Protection of Confidential Heath Information

Supersedes:
Effective: 03-05-03

PURPOSE

Each resident of the City of Boston and citizen of the Commonwealth has a fundamental right to privacy and confidentiality in his/her relationship with health care professionals and other entities that collect, use, or maintain confidential health information.

To further its mission, BPHC collects confidential health information for treatment, and use in public health surveillance, program development and evaluation, research, and for many other public health purposes. It is critical that BPHC staff and agents who carry out these core functions recognize the importance of protecting personal privacy and safeguarding the confidentiality of information obtained by BPHC to the greatest extent possible. To this end, BPHC adopts this Policy on Protection of Confidential Health Information.

This Policy is intended to ensure that BPHC staff (hereinafter includes but not limited to, employees, volunteers, contractors, agents) complies with all relevant state and federal laws and regulations concerning the protection of confidential health information. These include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), privacy and security regulations adopted pursuant to HIPAA, the Massachusetts Fair Information Practices Act (FIPA), and Massachusetts Executive Order #412.

POLICY PRINCIPLES

This Policy is based on the following principles:

A. **Accountability**. BPHC must be responsible for providing notice of this Policy and its requirements to its employees, volunteers, contractors, agents, and approved external researchers. Access to, use of and disclosure of confidential health information should be based on a legitimate need to know.

B. **Openness**. Individuals should be given notice about how BPHC collects, uses, maintains, and discloses confidential health information.

C. **Limiting Collection**. BPHC will collect the minimum amount of confidential health information necessary to enable BPHC to implement statutory and regulatory requirements, effectively provide health care, create public awareness of factors affecting good health, or otherwise fulfill BPHC's mission.

D. **Limiting Use**. BPHC will only use confidential health information as necessary to fulfill BPHC's mission or as authorized by the client. BPHC will also limit internal access to such information only to those staff members with a need to know.

E. **Limiting Disclosure**. BPHC may disclose confidential health information when authorized by the client as necessary to fulfill BPHC's mission provided that such disclosure is not prohibited by law. Confidential health information should not be communicated externally without the authorization of the client except: 1) in accordance with applicable research protocols established by BPHC; 2) when sharing client health

information with a direct care provider of the client; 3) for payment purposes; or 4) when otherwise permitted by law or regulations.

F. **Integrity.** BPHC shall endeavor to ensure the quality, accuracy, thoroughness, and reliability of confidential health information under its control, whether in written, electronic, or other form.

G. **Individual Access**. When BPHC collects confidential health information directly from a client, he/she shall be informed, upon request and if permitted by applicable law, of its existence, use, and disclosure and shall be given access to the information.

H. **Security**. BPHC shall establish and require from staff members a high level of physical and electronic security for client confidential health information.

SCOPE

This Policy applies to all BPHC employees, contract employees, consultants, agents, business associates, and temporary employees (including interns and volunteers). For the purposes of this Policy, all such individuals shall hereafter collectively be referred to as "BPHC staff." All BPHC staff that has access to confidential health information must adhere to this Policy. This Policy may be revised from time to time as necessary to comply with applicable state and federal law or to implement BPHC policy.

DEFINITIONS

For the purposes of this Policy, the following words and phrases shall have the following meanings:

"Access" means the provision by BPHC to an individual of an opportunity to inspect or review confidential health information about that individual held by BPHC.

"Aggregate Data" means data collected from individual-level records that have been combined for statistical or analytical purposes and that are maintained in a form that does not permit the identification of individuals.

"**Authorization**" means a written voluntary agreement by client or legal representative, consenting to the use, or disclosure of confidential health information.

"Business Associate" means a person who:

on behalf of BPHC, but other than an employee of BPHC, performs, or assists in the performance of a function or activity involving the use or disclosure of confidential health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for BPHC, other than an employee of BPHC, where the provision of the service involves the disclosure of confidential health information from BPHC, to the person or organization in the Business Associate role.

"Client" means the individual about whom the data or health information relates.

"Confidential health Information" means any individually identifiable information, including, but not limited to, medical and demographic information, that:

Reveals the identity of the client or is readily identified with the client, such as, but not limited to, name, address, telephone number, social security number, health identification number, or date of birth; or provides a reasonable basis to believe that the

information could be used, either alone or in combination with other information, to identify a client; and includes any protected health information, as defined by this Policy.

"Confidentiality" means BPHC's obligation to protect the health information with which it has been entrusted.

"Contact" means to communicate or attempt to communicate with a client or the client's parent, guardian, or health care provider by any means, including, but not limited to, in-person, telephone, facsimile, letter, or electronic mail.

"Data Linkage" means a method of assembling data contained in two or more different files or records to relate significant health and other events for the same individual, organization, community, or other unit of analysis.

"De-Identified Data" means data or information that has been subject to methods for rendering information not individually identifiable, such as removal of personal identifiers including name, address, telephone number, social security number, health identification number, or date of birth.

"Disclose" means to transfer, disseminate, release, or otherwise communicate or divulge any confidential health information to any person or entity outside BPHC.

"Health Information" means any information, whether oral or recorded in any form or medium, that: is created or received by BPHC; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

"Individual-Level Data" means any data or information collected and maintained concerning a specific individual.

"Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and:

is created or received by BPHC; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Institutional Review Board" means any board, committee, or other group formally designated by an institution, and approved by the federal Health and Human Services pursuant to 45 CFR Part 46 to review, approve, and periodically evaluate research projects to protect the rights of human research subjects.

"Personal Data" means any information concerning an individual who, because of name, identifying number, mark or description can be readily associated with a particular individual, provided that such information is not contained in a public record.

"Pledge of Confidentiality" means a written statement, dated and signed by an individual who is granted access to confidential health information, that certifies the individual's agreement to abide by the confidentiality restrictions stated in the written statement.

"Privacy" means the right of an individual to control the circulation of data or information about himself or herself, freedom from unreasonable interference in an

individual's private life, and an individual's right to protection against misuse or unjustified publication of his or her personal data or information.

"Protected Health Information" means individually identifiable health information that is: 1. transmitted by electronic media; 2. maintained in any medium described in the definition of electronic media in the Privacy Regulation, or 3. is transmitted or maintained in any other form or medium. Confidential Health Information includes Protected Health Information.

"Public Health Authority" means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors of persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

"Public Health Purpose" means a population-based activity or individual effort primarily aimed at: the reduction of morbidity or mortality; the prevention of injury, illness, disease, disability or premature mortality; the improvement of health outcomes; or the promotion of health in the community, including assessing the health needs and status of the community through public health reporting and surveillance, developing public health policy, and responding to public health needs and emergencies.

"Research" means a systematic investigation designed primarily to develop or contribute to general knowledge, including public health, medical, social, demographic, and historical research**.**

"Security" means the manner of assessing the threats and risks posed to confidential health information data and taking the appropriate steps to protect that data against unintended or unauthorized access, use, intrusion, disclosure or such other dangers as accidental loss or destruction.

"Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information by BPHC.

GENERAL PRIVACY POLICY

All BPHC staff shall comply with the following policy on use and disclosure of confidential health information.

A. COMPULSORY LEGAL PROCESS

1. Except for requests by the client or the legally authorized representative of the client, any BPHC staff that receives a request for access to confidential health information in BPHC's possession or receives a subpoena, discovery request, court order or any other form of compulsory legal process to provide such confidential health information shall immediately notify the Office of the General Counsel.
2. BPHC staff shall not disclose any confidential health information unless and until authorized to do so by the Office of the General Counsel.

B. LIMITING COLLECTION OF CONFIDENTIAL HEALTH INFORMATION

1. BPHC staff shall collect no more confidential health information than is necessary for the stated purpose.
2. BPHC staff shall collect confidential health information only when such collection is:
    a. authorized by law or regulation;
    b. or when confidential health information is deemed necessary to further a public health purpose.

C. LIMITING ACCESS TO CONFIDENTIAL HEALTH INFORMATION

1. Access shall be limited to the minimum number of individuals who are reasonably necessary to conduct the public health purpose.
2. BPHC staff shall limit access to confidential health information to only those staff that have a legitimate need to access the information in order to conduct the public health purpose.

D. LIMITING USE OF CONFIDENTIAL HEALTH INFORMATION

1. BPHC staff shall limit use of confidential health information to those purposes for which the information was collected or other public health purposes permitted by law which further the mission of BPHC.
2. Whenever identifiable information is not necessary to conduct the public health purpose, the confidential health information shall be de-identified.

E. LIMITING DISCLOSURE OF CONFIDENTIAL HEALTH INFORMATION

1. BPHC staff shall limit disclosure of confidential health information to only authorized persons.
2. Authorized persons include:
    a. the client;
    b. any other person authorized by the client pursuant to a written authorization;
    c. BPHC staff that need access for a public health purpose related to public health surveillance or investigation;
    d. law enforcement officers or other persons pursuant to law or court order when approved by the Office of the General Counsel; or
    e. to any other person authorized by law to receive such information when approved by the Office of the General Counsel.
3. BPHC staff shall limit disclosure of confidential Health Information to the minimum necessary amount of confidential health information that is required to accomplish the intended purpose of the use or disclosure.

F. AGREEMENT TO MAINTAIN CONFIDENTIALITY

1. All BPHC staff shall strictly maintain the confidentiality of all individually identifiable health information held by BPHC.
2. No person having access to confidential health information shall disclose, in any manner, any confidential health information except as necessary for conducting a

legitimate public health purpose, as defined in this Policy, or when authorized by law.

3. All BPHC staff will receive education and training regarding the confidentiality and security principles addressed in this Policy and the specific procedures developed and implemented pursuant to this Policy.
4. In addition, all new employees, at the time of hire, and current BPHC staff shall sign a Pledge of Confidentiality for Employees. (Form A)
5. Independent contractors, volunteers, and interns who have access to client confidential information shall enter into a written agreement agreeing to abide by this Policy.
6. BPHC staff shall agree to maintain the confidentiality of client confidential health information even after termination of employment or other contractual obligations.
7. Each supervisor shall insure that all current BPHC Staff and new employees receive a copy this Policy.
8. Copies of signed confidentiality pledges shall be maintained by the Human Resource Department for all BPHC staff.
9. Independent Consultant and Contractors of BPHC that will have access to confidential health information must sign a Business Associate Agreement. (Form B)

G. OPENNESS

1. BPHC is committed to giving individuals notice about how it collects, uses, and discloses confidential health information.
2. BPHC's Notice of Privacy Practice will be available upon request by making a written request to the Privacy Officer, Boston Public Health Commission, 1010 Massachusetts Ave., Boston, MA 02118, or visiting BPHC web site at http://www.bphc.org. This Notice of Privacy Practice is subject to change by BPHC. (Form C)

H. INDIVIDUAL ACCESS

1. When BPHC collects confidential health information directly from the client, he/she shall be informed, if permitted by applicable law, of its existence, use, and disclosure, and the client shall be given access to the information.
2. Clients may request permission to access and/or copy confidential health information about themselves in the possession of BPHC in accordance with section VII. of this Policy.
3. BPHC staff shall take reasonable measures to verify the identity of the client prior to the disclosure of the information.
4. Any confidential health information about a person other than the client shall be redacted before disclosure of confidential health information to the client.
5. A Client shall be permitted to inquire about the accuracy and completeness of confidential health information held by BPHC and to have the confidential health information amended if appropriate as set forth in section VII of this Policy.

6. BPHC may refuse to disclose information if the disclosure, as determined in writing by a licensed health care provider or the Office of the General Counsel, could reasonably be expected to:
    a. result in immediate and grave harm to the individual's safety;
    b. the information contains references to other individuals;
    c. the disclosure could reasonably be expected to harm public health or safety; or
    d. Massachusetts or federal law prevents BPHC from disclosure of the information.
7. A client shall be permitted to request in writing to receive confidential communications from BPHC if the client states that routine methods of communication would endanger the client.
8. A client shall be permitted to receive an accounting of disclosures of his/her confidential health information unless the disclosure is related to treatment, payment, health care operation or pursuant to a valid authorization.

I. SECURITY

1. BPHC staff that have access to confidential health information shall ensure that such information is maintained in a secure manner which prevents unauthorized individuals from gaining access to such information.
2. Confidential health information maintained in an electronic format shall be stored on a password-protected and secure computer system.
3. Confidential health information shall not be left in plain view or otherwise accessible on a computer screen or in a work area when the authorized user is not present.
4. Confidential health information shall not be transmitted by email.
5. All confidential health information maintained in paper format shall be stored in locked file cabinets or other appropriate storage method which prevents unauthorized access as determined and approved by the Operations Department.
6. BPHC staff shall not attempt to exceed the scope of their authorized access to client confidential health information or attempt to circumvent any BPHC systems security measures designed to prohibit unauthorized access to client confidential health information.

J. DATA INTEGRITY

1. Every effort shall be made by BPHC staff to ensure the quality, accuracy, and reliability of the data and records under its control, whether contained in written, electronic, or other format.
2. BPHC staff will only collect confidential health information that is relevant to the purposes for which it is to be used, and will use reasonable efforts to ensure that such data is accurate, complete, and timely.
3. BPHC staff must ensure that confidential health information is protected from unauthorized modification and destruction.

4. BPHC staff shall strive to maintain the accuracy of the confidential health information held, including allowing individuals to have the opportunity to review and amend their confidential health information as set forth in section VII.

K. NON-COMPLIANCE

1. All BPHC staff is required to comply with this Policy. Any BPHC staff member who fails to comply with this Policy may be denied further access to confidential health information and may be subject to disciplinary action up to and including termination of employment.
2. BPHC staff shall immediately report to his/her supervisor any violations of this Policy.
3. BPHC staff members are protected from retaliation for reporting violations of this Policy by Massachusetts law (M.G.L. c. 149, §185).
4. BPHC may audit the use and disclosure of confidential health information by BPHC staff in order to ensure compliance with this Policy.

L. CONFIDENTIALITY PROCEDURES

1. Each BPHC Department/Program shall implement the specific procedures, guidelines and utilized the forms adopted with this Policy.
2. A BPHC Department/Program may adopt additional procedures, practices or forms which specifically address the operations of the Department/Program provided that the procedures, practices, or forms are consistent with this Policy and have been approved by the Office of the General Counsel.
3. BPHC staff shall comply with all procedures and practices adopted pursuant to this Policy.

M. RESEARCH STUDIES

1. Approval of Research Project Using Confidential Health Information
    a. BPHC staff that are conducting a research project which requires access to confidential health information held by BPHC shall consult with the Director of the Research Office to ensure that appropriate research protocols are followed.
    b. BPHC staff that are conducting a research study or other public health investigation which involves contact with clients shall consult the Director of the Research Office for approval of the contact protocol (e.g., consent, authorization forms, questionnaires, interview scripts).

2. Data Linkage
    a. If confidential health information is used for data linkage, the linked data set shall be stripped of personal identifiers and all identifiers shall be destroyed unless there is a legitimate public health purpose for retaining such identifiers.
    b. BPHC staff shall conduct data linkage projects in-house whenever possible and disclose only the linked data set without personal identifiers, other than a unique identification number, unless otherwise approved in writing by the Director of the Research Office.

3. Data Destruction for Research Purposes

a. As soon as reasonably practicable, BPHC staff shall de-identify confidential health information and destroy all identifiable information used for research purposes unless there is a legitimate public health purpose for retaining such identifiable information or retention of the information is required by law.

4. Publications and Reports

a. All reports and publications based on confidential health information shall contain only aggregate data and no personally identifiable information or information which could lead to the identification of an individual.
b. A client's personal identifiable health information shall not be published or disclosed by BPHC without proper written authorization from the client which specifically grants BPHC the authority to use her/his confidential health information for such reports and publications.
c. All aggregate data presented in such reports or publications shall comply with BPHC guidelines on cell size suppression as determined by the Director of the Research Office to ensure that individuals cannot be identified based on the data presented.
d. No maps based on confidential health information may be published or disclosed with sufficient detail so as to allow for identification of individuals.

PROCEDURE, PRACTICE & GUIDELINES

A. COLLECTING AND DISCLOSING CONFIDENTIAL HEALTH INFORMATION

1. Mail

a. BPHC staff shall take reasonable measures to ensure that confidential health information being submitted to BPHC by mail or courier service is properly addressed by the sender.
b. If any Department/Program receives mail with confidential health information which was intended for a different Department/Program, a staff member must bring the mail to the appropriate Department/Program or seal it in another envelope marked "Confidential" and send it via inter-office mail to the intended recipient or appropriate program.
c. All outgoing mail containing confidential health information must have a return address (with room number, where appropriate) and shall be stamped "Confidential." All reasonable efforts shall be made to ensure that the addressee information is complete and correct.
d. All confidential health information shall be sent in a sealed envelopes which complete conceals the content of the envelope.
e. Confidential health information should be sent by registered or certified mail or other delivery service that allows for tracking delivery and receipt of documents whenever feasible.

2. E-Mail or Other Electronic Transmission

Confidential health information shall not be transmitted by e-mail. Any other electronic transmission of confidential health information shall be in accordance with BPHC policies related to the electronic transmission of information.

3. Fax
    a. BPHC staff shall make reasonable efforts to ensure that all faxes containing confidential health information are sent to secure areas.
        i. Secure areas are those areas in which only individuals that have a need to know confidential health information have access
        ii. Contact the Operations department for guidance and/or question regarding a secure location for fax machines
    b. When sending a fax containing confidential health information, BPHC staff should call the intended recipient of confidential health information to confirm the correct fax number and ensure that the intended recipient is waiting for the transmission, or that measures are in place to ensure confidentiality of the confidential health information.
    c. A cover sheet that contains a confidentiality disclaimer must accompany all faxed documents containing confidential health information. The following language must be included in all fax coversheets used to fax confidential health information.

"These transmitted documents contain confidential information and are intended solely for use by the individual named above as the recipient. If you are not the intended recipient or such recipient's employee or agent, be aware that any disclosure, copying, distribution, or use of the contents of this transmission is prohibited. If you have received this transmission in error, please notify the sender by telephone immediately so that we may arrange to retrieve this transmission at no cost to you."

4. Hand Delivery
    a. All confidential health information must be kept under protective cover, in a sealed envelope or locked briefcase, when being transported or delivered by hand.
    b. Hand delivery shall be to the intended recipient or the intended recipient's authorized agent only.
    c. Government or BPHC issued photo identification is required for all in-person releases of confidential health information unless the identity of the recipient is known.
5. Telephone
    a. Confidential health information shall not be transmitted by telephone communication unless the intended recipient is known to the caller or the intended recipient's identity can be reasonably verified.
    b. The identity and authority of unknown persons requesting confidential health information must be verified before confidential health information is released by telephone.
    c. In the case of a health care provider, verification may be made by obtaining the caller's name and phone number and returning his/her call to confirm identity before such information is released.

d. Confidential health information containing personal identifiers (e.g., names, Social Security numbers, medical record numbers, etc.) shall not be left on any voice-mail system or with a receptionist.
e. Use of a cellular phone or public telephone to communicate confidential health information should be avoided to the greatest extent possible.
f. All telephone calls in which confidential health information is discussed must be made, to the greatest extent possible, in a secure area which limits the unauthorized disclosure of client confidential health information.
g. No confidential health information shall ever be sent via a pager.
h. Confidential health information shall not be discussed in public areas, such as, but not limited to, lobbies, elevators, and cafeterias.

B. USE OF CONFIDENTIAL HEALTH INFORMATION

1. Use Within the Department/Program
   a. A Department/Program that possesses confidential health information shall use that information only for:
      i. thespecific purpose(s) for which it was collected, which includes treatment, payment,, quality assurance;
      ii. BPHC approved research as set forth in section V of this Policy,
      iii. when required by law or
      iv. as authorized by the client.
      v. access to confidential health information shall be limited to only those persons within the Department/Program that have a “need-to-know”.
2. Use Within BPHC
   a. confidential health information held by one Department/Program shall not be shared with any other Department/Program unless authorized by the Privacy Officer, required by law when approved by the Office of the General Counsel, or authorized by the client.
3. Access Rights
   a. Every BPHC staff member, including interns, volunteers and temporary employees who will be granted access to confidential health information, must sign a Pledge of Confidentiality for Employees, Contract Employees and Interns. (Form A)
   b. Independent Contractors and agents of BPHC that will have access to confidential health information must sign a Business Associate Agreement with BPHC **prior** to receiving access to confidential health information.
   c. each Department/Program shall identify in writing a list of those staff members within the Department/Program by name or job description and shall determine the level of access to confidential health information that each BPHC staff member shall have to perform his/her duties.
      i. The list must be updated as necessary to keep it current and a copy of the list shall be given to BPHC’s Privacy Officer.

ii. The list shall contain the level of access each employee has to paper files, databases, and secure areas where confidential health information is kept.

iii. A copy of this list shall be provided to the Director of Information Services and Manager of IT Users to ensure coordinate authorized access control to electronic databases.

d. Temporary employees, interns, and volunteers shall not be granted access to confidential health information, unless first authorized by the supervisor in charge of such individuals of written approval by the Department /Program Director.

C. DESIGNATED RECORD SET, STORAGE, MAINTENANCE AND DESTRUCTION OF CONFIDENTIAL HEALTH INFORMATION

1. Designated Records Set . Pursuant to this Policy, a client's right to request access, an amendment, place restriction on access and/or request copies of his/her personal health information is limited to that health information that is maintained in Designated Record Sets, as determined by each Program.

a. Evaluation of Documentation

i. Each Program/Department must evaluate client files and determine which documents contain individually identifiable confidential health information about the client. A written policy must be developed and implemented at the program level to evaluate the documentation maintained by each program to determine those groups of confidential health records that should be categorized as Designated Record Sets.

ii. The written policy should ensure that the following information is gathered about the evaluated records:

1. Documentation type (e.g., paper medical record, Sophia database)
2. Basic content (e.g., assessments, reports,, examinations)
3. Location of the documentation (e.g., School Based Health Clinic)
4. Contact person (e.g., caseworker)

b. Documentation of Designated Record Sets

i. Documentation must be maintained that supports the Programs' assessment of its records which were reviewed in making the determination of its Designated Record Sets. Documentation may be maintained electronically or on paper.

ii. Selected records which are determined to constitute the Designated Record Set shall be separate from other client information. The Designated Record Set must be kept current and available for reference should a client request access to his/her health information, including comments that identify any information included in a Designated Record Set that the client would not have a right of access, amendment, or copies.

iii. Records contained in the Designated Record Set must be maintained for a period of at least six years.

c. Inclusions Confidential health information in all types of media (e.g., paper, oral, video, electronic, film, digital) must be considered when determining what documents shall be included in the Designated Record Set. Minimally, the following categories of records should be considered Designated Record Sets:

i. Eligibility information maintained by health plans;

ii. Enrollment records maintained by health plans;

iii. Claims records submitted to or received from health plans;

iv. Remittance Advices and records of payments;

v. Client Statements related to health condition;

vi. Claims adjudication records;

vii. Case or medical management records maintained by health plans; and

viii. Other records used by BPHC to make health related decisions about individuals.

ix. Records created and/or maintained by a Business Associate for services rendered to a BPHC program must be considered when evaluating documentation for Designated Record Sets.

x. Confidential health information specifically created and/or maintained by Business Associates, when acting on behalf of a BPHC Program, is subject to the client rights provisions as set forth in section VII. to request access to or amendment of such information in accordance with the Business Associate Agreement.

d. Exclusions Confidential health information that will not be used to make decisions about treatment of a client should not be included in a Designated Record Set. Such information may be found in many types of records that include significant information not relevant to the client, as well as information about other persons.

2. Method of Storage for Paper Copies

a. All confidential health information shall be stored in locked areas that do not allow public access, including but not limited to, secured file cabinets.

b. When the Operations Department deems it feasible, a security measure including but not limited to pass code should be installed in areas where confidential health information is kept.

c. Operations shall document all security measures used by BPHC Programs/Department, their locations and who has access and/or who has authority to grant access to such secure area.

d. To protect confidential health information, BPHC staff shall not leave confidential health information on a desk or work area when he/she is away from the desk/office, unless the area is secured from unauthorized access. (e.g., locked door).

e. BPHC staff shall not take confidential health information from a assigned secured area unless it is required for a field visit, meeting, or when otherwise necessary for work r elated purposes.

3. Storage for Electronic Copies of Confidential Health Information
    a. Confidential health information stored in a computer system shall be stored in a secure manner.
    b. Access rights to stored confidential health information shall be limited to individuals who need the information to perform their job and are limited to only that information necessary to perform their job.
    c. No BPHC staff member shall share her/his passwords with anyone other than Department/Program directors, or the Director of the IT department.
    d. The IT, IS and Operations department must be immediately notified when BPHC staff are transferred, resign or are terminated. Transferees may need different access rights at their new job.
        i. Upon termination, or resignation of a BPHC staff member's employment with BPHC, all access rights shall be promptly removed, especially if they have dial-in access.
        ii. Program/Department management, Human Resources, Operations and IT Services staff shall coordinate the date and time of the termination of the staff member's employment so that computer network access and other access to confidential health information are terminated in a timely manner.
    e. To prevent BPHC staff from inadvertently displaying confidential health information when away from their workstation, computers providing access to confidential health information shall have screen saver or a desktop log-off that is automatically activated.
    f. If confidential health information is on a stand-alone computer and not on the network, then the stand-alone computer must be in a secured area and the confidential health information must be password protected.
4. Maintenance
    a. Policies and procedures adopted in this Policy and program policies created in accordance with this Policy to protect Confidential health information which is collected, used, and stored by the program shall be enforced within each Program/Department by a data custodian appointed by the Department/Program Director and approved by the Privacy Officer.
    b. Such data custodian shall implement this Policy and other reasonable measures which are in accordance with this Policy to protect the integrity of the information.
5. Destruction
    a. Confidential health information that is no longer needed should be destroyed whenever possible, or archived, consistent with BPHC's record retention policies whichever is later. The Director of Operations shall provide each Department/Program Director with a copy of BPHC's record retention policy.

b. Upon written approval by Operations and the Privacy Officer, each program should have access to a shredder to use for disposal of all records with personal identifiers.
c. Any materials containing confidential health information that is not required to be retained (See BPHC Retention Policy) must be shredded as soon as they are no longer needed.
d. Confidential health information stored on electronic media (e.g., disk, CD, etc.) shall be completely erased or destroyed before disposal of the electronic media.

D. PROCEDURES FOR RELEASE/DISCLOSURE OF CONFIDENTIAL HEALTH INFORMATION

1. When Confidential Health Information May Be Disclosed
    a. Confidential health information may not be disclosed to non-staff members, agents or business associates of BPHC without the written authorization of the client, except for the following purposes:
        i. The disclosure is authorized by law or regulation and the Office of the General Counsel has approved such disclosure.
        ii. The disclosure is required by judicial order or other legal process, and the disclosure is approved by the Office of the General Counsel. A subpoena does not mean automatic release of confidential health information. When BPHC staff person receives a subpoena potentially related to the release of confidential health information, he or she must immediately notify his/her supervisor and the Office of the General Counsel.
        iii. The disclosure is authorized by BPHC for research which has been approved in writing by the Director of the Research Office /or a member of the Executive Administration department. A Pledge of Confidentiality must be signed and returned to BPHC by all researchers who will have access to the data before confidential health information is disclosed.
        iv. The disclosure is required for coordination of benefits or for treatment, payment or health care operations consistent with the requirements of HIPAA.
2. To Whom Confidential Health Information May Be Disclosed
    a. Confidential health information may be disclosed under the circumstances listed above to the appropriate individual authorized to receive the information for the specified purpose.
    b. Each Department/Program must develop and maintain a list which specifies to whom it releases confidential health information on a routine basis and a specific contact person to whom information is disseminated. The list should be updated as necessary and a copy of this list shall be given to BPHC's Privacy Officer.
3. Accounting of Disclosures

a. Each Department/Program must maintain a log of disclosures of confidential health information with relevant information including, at a minimum:
    i. the date of the disclosure;
    ii. to whom, by whom, and the information provided;
    iii. A brief description of the information disclose; and
    iv. Purpose or basis for disclosure.
b. These logs must be maintained in a secure manner and retained for a period no less than six years or in accordance with BPHC retention policy whichever is later.

4. Disclosure Procedures
    a. Requests for disclosure of confidential health information should be in writing unless necessary for the urgent care of an individual which makes a written request unfeasible.
    b. Each Department/Program should utilize the authorization form issued pursuant to this Policy (Form I) to document all requests for disclosure of confidential health information.
    c. Disclosure of confidential health information should be by mail or in-person delivery, whenever feasible. Disclosure shall not be made by telephone unless necessary for the urgent care of an individual.
5. Verification of Authorized. Recipient Reasonable measures must be taken to verify the identity of the client or the individual authorized by the client to receive confidential health information.
    a. When the request is made by a client, the client must present government issued photo identification before disclosing confidential health information.
    b. When the request for disclosure is made by a representative/agent of the client, no disclosure shall be made without a written authorization which specifies to whom the confidential information can be disclosed and what information shall be disclosed along with government issued photo identification.

CLIENT RIGHTS AND THE COMPLAINT PROCESS

A. CLIENT RIGHTS

1. This Policy, in accordance with the HIPAA Privacy Rule, requires that BPHC staff providing direct and indirect health care shall provide the client, upon first contact, with a copy of BPHC's Notice of Privacy, (Form C) and/or inform the Client where the Notice of Privacy is located in the facility
    a. After providing the client with a copy of BPHC's Notice of Privacy, BPHC staff shall obtain the client's written acknowledgement of receipt or opportunity to receive BPHC's Notice of Privacy Practice using the coversheet of Form D of this Policy.
    b. The executed Notice of Privacy Practices Acknowledgment Form shall be placed in the client's designated health records for a period of no less than

six years or in accordance with BPHC's retention policy, whichever is later.

2. BPHC staff shall provide clients upon written request, reasonable access to designated records sets containing confidential health information about the client, to request an amendment to the designated record set and an accounting of the disclosure or his/her confidential health information not related to treatment, payment, health operations, or pursuant to a client's authorization.
3. BPHC staff shall provide a client, upon request, the proper Form as set forth in Section IX of this policy, to request access, to request an amendment, to request a limitation to the disclosure or an accounting of disclosure of disclosure of his/her confidential health information.
4. All privacy request for access, request to amend, request to restrict disclosure and/or request for an accounting of disclosures must be documented and given the staff member's immediate supervisor.
5. BPHC shall not amend, at a client's request, any information in a record that the Program/Department knows to be true and accurate.
6. The supervisor shall forward the client's request(s) for amending, placing restrictions and an accounting of disclosure of their confidential health information to the Privacy Officer and/or his/her designee(s) within the Department.
7. The Privacy Officer shall ensure that all client requests related to this Policy are recorded accurately, and are retained for a period of at least six years from either the date of creation or the date when it was last in effect, whichever is later.
8. The Privacy Officer shall consult with a license health care provider and/or the Office of the General Counsel when necessary to determine whether to grant or deny the client's rights as set forth in Article VII, Section A2 of this Policy.

B. COMPLAINT PROCEDURE

1. When a BPHC staff member receives a complaint from a client and/ or wishes to file a complaint regarding a violation of this Policy, the staff member shall report the complaint immediately to his/her supervisor who shall report the alleged violation to the Privacy Officer or his/her designee within the Department.
2. The Privacy Officer and/or his/her designees shall respond immediately to privacy complaints that are general in nature and do not require additional research or privacy expertise.
3. The Privacy Officer shall document all the facts provided by an individual and the resolution, if any, in their information referral system.
4. The Privacy Officer shall forward all privacy complaints that require additional research to the Office of the General Counsel for resolution.
5. The documentation of all privacy complaints and the resolutions of such complaint shall be maintained by the Privacy Officer for a period of at least six years from either the date of creation or the date when it was last in effect,

whichever is later, and shall contain no individually identifiable health information other than that provided by the individual.

6. The Privacy Officer shall provide reports about privacy complaints to the Director of Administration each quarter and as requested by the Director of Administration.
7. Such report information will be used for evaluation and process and/or procedure enhancement, as appropriate.

C. IMPLEMENTATION

The Privacy Officer shall use designated a staff member within each Department that create, use or disclose protected health information to document the receipt and disposition of all written request for access, amendments to his/her designated record set and complaints alleging a violation of this Policy

CONTACT INFORMATION

Any questions concerning this Policy and/or Procedures should be directed to the Office of the General Counsel, in writing at:

Boston Public Health Commission
Office of the General Counsel
1010 Massachusetts Ave., 6th Fl.
Boston, MA 02118