed by Bread for the City are permitted to be connected to Bread for the City's network. Only software that has been approved for use by the network administrator may be installed on Bread's equipment.

Retention and Ownership

All email users are expected to read, digest, and respond as appropriate (and appropriately) to electronic communications. All electronic communication on Bread for the City owned tools are the property of Bread for the City and not the property of the individual users. We store all email communications for 10 years. This policy applies to all Bread for the City computer users and covers all electronic communications on Bread for the City software and hardware including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, mobile devices, and servers.

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of Bread for the City are the property of Bread for the City are the property of Bread for the City. Bread for the City may agree (through the Chief Executive Officer) to share ownership with the creator or to release a tool as open source software when appropriate. Bread for the City uses electronic communications with all staff.

Retention / Destruction of Paper Documents

State and federal laws regulate the storage and destruction of medical information, and Bread for the City actively follows these laws. If ever there is a conflict between two laws, we follow the strictest regulation.

Medical Record Retention

Since August 2008, all Bread for the City patient information is stored in our electronic health record system, eClinicalWorks (eCW). Paper charts for active patients who were also seen in the medical clinic prior to 2008 have been scanned into the electronic health record system. Patient records for patients who have not come back to Bread for the City since 2008 are retained in storage.

All documents relating to patient care (such as progress notes, lab results, medications, uses and disclosures of personal health information (PHI), authorization forms, business partner contracts, responses to requests to amend medical records) are maintained for a period of 7 years. Records for Pediatric and Prenatal patients are kept until the pediatric patient or the child of the prenatal patient is 25 years old.

When the allotted retention time has passed for charts in storage, the charts are reviewed against the electronic record before destruction. If the paper chart should be kept longer, for example the patient has an active electronic chart, then the entire chart will be scanned into eCW and then destroyed appropriately.

Record Destruction

All hard copy medical records that require destruction are shredded using NIST 800-88 guidelines. This means that for hardcopy data, cross cut shredders should be used to produce particles that are 1 x 5 millimeters in size. We contract with a shredding company that works to that standard. Medical records requiring this shredding may be placed in the locked gray bins marked "Shred," which are found at both centers.

More on NIST guidelines can be found here:
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Shredding:

Any papers containing sensitive information that are no longer needed, must be shredded before disposal. As noted above, there are designated locked shredding bins throughout the office.

Bread for the City contracts with shredding company Iron Mountain. Work orders from the shredding company are shared in Bread for the City's Finance Department files F:\Financials\Vendors\Iron Mountain.

Building Security

Bread for the City is committed to maintaining a safe working environment and protecting our information and staff. Building security has been designed in such a way to limit access to certain areas where sensitive information and resources are stored. This means:

- The entrances to the building are controlled by a security code system. When the building is closed to client services, staff need to use their codes and key fobs to get in.
- If you mis-enter your code, use a code that is not connected to you key fob, or do not close the building quickly enough, the police will be alerted and the Privacy Officer/COO will be called.
- Areas of the building that house sensitive information; devices with access to sensitive information; and valuable equipment and supplies are protected by specific keys and are always locked when not in use.
- All keys and security codes are issued by the HR Manager in NW and Facilities Manager in SE. Individual Bread for the City employees are given security codes for opening and closing the building. Sharing security codes with unauthorized individuals is strictly prohibited.
- When a staff member is no longer employed at Bread for the City, all keys and key fobs are returned to the HR Manager in NW or Facilities Manager in SE. Key fobs and security codes are deactivated immediately.
- Guests in the building should always be accompanied by authorized personnel (or other trusted individuals). Guests are only permitted in waiting areas when reception staff are present or the reception area is secured. Reception staff will stay until the last clients and guests leave and will close and lock reception areas when they leave for the day. On occasions when BFC's facilities are used by outside groups (i.e. EJC, DC Bar, groups renting the conference rooms), BFC staff should take extra caution when cleaning up workspaces and reception areas before guests come in.
- Visitors should be encouraged to wait in one of the appropriate waiting areas (intake rooms, exam rooms, waiting rooms). Any person who does not respond appropriately when told to wait in these areas should be immediately reported to senior staff. All visitors to the building should check in at the appropriate front desk of the service area they intend to visit (medical visitors at the medical reception, RPP at the RPP desk, food and all other inquiries at the main reception, etc.)
- In some situations, non-Bread for the City personnel may sign a confidentiality agreement and be granted access to protected areas and information for a specific amount of time but just as with staff, when they leave they must hand over any keys and equipment they may have been given and their access codes, usernames and passwords will be deactivated.

Challenge Unrecognized Personnel

If you see an unaccompanied person you do not recognize in a part of the office that is “staff and volunteers only,” you should ask if they are in the right place and need help getting somewhere. If the person does not respond appropriately, you should immediately report the issue to senior staff. Encourage visitors to wait in one of the appropriate waiting areas (intake rooms, exam rooms, waiting rooms). Alert other staff that you encountered a wanderer. All visitors to the building should check in at the appropriate front desk of the service area they intend to visit (medical visitors at the medical reception, RPP at the RPP desk, food and all other inquiries at the main reception, etc.).

Email

While email is a terrific communication tool it has some particular challenges and limitations. The following points may help you use email to its best advantage:

- Keep in mind that it is not easy to convey intonation clearly so choose your words wisely.
- Reread your email aloud to make sure that your message is clear and polite.
- "CC" people who should be in the know, but do not necessarily need to respond to your email.
- As a general rule, please refrain from the "Reply All"
- Forward non work-related emails (for example: humor, political, inspirational) sparingly and carefully.
- Always be conservative when including client confidential information in email communication. Follow program-specific and organization policies around sharing client-confidential information and protected health information (PHI).

Internet Access & Blocked Sites

Internet access is a great resource that Bread for the City provides to all computer users. This resource is costly to operate and maintain, and must be allocated primarily for operational needs. Bread for the City's Internet access should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Using the Internet as a radio or to constantly monitor the weather or stock market results can eat sufficient bandwidth to cause problems for staff using the network. While seemingly trivial to a single user, wide use of these non-business sites limits the amount of Internet bandwidth available for mission-critical work.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites have already been blocked by Bread for the City routers and firewalls. This list is constantly monitored and updated as necessary.

If you need access to a work appropriate blocked website, please email techsupport@breadforthecity.org and cc your manager with the request for access.

Proper Internet Use at Work

We are required to block public Internet access to Bread for the City information resources that need to be private, and to protect confidential Bread for the City information when it is transmitted over the Internet.

The following rules must be followed when using Bread for the City's private Internet network.:

- Users do not have permission to download software, as it could compromise Bread for the

City's technical infrastructure. If users have a need for additional software, the user must contact their supervisor;

- Please use the Internet in a way that is consistent with the goals of Bread for the City. Use of the network for personal profit or gain is prohibited, and is also not an appropriate use of work time.
- Do not enter confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other tools that can be used to access goods or services - without using an encrypted connection. Usually, this looks like "HTTPS" at the top of your web browser.
- Do not put Bread for the City software on your home or other non-Bread for the City equipment.
- No personal devices should be connected to Bread for the City's network, as they fall outside of the security protocols set up by our network administrator. In the event that you have a request to transfer Bread for the City data to a non-Bread for the City Computer System, you should speak with your manager, as well as the Chief Operating Officer (COO) and Network Administrator, about the appropriate and best way to proceed.
- All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any client level information to anyone outside Bread for the City with whom a written agreement does not exist.

Please consult with the IT Network Administrator if you or a guest:

- Need to connect to the Internet through a wired connection;
- With prior permission from a manager, need to connect to the private wireless network;
- Need to share private Bread for the City information (including notices, memoranda, documentation and software) via an FTP Server or similar device
- Cannot access mission critical websites or devices

Screensavers/Desktop Images

Some screen savers may be considered inappropriate for our work environment: please remember that every computer screen in the building can be seen by your colleagues, our clients, volunteers, and/or donors who come to us with a variety of concerns and experiences. If your screen saver or background might be inappropriate - please change it. If you are not sure -- you should probably change it.

Signature Lines

Any staff who may send email with client confidential information or protected health information via email should include one of the following statements in their signature line:

> ***Generic:*** *This message and any attachments may contain confidential and privileged information. If you are not the intended recipient or have received this message in error, please notify the sender and promptly delete the message.*
>
> ***Social Services:*** *This communication and any attachments may contain information*

which is confidential and/or privileged. This information is intended for use only by the addressee indicated above. If you are not the intended recipient, please be advised that any disclosure, copying, distribution, or use of the contents of this information is strictly prohibited. If you have received this communication in error, please notify the sender immediately and destroy all copies of the original transmissions. This message may contain sensitive information covered under HIPAA and the District of Columbia Mental Health Information Act of 1978.

Many of us want to express our own individuality with our Bread for the City email correspondence signature lines. If you choose to personalize your signature line, please consult with our Communications Associate who can provide appropriate graphics and signatures.

BFC's Wireless Networks

This section outlines how to obtain wireless access, how to use wireless access, and how to protect security of Bread for the City laptops and mobile devices when on a wireless network.

Wireless Availability - Bread for the City has two public wireless access points.

SE Wireless Availability:
The public wireless is provided by DC-CAN, and called "DC Free WiFi". There is no password required, but you must agree to their terms of service when you login. It is only available for 20 minutes at a time, and can be accessed reliably from the top floor, and less reliably from the fishbowl, and cannot be accessed from intake rooms.

NW Wireless Availability:
The guest wireless access point is located in the development office near the server closet. It has a password that should be posted publicly, and can be accessed throughout the first floor on the new side of the building. It has less reliable access throughout the second floor on the new side of the building, and generally cannot be accessed on the old side of the building.

There is private wireless available in both locations, which is administered by the Network Administrator. Any requests to access the private wireless must be directed to the Network Administrator to check your software and to make sure that your device can be safely added to the network.

Software Requirements - The following is a list of minimum software requirements for any Bread for the City laptop that is granted the privilege to use wireless access outside of the building:

- Windows XP with Service Pack 3 (Firewall enabled)
- Antivirus software
- Full Disk Encryption
- Appropriate VPN Client, if applicable

- Internet Explorer 6.0 SP2 or Greater

Training Requirements - All BFTC staff using BFC laptops outside of the office must receive a brief training. You will be expected to know the basics of connecting to wireless networks, how to secure your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks.

Smartphones and Personal Devices
When using personal devices, including smartphones, for work purposes, the following setup and precautions are required (ask Tech Support if you need any help setting these up):

1. A passcode lock must be set
2. HTTPS browsing must be enabled
3. The "Find My Phone" feature must be turned on

Telecommuting

If you want to know if you can work remotely, please consult the Policies and Procedures Work from Home Policy and speak with your manager. Users who plan to connect to any Bread for the City systems from outside of the network must follow the procedures outlined below as working outside of Bread for the City's network opens our network to possible trojans, malware, and other viruses.

General Requirements
Telecommuting workers are required to follow all organizational policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting users will have access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password on your various systems (GoogleApps, eCW, Salesforce, etc.), is even more critical in the telecommuting environment. Passwords must be changed every 90 days. Do not share your password or write it down where someone might see it.
- **Job Specific:** You may have additional security requirements not outlined here, depending on the nature and location of your work.

Bread for the City's IT staff may provide the user with the following:

- a Bread for the City approved workstation
- a cable lock
- VPN connection (required hardware firewall and access, if applicable)
- Software and hardware updates

Employees are responsible for the following:
-- Maintaining their own internet connections

-- Keeping documents, hardware, and data secure
-- Disposing properly of confidential documents and external media, either by shredding them at home, or returning them to the office for proper disposal
--Virus Protection**:** Home users must never stop the update process for Virus Protection on Bread for the City issued computers. This update is critical to the security of all data, and must be allowed to complete.

If you ever plan to do work at home or offsite:
-- If you use eCW, you will need to use remote desktop in order to access files and records containing personal health information.

-- For those staff using Salesforce, but not downloading files (eg. editing records or making case notes), you will need to "authenticate your device" (follow the instructions Salesforce gives you), and log out of Salesforce (not just close your browser) when you are done.

-- For those using Salesforce and downloading files from Box.com, you must have the Box Editor installed so that you are able to edit directly in Box, without downloading documents onto your device.

-- With GoogleDrive, you must edit within Google Drive - do not download documents with ePHI onto your personal machines.

-- If you download BFC files onto a personal computer or device, those files should be permanently deleted immediately after use. Files in the recycling bin on your computer are not fully deleted until you "empty it."

-- Using Non-Bread for the City Internet: Extreme care must be taken when connecting Bread for the City equipment to any outside internet network. Bread for the City has no ability to monitor or control the security procedures on non-Bread for the City networks.

--E-mail: Do not send any individual-identifiable information via e-mail, unless you have been instructed in how to use Postini Encryption tools. These will be enabled in 2013. If you need assistance with this, contact the Privacy Officer or technology personnel.

--Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

--Do not perform work tasks which require the use of sensitive organization or client level information when you are in a public area, i.e. cafe, airport, lobby. Computer screens can easily be viewed from beside or behind you.

When something goes wrong

Reporting Software Malfunctions

If you are having problems with any software (eCW, Gmail, Salesforce, etc...), you should send an email (or have someone send one on your behalf) to:

techsupport@breadforthecity.org [For all computer, email, Salesforce, phone, and general technology related issues]
ecwsupport@breadforthecity.org [ALL issues and questions related to eClinicalWorks]

Malfunctions may pose an information security risk. Computer viruses can be transmitted through email attachments and links on some websites. Computer users should be cautious and use good judgment when navigating the Internet and email. ***If a user suspects a computer virus infection, the user should immediately stop using the computer and report to TechSupport staff, noting anything new and/or unusual.***

TechSupport staff will monitor the resolution of the malfunction or incident, and report to the Confidentiality Security Team (CST) the result of the action with recommendations on action steps to avert future similar occurrences for any notable incidents.

Reporting Security Incidents

All computer users are responsible for reporting perceived security incidents. If you have reason to suspect a security breach (confidential information has been, or could have been, accessed by an unauthorized person), you should report that immediately to Privacy@breadforthecity.org (goes to everyone on the Confidentiality Security Team (CST)) and your supervisor.

Each incident will be analyzed quickly to determine any additional steps needed to protect our infrastructure. All incidents reported to privacy@breadforthecity.org (and actions taken) will be logged by the CST in a Quality Assurance Incidents and Grievances spreadsheet for additional review by the Quality Assurance and Improvement Committee. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Bread for the City Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately.

Breach Notification Procedures

HIPAA and HITECH require us to notify affected individuals if there is a breach of our systems - the unintentional or intentional release of Personal Health Information (PHI). The following procedure describes what a breach is, and how to manage one should it occur.

Definitions

Breach – Unauthorized acquisition, or reasonable belief of unauthorized acquisition, of Personal Information that compromises the security, confidentiality or integrity of the Personal Information. Also

referred to as HIPAA Breach or Privacy Act Breach to indicate unauthorized acquisition, access, use, or disclosure of unsecured Protected Health Information (PHI).

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
(from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html)

There are situations which are exceptions to being defined as a Breach:
-- If the information is encrypted
-- Accidental acquisition/use by a colleague or person acting under the authority of a covered entity or business associate, if the the acquisition/use was in good faith and the information was not further released.
-- Good faith that the unauthorized person who access the information would not reasonably have been able to retain the information.

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Protected Information in the custody or control of Bread for the City will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach. In no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer.
    b. The supervisor/manager will provide the Privacy Officer with as much detail as possible.
    c. Both the employee and supervisor will be responsive to requests for additional information from the Privacy Officer.
    d. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
3. The Privacy Officer, in conjunction with Bread for the City's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness

and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with the department(s) to immediately contain the breach. Examples include, but are not limited to:
        - Stopping the unauthorized action
        - Recovering the records, if possible
        - Shutting down the system that was breached
        - Correcting weaknesses in security practices
        - Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach
There are four main factors in analyzing a breach (this part is lifted from a presentation by EpsteinBeckerGreen):

1. The nature and extent of the PHI involved, including the types of identifies and likelihood of re-identification. Of particular concern are the likelihood of:

a. Identity Theft

or

b. Embarassment (eg. the Nature of the services being performed, treatment plan, diagnosis, medication, medical history, or test results).

2. The unauthorized person who used the PHI or to whom the disclosure was made. The factors there include:

a. Capabilities

b. Responsibilities (e.g. if personal health information is sent to the wrong medical clinic, that medical provider is legally obligated to destroy it)

c. Motive

3. Whether the PHI was actually acquired or viewed. If the device is recovered, treat the device as evidence. Do not turn it on or use it without a member of the technology team examining the information on the device.

a. A forensic analysis could determine that the computer was never accessed, thereby ensuring that the information was not actually acquired by an unauthorized individual.

4. The extent to which the risk to the PHI has been mitigated.

a. We can rely on the assurances of an employee, affiliated entity, business associate, or other "covered entity" that they destroyed the information if it was received in error, while such assurances from third parties may not be sufficient. Please see the CST for potential ways to mitigate this threat.

To determine what other steps are immediately necessary, the Privacy Officer, in collaboration with Bread for the City's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.

a. The Confidentiality Security Team (CST), or designees, will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
b. The Privacy Officer, in collaboration with Bread for the City's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
    i. Contractual obligations
    ii. Legal obligations – Bread for the City's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
    iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
    iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
    v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
    vi. Number of individuals affected

Notification

1. The Privacy Officer will work with the department(s) involved, Bread for the City's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is

implicated. As a result, Bread for the City's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.

4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, Bread for the City will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify Bread for the City if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with Bread for the City in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If Bread for the City's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, Bread for the City will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Sanction Policy

Bread for the City will take appropriate disciplinary action against employees, contractors, or any individuals who violate Bread for the City's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Definitions

Worker means employees, volunteers, and other persons whose conduct, in the performance of work for Bread for the City, is under the direct control of Bread, whether or not they are paid by us. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive information, includes, but is not limited to, the following:

- Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.
- Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by Bread for the City.
- Payroll data – Any information related to the compensation of an individual during that individual's' employment with Bread for the City.
- Financial/accounting records – Any records related to the accounting of Bread for the City's finances or financial statements of Bread for the City.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and usable upon demand by an authorized person.
Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations and Recommended Disciplinary Actions

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1 and 2 depending on the seriousness of the violation.

In the event that a workforce member violates Bread for the City's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Important Note: The recommended disciplinary actions are listed to provide guidance and are not meant to be all-inclusive. If formal discipline is deemed necessary, Bread for the City will consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps will be followed allowing the employee to correct the behavior which caused the disciplinary action.

Level	Description of Violation	Disciplinary Action
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public are or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Using another person's computer access code (user name & password). • Failing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee. • Failing to comply with a remediation resolution or recommendation.	• Verbal (or written) reprimand • Retraining on privacy/security awareness • Retraining on Bread for the City's privacy and security policies • Retraining on the proper use of intern or required forms
2	• Second or third occurrence of any Level 1 offense (does not have to be the same offense). • Intentional unauthorized use or disclosure of sensitive information. • Refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee. • Refusing to comply with a remediation resoluti or recommendation. • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information f commercial advantage, personal gain, or malicio harm.	• Written warning or final written warning and/or suspension • Retraining on privacy/security awareness • Retraining on Bread for the City's privacy and security policies • Retraining on the proper use of intern or required forms • Termination of employment or contr • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Exceptions
Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with Bread for the City.

References
U.S. Department of Health and Human Services
Health Information Privacy. Retrieved April 24, 2009, from
http://www.hhs.gov/ocr/privacy/index.html

Information Security Acknowledgment

I, the undersigned employee contractor or volunteer, hereby acknowledge that I have read the Bread for the City Information Security Policies & Procedures and have received a copy of the Sanction Policy for Bread for the City.

I understand that any unauthorized use or disclosure of information residing on Bread for the City information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

Dated this _____ day of _____, 20____.

_____
Print Name

_____
Signature of Employee/Contractor/Volunteer