Massachusetts Executive Office of
Health and Human Services

Department of Public Health

Department of Public Health Confidentiality Procedures

Revised October 1, 2012

MDPH Privacy Office
250 Washington St.
Boston, MA 02108
Privacy.DPH@state.ma.us

(Page intentionally blank)

Massachusetts Department of Public Health
Confidentiality Procedures
Table of contents

Massachusetts Department of Public Health
Confidentiality Procedures

Massachusetts Department of Public Health
Confidentiality Procedures

(Page intentionally blank)

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures

Summary of Confidentiality Procedure Changes – Change 3

Change Effective Date: October 1, 2012

Procedure	Version number	Version effective date	Summary of change
Glossary	-	10/1/2012	• Limited Data Set description updated to reflect changes to procedure 7
3	4	10/1/2012	Table 3.1 • Table updated to reflect changes to procedure 7
6	4	10/1/2012	• Procedure removed and will be rewritten
7	6	10/1/2012	• Limited Data Set Standard updated

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures

Summary of Confidentiality Procedure Changes – Change 2

Change Effective Date: June 1, 2009

Procedure	Version number	Version effective date	Summary of change
2	6	6/1/2009	• Updated to incorporate regulatory changes and new Information Technologies policies
4	4	6/1/2009	• Reformatted for plain language
10	4	6/1/2009	• Updated to reflect changes in Information Technologies policies
10A	5	6/1/2009	• Updated to reflect changes in Information Technologies policies
14	1	6/1/2009	• New procedure
CC-2	4	6/1/2009	• Updated to include confidentiality agreements.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures

Summary of Confidentiality Procedure Changes – Change 1

Change Effective Date: April 21, 2008

Procedure	Version number	Version effective date	Summary of change
1	3	4/21/2007	• Procedure edited and reformatted.
2	5	12/1/2007	• Procedure edited and reformatted.
3	3	4/21/2007	• Procedure edited and reformatted.
4	3	4/21/2007	• Procedure edited and reformatted.
5	3	4/21/2007	• Procedure edited and reformatted.
6	3	4/21/2007	• Procedure edited and reformatted.
7	5	4/21/2007	• Procedure edited and reformatted.
8	3	4/21/2007	• Procedure edited and reformatted.
9	4	4/21/2007	• Procedure edited and reformatted.
10	3	4/21/2007	• Procedure edited and reformatted.
10A	4	12/1/2007	Table 10A.1 • Procedure edited and reformatted. • Exemption added when emailing between a MDPH Hospital and representatives of the Department of Corrections
11	3	4/21/2007	• Procedure edited and reformatted.
12	3	4/21/2007	• Procedure edited and reformatted.
13	3	4/21/2007	• Procedure edited and reformatted.
CC-1	3	4/21/2007	• Procedure edited and reformatted.
CC-2	3	4/21/2007	• Procedure edited and reformatted.
CC-3	3	4/21/2007	• Procedure edited and reformatted.

(Page intentionally blank)

Glossary

For the purposes of MDPH's Confidentiality Policy and Procedures, the following words and phrases shall have the following meanings:

Access means the provision by MDPH to an individual of an opportunity to inspect or review confidential information about that individual held by the Department.

Acknowledgment means a written statement, dated and signed by all workforce members, that certifies the individual's agreement to abide by MDPH's Confidentiality Policy and Procedures.

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 the permission that a data subject or his or her personal representative gives to another person or entity allowing that person or entity to disclose the data subject's confidential information.

Breach means the use of or disclosure of confidential information in violation of applicable MDPH Confidentiality Policy and Procedures.

Business Associate (BA) means a person or entity who, on behalf of a covered component of the Department, and other than in the capacity of a workforce member, performs or assists in the performance of a function or activity that involves the use or disclosure of confidential health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services, where the provision of the service involves the use or disclosure of confidential health information.

Cell Size Suppression means a statistical method used to report aggregate data in tables that restricts or suppresses disclosure of subsets of aggregate data to protect the identity and privacy of data subjects and to avoid the risk of identification of individuals in small population groups.

Confidential Information means, unless otherwise defined by law, any individually identifiable information, including, but not limited to, medical and demographic information, that:

1. Reveals the identity of the data subject or is readily identified with the data subject, such as name, address, telephone number, social security number, health identification number, or date of birth; or
2. Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a data subject.

Confidential Information includes any protected health information, as defined by HIPAA, and any personal data, as defined by FIPA. To the extent that certain information held by the Registry of Vital records is deemed under state law to be unrestricted, this information is not confidential information for the purposes of these procedures. Nothing in the

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Glossary

Confidentiality Policy or Procedures shall be read or interpreted to restrict the disclosure of Registry information, where identifiable information is otherwise unrestricted and permitted to be disclosed.

Confidentiality means the MDPH's obligation to protect the privacy of the health and other personal information with which it is entrusted.

Consent means voluntary agreement with what is being done or proposed (express or implied).

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

Covered Health Care Component means those programs that would meet the definition of a covered entity if each were a separate legal entity. It may also include a program:

1. To the extent that it performs a covered function, but does not strictly meet the definition of a covered entity (i.e., a provider that does not transmit information electronically in connection with a covered transaction); or
2. It engages in activities that would make it a business associate of a component that performs covered functions if the two were separate legal entities.

Covered Entity (CE) means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Custodian means the program or bureau that collects and maintains data and is responsible for the use of the data in accordance with applicable laws, regulations, policies, and procedures.

Data Holder has the same meaning as under FIPA, and means an agency which collects, uses, maintains, or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part of as a result of performing a governmental or public function or purpose.

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

Data Subject means the individual about whom the data or information relate.

De-Identified Data means information that has been subject to methods for rendering it not individually identifiable, such as the removal of personal identifiers including, but not limited to, name, address, telephone number, social security number, health identification number, or all elements of dates except year relating to the individual.

Disclosure means the transfer, dissemination, release, or communication by other means of any confidential information to any person or entity outside the Department or, for a HIPAA covered component, outside the covered component.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Glossary

Electronic Confidential Information means information defined as confidential information in this glossary, which is stored or transmitted by electronic media.

Electronic media means:

1. *Electronic storage media* including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. *Transmission media* used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Faxes sent directly from one fax machine to another, person-to-person telephone calls, video teleconferencing, and messages left on voice-mail are not considered transmission media. However, any faxes sent from a computer, including those made by a fax-back system, are considered transmission media.

Electronic Transmission means the use of email and file transfer protocols to exchange information over a computer network.

Fair Information Practices Act (FIPA) means M.G.L. c. 66A, the state law protecting the confidentiality of personal data held by state agencies or entities conducting business on behalf of state agencies.

Health Information has the same meaning as under the HIPAA Privacy Regulation, and means any information, whether oral or recorded in any form or medium, that:

1. Is created or received by MDPH; and
2. 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.

Health Insurance Portability and Accountability Act (HIPAA) means the federal law passed in 1996 that was intended to reform the health insurance market and simplify many health care administrative processes. While the HIPAA legislation addresses many issues, the provisions that directly affect the Department of Public Health are contained in Title II, Subtitle F - Administrative Simplification and the regulations relating to Privacy, Security and Transactions and Code Sets, implemented pursuant to the Administrative Simplification requirements.

Hybrid Entity means MDPH as a single legal entity under HIPAA, whose business activities include both covered and non-covered functions, and that designates the covered functions to be included in its covered components. Only covered components are required to comply with HIPAA's Privacy and Security regulations. All covered and non-covered components must follow the Department's Confidentiality Policy and Procedures, except where otherwise indicated.

Indirect Treatment Relationship means a relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and

Massachusetts Department of Public Health
Confidentiality Procedures – Glossary

2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the service or products or reports to the individual.

Individual means the person who is the subject of confidential information.

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

Individually Identifiable Health Information has the same meaning as under the HIPAA Privacy Regulation and means information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by MDPH; and
2. 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 U.S. Department of Health and Human Services pursuant to 45 C.F.R. Part 46 to review, approve, and periodically evaluate research projects to protect the rights of human research subjects.

Limited Data Set means, as described in Procedure 7, confidential information that excludes specific direct identifiers of the individual, or of relatives, employers or household members of the individual, which may be disclosed for research, public health, or operations purposes, at the discretion of MDPH, if approved by the Department's Confidential Data Officer and an authorization in accordance with M.G.L. c.111, §24A is executed.

Personal Data has the same meaning as under FIPA, and means any information concerning an individual which, 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.

Personal Representative means a person authorized under state law to act on behalf of an individual (data subject). Certain information may be collected from or disclosures may be made to personal representatives if they are so authorized under Massachusetts law.

Pledge of Confidentiality means a written statement, dated and signed by an individual who is granted access to confidential 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 disclosure 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 inappropriate disclosure of his or her personal data.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Glossary

Protected Health Information has the same meaning as under the HIPAA Privacy Regulation, and means individually identifiable health information, with limited exceptions, 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.

Protected Health Information is a subset of Confidential Information.

Public Health Authority has the same meaning as under the HIPAA Privacy Regulation, and 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 or 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 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.

Public Record has the same meaning as under the Massachusetts Public Records Law, M.G.L. c. 4, § 7(26), and means all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by an officer or employee of any agency, executive office, department, board, commission, bureau, division, or authority of the Commonwealth, or of any political subdivisions thereof, or of any authority established by the general court to serve a public purpose, unless such materials or data fall within the listed exemptions.

RaDAR means the Research and Data Access Review Committee, which is the body responsible for reviewing applications for authorization of research or studies in accordance with M.G.L. c.111, §24A and for granting access to confidential MDPH data. RaDAR makes recommendations to the Commissioner for approval.

Required by Law means, with respect to confidential information, a mandate contained in law that compels an entity to make a use or disclosure of confidential information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Glossary

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

Safe Harbor Method means, as defined under the HIPAA Privacy Regulation and Procedure 7, that data are deemed to be de-identified when all specified identifiers are removed and the resulting data could not lead to the identity of any individual.

Secure File and Email Delivery System (SFED) means a system used by Commonwealth governmental agencies to ensure the security of electronic transmission of Confidential Information. The SFED system uses encryption to protect data during transmission.

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

Subpoena means a formal request to compel MDPH to produce an individual to testify or to produce documents in relation to a proceeding in which MDPH may or may not be a party to the action. A subpoena may be issued by an attorney or, in some instances, by the court. It is often accompanied by a witness fee. Failure to respond to a subpoena may result in legal sanctions.

Surveillance means the public health function of monitoring the occurrence and spread of disease and indications of such occurrence and spread.

Treatment, Payment and Health Care Operations (TPO) has the same meaning as under the HIPAA Privacy Regulation and includes the following:

- Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
- Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

Use has the same meaning as under the HIPAA Privacy Regulation, and means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information among the non-covered components and within each covered component.

Workforce Members means all employees, volunteers, interns, long-term temporary workers, trainees, and other persons whose conduct, in the performance of work for MDPH is under the direct control of MDPH, whether or not they are paid by MDPH.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 1

Procedure 1 Administrative Requirements

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes the Department's obligations related to the implementation of the Confidentiality Policy and Procedures. While the Confidentiality Policy and Procedures will be implemented generally through the Department's programs, in certain instances it may be more appropriate to implement procedures at the Bureau level. This procedure applies to both covered and non-covered components of the Department, and all workforce members.

PART II. Personnel Designations

The Department must designate and document the following:

A. Privacy Officer

The Department must designate an individual to be the privacy officer for the Department.

The privacy officer is responsible for the development and implementation of the Department's Confidentiality Policy and Procedures. Each MDPH Hospital shall also designate a privacy officer.

B. Privacy Liaisons

Each Bureau shall designate at least one contact person to serve as a liaison to collaborate with the Privacy and Data Access Office. The privacy liaisons will work with the privacy officer to help Bureaus meet and monitor compliance with the requirements of the Confidentiality Policy and Procedures. Privacy liaisons will also work with the privacy officer in resolving any complaints related to privacy and confidentiality as required in Procedure # 13.

C. Security Officer

The Department must designate an individual to be the security officer for the Department prior to the April 21, 2005 compliance date for the HIPAA Security Rule. The security officer is responsible for the development and implementation of Department-wide policies and procedures relating to the security of confidential information.

PART III. Privacy and Confidentiality Training Requirements

The Department must meet the following obligations related to training workforce members:

A. Length of employment

1. Thirty-day rule

All workforce members who will work at the Department for one month or longer or who will work at the Department for less than one month but who will have contact with confidential information must:

- Complete an online training on the Department's Confidentiality Policy and Procedures; and
- Sign the MDPH Confidentiality Acknowledgement after completing the training.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 1

Workforce members who will work at the Department for less than one month must read the Confidentiality Download.

Each new and returning workforce member shall receive training on their responsibilities under the Confidentiality Policy and Procedures within a reasonable time after starting work at the Department.

These requirements apply to all employees, volunteers, interns, long-term temporary workers, trainees, and other persons whose conduct is under the direct control of the Department, whether or not they are paid by the Department. The requirements apply despite any previous training that the workforce member may have received related to HIPAA. These training requirements are summarized in the Appendix at the end of this procedure.

2. **Exceptions:**
This requirement does not apply to employees from the Bureau of Public Health Hospitals or the State Office of Pharmacy Services (SOPS) who must complete hospital-mandated trainings or the Board of Registration in Medicine.

Individuals who are under contract to perform roles for the Department at an off-site location who have signed an appropriate pledge of confidentiality associated with a contract-specific confidentiality agreement are not required to complete this training.

Table 1.1: Training Requirements

Employment Status	Online Training Required?	Confidentiality Acknowledgement to Sign and Submit	Confidentiality Agreement and Pledge*
DPH Employee	√	Online Training Acknowledgement	
Contract Employee or Contractor Working On-Site	√	Online Training Acknowledgement	
Temporary Employee:* More than 30 days	√	Online Training Acknowledgement	
Temporary Employee:* Less than 30 days with access to Confidential Information	√	Online Training Acknowledgement	
Temporary Employee: * On-Site for less than 30 days with no access to Confidential information		Best Practices Acknowledgement	
Off-site Contractor			√
*** Temporary employee is any workforce member who is an intern, student, resident, or volunteer**			

3. **Recording training**
   The Department must document and maintain records of the successful completion of privacy and confidentiality training by workforce members.

B. Access to Confidential Information

1. **In electronic mail**
   All workforce members who have received authorization from the Privacy & Data Access Office to transmit confidential information by email must complete this online training as well as the training in the Transmission of Confidential Information prior to transmitting any information;

2. **Using secure file and electronic systems**
   All workforce members who have received authorization from the Privacy & Data Access Office to transfer confidential information through the secure file and electronic delivery (SFED) system and who have an SFED account must complete this training as well as the SFED training prior to transferring any files containing confidential information;

3. **Changes to policy or job responsibilities**
   Each workforce member whose functions are affected by a material change in the Confidentiality Policy and Procedures or by a change in position or job responsibilities must receive training within a reasonable time after the change becomes effective, and;

4. **Work-specific training**
   Workforce members who routinely have access to confidential information will receive additional confidentiality training as it relates to specific job functions.

PART IV. Safeguards for Confidential Information

Each Bureau must comply with the administrative, technical, and physical safeguards described in Procedure # 10, as well as all applicable DPH and EOHHS security policies and procedures to protect against intentional or unintentional unauthorized uses or disclosures. In addition, Department programs that are designated covered health care components under the Department's hybrid entity status must have safeguards in place to protect against unauthorized disclosures of confidential information to non-covered components within the Department.

PART V. Complaint Process

A. Submitting Complaints

All complaints regarding the Department's obligations and compliance with the Confidentiality Policy and Procedures should be directed to the MDPH privacy officer. The privacy officer will consult with the appropriate privacy liaison to investigate the complaint as described in Procedure # 13.

All complaints regarding the MDPH hospitals' obligations and compliance with their confidentiality procedures should be directed to their respective designated privacy officer. Within thirty days of receipt of the complaint, the hospital privacy liaison shall file a report with the Department's privacy officer

---

PART VI. Breaches

As described in Procedure # 2, breaches of confidential information should be reported to the privacy officer, who will coordinate the investigation process.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 1

The Department will enforce sanctions against workforce members who fail to comply with the Department's Confidentiality Policy and Procedures. Each Bureau must mitigate, to the extent feasible, any harmful effects from unauthorized uses or disclosures of confidential information by any member of the Department's workforce.

If any workforce member discovers that confidential information was disclosed in error, a written report must be timely completed to the MDPH privacy officer. The report shall include a description of what occurred, including to whom the disclosure was intended, who received the confidential information, and what was done to mitigate any harmful effects of the disclosure.

Mitigation may include, but is not limited to, contacting the individual who received the information in error and requesting that the information be returned, destroyed, and/or deleted. Supervisors shall also evaluate necessary steps to preclude future erroneous disclosures, including retraining the responsible workforce member, or restricting the member's access to confidential information.

Determination of any additional steps required to mitigate the effects of the disclosure will be accomplished through consultation with the appropriate Bureau director, the privacy officer, and the Office of the General Counsel.

PART VII. Retaliation Prohibited

No member of the Department's workforce shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her rights under the Confidentiality Policy and Procedures, or for participation in any process relating to compliance with the Policy and Procedures. Workforce members are protected from retaliation for reporting violations of the policy and procedures in accordance with M.G.L. c. 149, §185.

PART VIII. Required Policy and Procedures

The Department must document the following actions relating to the Confidentiality Policy and Procedures:

A. Policy and Procedures

The Department shall implement Confidentiality Policy and Procedures to ensure the privacy and security of confidential information. A Bureau may adopt additional procedures that specifically address its operations, provided that the procedures are consistent with Department's Policy and Procedures, and they are available for review by the Privacy & Data Access Office.

B. Changes to Policies and Procedures

The Department must revise its policy and procedures whenever necessary to conform to changes in law or regulation. The Department may also revise its policy and procedures at any time when deemed necessary to meet the needs of the Department. The Privacy Officer will provide notice to Bureau Directors and privacy liaisons whenever the Confidentiality Policy or Procedures are revised.

C. Documentation Requirements

The Department must maintain current and prior versions of the required policy and procedures and any other written documentation relating to the policy and procedures, in written or electronic form, for a period of six years from the date of creation or as required by the Records Conservation Board.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 1

PART IX. Employee Acknowledgement

All current Department workforce members and new workforce members at the time of hire shall sign a Confidentiality Acknowledgement agreeing to abide by the Department's Confidentiality Policy and Procedures. Copies of signed Confidentiality Acknowledgements shall be maintained permanently by the Human Resources Department (HRD). For workforce members that are not captured by HRD, the Bureau Director or Supervisor shall maintain the acknowledgement. Contractors and agents of the Department that will have access to confidential information must sign a confidentiality pledge or other acceptable confidentiality agreement as approved by the Privacy Officer. As stated in the Confidentiality Agreement, Department workforce members shall agree to protect confidential information from unauthorized disclosure even after termination of employment or other contractual obligations.

Authority:

M.G.L. c. 66A, §§ 2(a) and (b)

45 C.F.R. § 164.530

For further confidentiality training information: See Healthnet, look under the Privacy & Data Access pages (available to MDPH Intranet users only)

(Page intentionally blank)

Procedure 2 Breaches of Confidential Information

Version: 6 Effective Date: June 1, 2009

PART I. Purpose & definitions

A. Introduction

Federal and state laws require DPH to provide a process for individuals to lodge complaints regarding the handling of Confidential Information and to report possible violations of privacy laws and/or DPH Confidentiality Policies and Procedures. This procedure establishes a process for the public and workforce members to register complaints regarding a possible Breach of Confidentiality.

B. Purpose

This procedure:

Describes the reporting and investigation procedures for Breaches of Confidentiality;

Describes the notification procedure for Breaches of Confidentiality to Affected Individuals;

Specifies the possible disciplinary actions and Sanctions that may result from violation of DPH Confidentiality Policy and Procedures, any applicable state of federal privacy law, or failure to cooperate in any disciplinary investigation or proceeding relating to violations of law.

C. Scope

This procedure applies to both covered and non-covered components of the DPH and to all DPH workforce members.

D. Definitions

1. **Affected Individual**
   A person who's Confidential Information has been disclosed in violation of DPH Confidentiality Policy and Procedures.

2. **Breach of Confidentiality (Breach)**
   The use of or disclosure of Confidential Information in violation of applicable DPH Confidentiality Policy and Procedures.

3. **Confidential Information**
   For the purposes of this policy, any individually identifiable information, including, but not limited to, medical and demographic information that:

   Reveals the identity of the subject or is readily identified with the data subject such as name, address, telephone number, social security number, 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 data subject; and

   Includes any protected health information as defined by HIPAA, any personal data as defined by FIPA, and any personal information as defined by Chapter 93H.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 2

4. **Data Owner**
   For the purposes of this procedure, the DPH Bureau director responsible for the Confidential Information that was used or disclosed in violation of the applicable MDPH Confidentiality Policy and Procedures

5. **Disclosure of Confidential Information**
   The release, transfer, provision, access to, or divulging, in any other manner, information outside the entity holding the Confidential Information

6. **Level I Breach**
   Improper and/or Unintentional Breaches or Violations. The unintentional or careless violation of DPH Confidentiality Policy and Procedures.

   Examples include, but are not limited to unintentionally:
   - Discussing Confidential Information in public areas;
   - Leaving a copy of Client Confidential information in a public area;
   - Inadvertently faxing Confidential Information to the wrong fax number;
   - Leaving a computer unattended in an accessible area with Confidential Information unsecured;

7. **Level II Breach**
   Unauthorized Use and/or Misuse. The intentional access to or disclosure of Confidential Information that is inconsistent with DPH Confidentiality Policy and Procedures but not for personal gain.

   Examples include, but are not limited to:
   - Looking up the birth dates or addresses of friends or relatives
   - Disclosing Confidential Information to someone known to be without appropriate authorization
   - Reviewing a public personality's Confidential Information
   - Accessing and reviewing Confidential Information out of curiosity or concern

8. **Level III Breach**
   Willful and/or Intentional Disclosures or Violations. Access to, review, or disclosure of Confidential Information for personal gain or malicious intent.

   Examples include, but are not limited to:
   - Using or disclosing Confidential Information for commercial advantage or to improve one's position
   - Using or disclosing Confidential Information for harassment or to spread gossip

9. **Sanction**
   A penalty imposed upon finding that a person is responsible for a breach.

10. **Security Incident**
    Internally or externally initiated events, intentional or accidental, that threaten or exploit an unauthorized and/or illegal use of Commonwealth electronic information systems and/or services. Such events include, but are not limited to, a criminal use of Commonwealth systems and/or services as well as disclosure, destruction, and/or alteration of state-managed systems or data. This may or may not involve a Breach of Confidential Information.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 2

PART II. Reporting & investigation protocols

A. Breach of Confidentiality Reporting Protocol – Workforce Member

The reporting protocol for the Breach of Confidentiality identified by a DPH workforce member organized by involved party is described in table 2.1.

Table 2.1: Breach course of action

Reporting Individual (Workforce Member)	Reporting Individual's Supervisor	Privacy Officer
1) Observes Breach of Confidentiality.		
2) Immediately informs supervisor.	3) Instructs reporting individual to complete an incident report.	
4) Completes incident report on same business day and faxes to privacy officer, 617.624.5234	5) Contacts privacy officer on same business day.	6) Contacts reporting individual to obtain additional details about Breach on same day.
		7) Contacts Data Owner to initiate investigation procedure within one business day.

B. Obligation to Report Breaches of Confidentiality

A workforce member who is responsible for a Breach of Confidentiality or who is aware of such a Breach must immediately report it to his or her supervisor. Failure to report a Breach of Confidentiality of which the workforce member has knowledge may result in disciplinary action.

C. Policy of No Retaliation for Good Faith Reporting

- A workforce member who makes a report in good faith of a suspected or actual violation will not be retaliated against for making the report.
- Reporting a Breach of Confidentiality in bad faith or for malicious reasons are grounds for disciplinary action.

D. Breach of Confidentiality Reporting Protocol – General Public

The reporting protocol for the Breach of Confidentiality identified by a member of the general public organized by involved party is described in table 2.2.

Table 2.2: Breach reporting protocol

Reporting Individual (General Public)	DPH Workforce Member Receiving Information	Privacy Officer
1) Relays information to DPH workforce member or privacy officer.	2) Takes contact information from individual and informs the privacy officer within one business day.	3) Contacts reporting individual, obtains additional details as necessary, and documents information about the Breach on a privacy complaint form within one business day.
		4) Contacts data owner to initiate investigation protocol within one business day.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 2

E. Breach of Confidentiality Investigation Protocol

The investigation protocol for Breaches of Confidentiality organized by DPH function is described in table 2.3.

Table 2.3: Breach investigation protocol

<table>
<tr><th>Data Owner</th><th>Privacy Officer</th><th>Office of General Counsel, Senior Management</th><th>Human Resources</th></tr>
<tr><td colspan="2">1) Evaluate mitigation steps.</td><td></td><td></td></tr>
<tr><td colspan="2">2) Determine whether the Office of the General Counsel and/or senior management are required.</td><td></td><td></td></tr>
<tr><td colspan="2">3) Notify Human Resources of the reported incident.</td><td></td><td></td></tr>
<tr><td colspan="2">4) Assign responsibilities for investigating and validating facts included in the incident report.</td><td colspan="2">[Participates as appropriate]</td></tr>
<tr><td colspan="2">5) Review investigation materials and make findings.</td><td colspan="2">[Participates as appropriate]</td></tr>
<tr><td></td><td>6) Convene Breach Response Team as appropriate (see Section F).</td><td colspan="2"></td></tr>
<tr><td></td><td>7) Determine whether any intra-governmental notifications are required (see Section H) and follow through as required.</td><td colspan="2">8) Recommend an appropriate Sanction (see “Sanctions Against Workforce Members Committing Breaches of Confidentiality”).</td></tr>
<tr><td></td><td></td><td></td><td>9) Provide the sanctioned workforce member with a notice of the finding and the recommended Sanction in accordance with Civil Service or collective bargaining procedures, if applicable.</td></tr>
<tr><td></td><td colspan="3">10) Document the investigation in accordance with Department policies and applicable laws.</td></tr>
</table>

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 2

F. Convening a Breach Response Team

The privacy officer shall convene a Breach Response Team as s/he determines necessary. The members of the Breach Response Team shall consist of:

- The DPH privacy officer;
- The director of the Privacy & Data Access Office;
- The DPH security officer;
- The director, Public Health Strategies & Communications; and
- Other individuals as appropriate to the specific situation.

G. Responsibilities of the Breach Response Team

The responsibilities of the Breach Response Team are as follows:

As appropriate to the situation:

- Develop and oversee a mitigation plan;
- Develop and oversee the notification of Affected Individuals; and
- Coordinate internal and external communication.

H. Intra-Governmental Notification Requirements

Pursuant to Chapter 93H, Executive Order 504, and the Enterprise Cyber crime & Security Incident Response Policy and Procedures, the following Intra-Governmental notifications are required for breaches meeting the criteria outlined in table 2.4.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 2

Table 2.4: Breach notification requirements

Nature of Breach	Departments to be Notified	Contents of Notification
Unauthorized acquisition or unauthorized use of unencrypted data or encrypted data with the key that involves a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account (Chapter 93H)	• Office of Consumer Affairs and Regulation • Attorney General	• A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information • The number of Massachusetts residents affected as of the time of notification • The steps already taken relative to the incident • Any steps intended to be taken relative to the incident subsequent to notification • Information regarding whether law enforcement is engaged investigating the incident.
	• ITD • Department of Public Records	• Written notification of the nature and circumstances of the breach or unauthorized acquisition or use
Security Incident (ITD Enterprise Cybercrime & Security Incident Response Policy and Procedures)	CommonHelp (866) 888-2808	• Date • Name of person reporting Incident • Agency MMARS Code • Date/Time CommonHelp was contacted (Include ticket number) • Date/Time/Person at Agency contacted • Description of threat or incident • Whether the incident is continuing • How the incident began • IT assets being compromised, including identification and classification (i.e., level of confidentiality) of affected data or systems • Whether DPH has determined the cause and origination of the incident • A list of the actions which must be and/or have been taken and the resources required to stop and/or remedy the incident • The steps taken to mitigate or remediate the damage • Evidence available to assist in the investigation (e.g., log files)

PART III. Notification of Affected Individuals

A. Notification of Affected Individuals

The notification of Affected Individuals is made on a case-by-case basis in consideration of the following factors:

1. **Federal or Massachusetts Regulations Requiring Notification.**
   DPH shall comply with all applicable state and federal requirements including Chapter 93H.

2. **Risk of Identity Theft.**
   Does the Breach of Confidentiality put the Affected Individual(s) at risk of identity theft or other fraud? This is a concern if the Breach of Confidentiality includes unencrypted information such as first and last names in conjunction with Social Security Numbers, medical record numbers, or other information that can be used for fraud by third parties.

3. **Risk of Further Damage.**
   Will notification potentially compound the problem by increasing awareness of breached sensitive information?

4. **Risk of Physical Harm.**
   Does the loss of information place any Affected Individual at risk of physical harm or harassment? Does the loss of information put the public health of any segment of the population at risk?

5. **Risk of Humiliation or Damage to Reputation to Individual.**
   This type of harm can occur with the loss of information such as behavioral health, medical, or personnel records.

6. **Risk of Humiliation or Damage to Reputation to DPH.**
   Could the loss of information result in damage to the reputation to the Department, the loss of trust in one or more of its programs, the loss of its assets, or put it at risk for a lawsuit or legal claim?

7. **Risk of Loss of Business or Employment Opportunities.**
   Could the loss of information result in damage to the reputation to an Individual, affecting business or employment opportunities?

   Notifications of Affected Individuals require approval from the Office of the Commissioner.

B. Method for Contacting Affected Individuals

The appropriate Bureau director, in collaboration with the director of the Privacy & Data Access Office, the privacy officer, the Office of the General Counsel, the Communications Department, the Commissioner's Office, and others as appropriate, shall determine the method for contacting the Affected Individuals based on the nature of the Breach, applicable state and federal requirements, the number of Affected Individuals involved, and the availability of contact information.

C. Contents of Written Notification

The Department shall determine the elements contained in the notification based on:

- The nature of the Breach; and
- Applicable regulatory and statutory requirements.

PART IV. Sanctions

A. Sanctions Against Workforce Members Committing Breaches of Confidentiality

DPH is strongly committed to ensuring that workforce members perform their duties in a professional manner that protects the confidentiality of information. Nothing in this procedure, however, should be construed to contain binding terms and conditions of employment or to construe a contract between DPH and its workforce members.

Sanctions against workforce members committing a Breach of Confidentiality will be handled in accordance with applicable laws, collective bargaining units, civil service regulations, and DPH procedures depending on the classification of workforce member being disciplined. Additionally, the type of Sanction will depend on the intent of the individual and the severity of the violation. Sanctions shall be proportionate to the severity of noncompliance and may reflect, among other things, the extent to which non-compliance affects the confidentiality of the information, the workforce member's awareness of non-compliance, and the past record of the workforce member with respect to non-compliance as well as other work history.

B. Range of Sanctions

As described in "Sanctions Against Workforce Members Committing Breaches," the Sanction levied is determined on a case-by-case basis taking into account factors including, but not limited to, the specific facts surrounding the incident and any mitigating or aggravating circumstances. Table 2.5 is intended to assist the Department in the consistent application of Sanctions.

Table 2.5: Range of Sanctions

Level of Breach of Confidentiality	Recommended Range of Sanctions
Improper and/or Unintentional Breaches or Violations	• Documentation by supervisor of first-time offense which, using discretion, does not warrant an official verbal warning • Verbal warning • Written warning • Retraining Note: The recurring violation of same Breach may warrant a more severe Sanction. Repeated Breaches of Group I violations may be treated as a Group II or III breach.
Unauthorized Use and/or Misuse	• Written warning • Suspension • Retraining Note: The recurring violation of same breach may warrant a more severe Sanction. Repeated Breaches of Group II violations may be treated as a Group III Breach.
Willful and/or Intentional Disclosures or Violations	• Suspension • Termination

Authority:

M.G.L. c. 66A, § 2(b)

45 C.F.R. § 164.530(e)

M.G.L. c. 93H

Executive Order 504

Procedure 3 Use and Disclosure of Confidential Information

Version: 4 Effective Date: October 1, 2012

PART I. Purpose & Definitions

A. Purpose

This procedure describes:

- The limited circumstances under which bureaus and programs may collect, Use, and Disclose Confidential Information;
- MDPH's Minimum Necessary standard;
- MDPH's Role-Based Access standard; and
- Bureau and data liaison responsibilities under this procedure.

B. Scope

This procedure applies to:

MDPH covered and non-covered components

MDPH workforce members

C. Definitions

Confidential Information - unless otherwise defined by law, any individually identifiable information, including, but not limited to, medical and demographic information, that:

1. Reveals the identity of the Data Subject or is readily identified with the Data Subject, such as name, address, telephone number, social security number, health identification number, or date of birth; or
2. Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a Data Subject.

Data Subject - the individual about whom the data or information relate.

Disclosure - the transfer, dissemination, release, or communication by other means of any Confidential Information to any person or entity outside MDPH or, for an MDPH covered component, outside the covered component.

Health Care Oversight Agency – a government agency or its designated authority authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Examples: Massachusetts Department of Public Health
Centers for Medicare and Medicaid Services

Minimum Necessary - The least amount of information required to accomplish the business objective.

Public Health Authority – a government agency or its authority that is responsible for public health matters as part of its official mandate.

Examples: Massachusetts Department of Public Health
Centers for Disease Control & Prevention

Role-Based Access - Access to the exact amount of Confidential Information needed – no more and no less – to perform a workforce member's job duties.

Use - with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information among the non-covered components and within each covered component.

PART II. The Collection of Confidential Information

A. Policy

MDPH workforce members may collect Confidential Information only when:

1. Consistent with law or regulation
2. Authorized by the Data Subject based on a valid authorization (this is described in Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information)
3. Submitted by the Data Subject to receive services or benefits offered or funded by the Department

   Note: If submitted by the Data Subject's personal representative, follow Procedure 9, Verification of Individuals or Entities Requesting Disclosure of Confidential Information.
4. Submitted to the Department for research purposes in accordance with M.G.L. c. 111, § 24A
5. Submitted by a vendor in relation to a contract with MDPH

B. Unauthorized Receipt of Confidential Information

Bureaus must develop procedures for receiving Confidential Information that:

- The bureau is not authorized to receive; and
- Is in excess of the Minimum Necessary to achieve the intended business purpose (see Section V.A for a description of "Minimum Necessary.)

At minimum, the procedure should contain provisions for:

- Informing the disclosing party that the Confidential Information should not have been disclosed;
- Working with the disclosing party to determine what to do with the Confidential Information, for example, destroying it or returning it to the disclosing party; and
- Preventing a reoccurrence in the future.

PART III. The Use of Confidential Information

A. Expanded Definition of "Use"

"Use" means access to or the release of Confidential Information:

- From a non-covered component to a covered component within MDPH;
- From a non-covered component to a non-covered component within MDPH;
- Within a non-covered component; or
- Within a covered component.

B. When Confidential Information May Be Used

1. When authorized by law or regulation
2. When consistent with the intent of a law or regulation that required or authorized the Use;
3. When authorized in writing by the Data Subject based on a valid authorization (this is described in Procedure 4, Authorizations for the Use and Disclosure of Confidential Information);
4. For research or scientific studies approved by the Commissioner in accordance with MGL c. 111, § 24A, or other statutes authorizing public health research.
5. For program evaluation; quality improvement; payment verification; public health investigation, surveillance, or intervention; or other health care operations provided that an MDPH Intra-Department Data Use Agreement is executed between the data custodian and the program that needs the data and a copy is filed with the Confidential Data Officer.

C. When Confidential Information May Not be Used

Confidential Information may not be used:

1. In any way that conflicts with restrictions made by the Data Subject on an authorization or consent form.
2. By MDPH workforce members for their own purposes.

   Example: Independent research without meeting the requirements specified in Procedure # 6; and

3. By MDPH workforce members for their own purposes after leaving the workforce unless approved to do so in accordance with MDPH Confidentiality Policy and Procedures.

PART IV. The Disclosure of Confidential Information

A. Expanded Definition of "Disclosure"

"Disclosure" means the release of Confidential Information:

- From a covered component within MDPH to another covered component within MDPH;
- From a covered component within MDPH to a non-covered component within MDPH;
- From a non-covered component to a third-party outside MDPH; or
- From a covered component to a third-party outside MDPH.

B. Summary of Permitted Disclosures of Confidential Information

Table 3.1 summarizes permitted Disclosures and any required supporting documentation. In some instances, the Disclosure is described in more detail in other MDPH Confidentiality Procedures; these are cited.

Workforce members processing disclosures should adhere to Procedures #12 Accounting for Disclosures and #9 Verification of Individuals or Entities Requesting Disclosure of Confidential Information.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 3

Table 3.1: Permitted Disclosures of Confidential Information

To whom	Nature of Disclosure	Authority or Documentation Required & Whom Completed by	Referenced Procedure
As directed by Data Subject	Confidential Information relating to Data Subject	Valid authorization form completed by Data Subject or his/her personal representative submitted to data holder	4
Vital Record Requestor	Identifiable vital record information considered unrestricted in accordance with applicable laws in M.G.L. c 46 and disclosed by the Registry of Vital Records and Statistics	Request submitted to Vital Statistics by the record requestor	
Another MDPH Program	Confidential Information related to program evaluation, quality improvement, payment verification, public health investigation, surveillance or intervention, or other health care operations	MDPH Intra-Department Data Use Agreement executed between data custodian and program needing data; copy submitted to confidential data officer	
Another EOHHS agency pursuant to 101 CMR 16.00	Confidential client Information related to: • Administration of agency programs; • Eligibility determinations or benefit amounts; • Helping clients obtain services; • Improve coordination or management of services; • Quality assurance activities; • Serving the interests of agencies' clients; • Other circumstances that improve the provision of services	Appendix B submitted by data requestor to confidential data officer	MOU for Data-Sharing Between and Among EOHHS and its Constituent Agencies
Public Health Authority	Confidential Information necessary for preventing or controlling disease, injury, or disability; reporting vital records, federal grant compliance; conducting public health surveillance, investigations, or interventions.	The disclosure must have underlying authority in a statute or regulation. No documentation required	
Healthcare Oversight Agency	Confidential Information necessary to conduct audits; civil and criminal investigations and proceedings; inspections; and licensure and certification actions. The disclosure must have underlying authority in a statute or regulation.	The disclosure must have underlying authority in a statute or regulation. No documentation required	
MDPH Vendor	Confidential Information pursuant to the contract between the vendor and MDPH	Covered Components: Business Associate Agreement Non-Covered Components: Confidentiality Agreement • Executed between MDPH and vendor	CC-2
Public Health Evaluator	Partially De-identified Confidential Information for public health purposes or health care operations	Application for access to confidential data completed by a public health evaluator and submitted through IRBNet for review by the confidential data officer for approval in accordance with MGL c.111, §24A.	7
Researcher	Individually identifiable data or partially de-identified data for research or scientific studies pursuant to MGL c. 111 §24A or other statutes authorizing public health research as authorized by the Commissioner of DPH	24A approval letter co-signed by the Principal Investigator. Pledge of Confidentiality submitted for each research project participant with access to Confidential Information.	6
Individual or court specified in a court order or other legal process	Confidential Information belonging to a Data Subject(s) specified in a judicial order or other legal process	Valid Authorization Form completed by Data Subject or his/her personal representative submitted to data holder or court order after notice to Data Subject	5
As required by law	Required or authorized by law or regulation Example: Report of elder or child abuse	None required	

PART V. Minimum Necessary

A. Minimum Necessary Standard

The amount of Confidential Information collected, used, and disclosed by authorized persons is limited to the Minimum Necessary to complete his/her job function(s).

Bureaus are responsible for determining the Minimum Necessary Confidential Information required to accomplish a job function.

B. How to Determine the Minimum Necessary

Consider the following when determining the Minimum Necessary Confidential Information required for collection, Use, and Disclosure:

- Statutory or regulatory requirements
- The scope of the authorization
- The grant specifications provided there is underlying legal authority

Under some circumstances and at their discretion, bureaus may also rely on the judgment of the requesting party as to what constitutes "Minimum Necessary." Refer to table 3.2.

Table 3.2: Determining Minimum Necessary

Party Making Request	Purpose of Request
A public official, as permitted under 45 C.F.R § 164.512	Public health reporting
Health care provider	Treatment, payment, or operations
U.S. Department of Health & Human Services	Conduct a privacy investigation

C. Bureau-Specific Minimum Necessary Procedures

Bureaus must develop Minimum Necessary procedures for the following categories of Disclosures

Table 3.3: Minimum Necessary Documentation

Disclosure Type	Documentation Required
Routine and Recurring	A list or matrix that describes: • The Minimum Necessary elements to be disclosed • The purpose of the Disclosure • The recipient of the Disclosure
Non-Routine	Procedures for reviewing and approving non-routine Disclosures to ensure the Minimum Necessary Standard is met.

PART VI. Role-based Access

A. Role-Based Access Standard

A workforce member's access to Confidential Information is limited to the information needed to perform his/her job responsibilities and to which s/he is permitted access rights.

B. Restriction on Access for Temporary Employees, Interns, and Volunteers

Access to Confidential Information by a temporary employee, intern, or volunteer requires the approval of his/her supervisor and the completion of the advanced training related to Confidential Information.

C. Role-Based Access Workforce Member List

Each bureau is responsible for the development of a Role-Based Access Workforce Member List and the designation of individual(s) who can approve access.

D. Content of Role-Based Access Workforce Member List

The Role-Based Access Workforce Member List must contain the following elements:

- Workforce member name*
- Job title or function(s)
- Name and location of data accessed
- Workforce member's access level and rights
- Time or frequency of access
- Access and authentication controls

*Organize the list by job title or function(s) only if:

1. all workforce members within that title or function have identical access privileges; and
2. the bureau can identify all workforce members by name within that title or function

E. Updating the Role-Based Access Workforce Member List

The bureau data liaison is responsible for updating the Role-Based Access Workforce Member List. The list should be updated to reflect:

1. Employment terminations
2. Change in job responsibilities
3. Addition of new workforce members, job titles, or functions

---

PART VII. Bureau & Data Liaison Responsibilities

A. Bureau Responsibilities

1. Developing the following procedures:
   - Handling the Receipt of Unauthorized Confidential Information
   - Recording Disclosures of Confidential Information
   - Minimum Necessary Procedures for Routine and Recurring Disclosures
   - Minimum Necessary Procedures for Non-Routine Disclosures
2. Determining the Minimum Necessary Confidential Information required to accomplish a job function
3. Developing a Role-Based Access Workforce Member List

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 3

B. Data Liaison Responsibilities

Updating the Role-Based Access Workforce Member List.

Authority:

M.G.L. c. 66A, § 2

45 C.F.R § 164.502(e) and 164.506-512

(Page intentionally blank)

Procedure 4 Authorizations for the Use and Disclosure of Confidential Information

Version: 4 Effective Date: June 1, 2009

PART I. Purpose and definitions

This procedure describes DPH policies and procedures governing the use of Authorization Forms as well as their content.

A. Definitions

1. **Authorization**
   The permission that a data subject or his or her personal representative gives to another person or entity allowing that person or entity to disclose the data subject's confidential information.

2. **Authorization Form**
   The form signed by a data subject or his/her Personal Representative allowing another entity to disclose the data subject's confidential information unless subject to other legal restrictions or requirements.

3. **Covered Component**
   Those DPH programs that would meet the definition of a covered entity if each were a separate legal entity. For the purposes of this procedure, this includes the DPH hospitals, the State Office of Pharmacy Services, and the Childhood Blood Lead Laboratory.

4. **Disclosure**
   The transfer, dissemination, release, or communication by other means of any confidential information to any person or entity outside the Department or, for a HIPAA Covered Component, outside the Covered Component.

5. **Personal Representative**
   A person authorized under state law to act on behalf of an individual (data subject). Examples include parents, legal guardians of minors, and court-appointed guardians.

6. **Psychotherapy Notes**
   Notes recorded in any medium by a mental health professional documenting or analyzing the content of conversations during a private, group, joint, or family counseling session that are separated from the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the client's diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

7. **Use**
   With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information among the non-covered components and within each Covered Component.

B. Scope

- DPH Covered and non-covered Components
- DPH workforce members.

PART II. MDPH Authorization Forms: General Requirements

Follow the guidelines contained in table 4.1 when deciding which authorization form to utilize.

Table 4.1: General Requirements

If the Bureau/Program is ….	Then it should ….
Requesting Confidential Information	Use an Authorization Form with the Core Elements described in Section III below. Note: Bureaus and Programs may use the DPH model Authorization Form or, in consultation with the Office of the General Counsel, develop Authorization Forms containing, at a minimum, these Core Elements. Any Bureau/Program-specific Authorization Form must be made available to the Privacy & Data Access Office upon request.
Requesting Confidential Information from a HIPAA-covered entity	Use an Authorization Form with each of the Core Elements
Providing Authorization Forms to a vendor	Provide Authorization Forms with each of the Core Elements
Providing constituent data in response to legislator request	Obtain a valid Authorization Form containing each of the Core Elements from the constituent

PART III. The Authorization Form

A. Core Elements of a Valid Authorization Form

A valid Authorization Form contains the following ten elements:

1. A specific and meaningful *description of the information* to be used.
   Example: My medical records for my cancer treatment.
2. The name or other specific identification of the category of *person or person(s) authorized to make the requested Use or Disclosure*.
   Example: Dr. John Smith; South Shore Hospital; Harvard School of Public Health Epidemiology Department
3. The name or other specific identification of the category of *person or person(s) to whom the requested Use or Disclosure may be made*.
   Example: Dr. John Smith; South Shore Hospital; Harvard School of Public Health Epidemiology Department
4. A description of *the purpose of the Disclosure* or, if the data subject chooses not to state a purpose, a statement to that effect.
5. An *expiration date* or expiration event.
   Example: The end of the research study
6. A statement regarding the *data subject's right to revoke* the Authorization in writing, including a description of the process for doing so. It must also include a

statement that information previously released based on the Authorization is not affected by the revocation.

7. A statement regarding *the conditioning of the Authorization*. Generally, the provision of treatment, payment, enrollment, or eligibility for benefits cannot be conditioned on signing the Authorization Form. Research-related treatment, health plan enrollment, the determination of eligibility for benefits, or the provision of health care that is solely for the purpose of creating confidential health information for disclosure to a third party may be conditioned on signing an Authorization Form.
8. A statement that there is potential for information disclosed pursuant to the Authorization to be *subject to redisclosure* by the recipient, who may not be subject to state or federal privacy laws.
9. The *signature of the data subject* or his/her Authorized Representative and the date.
10. If the Authorization Form is signed by an Authorized Representative of the data subject, *a description of the Authorized Representative's authority* to act on the data subject's behalf.
    Example: Parent.

B. The Use of Photocopied Authorization Forms

The use of an original Authorization Form is preferable, but a clear and legible photocopy or fax is acceptable for the Disclosure of confidential information.

C. Record Retention

When DPH releases or uses confidential information because of an Authorization Form it has received, it must keep a copy of the Form.

All Authorization Forms must be kept for a minimum of six years or as required by the Massachusetts Records Conservation Board (MCRB). Information related to the MCRB is available at http://www.sec.state.ma.us/arc/arcrcb/rcbidx.htm.

D. Links to DPH Model Authorization Forms

English:

http://www.mass.gov/Eeohhs2/docs/dph/privacy/model_authorization_eng.pdf

Spanish:

http://www.mass.gov/Eeohhs2/docs/dph/privacy/model_authorization_span.doc

PART IV. Processing Requests for Confidential Information

A. Covered Component Release Process

DPH Covered Components should follow the process outlined in table 4.2 when presented with a request to release confidential information.

Table 4.2: Covered Component Release Request Protocol

Step	Action
1	Verify the identity of the requesting individual as described in Procedure 9, Verification of Individuals or Entities Requesting Disclosure of Confidential Information.
2	Verify that the Authorization Form contains all ten core elements and is fully completed.

3	Verify that the Authorization Form has not expired or has not been revoked.
4	Verify that the Authorization is not improperly conditioned. Generally, the provision of treatment, payment, enrollment, or eligibility for benefits cannot be conditioned on signing the Authorization Form. Research-related treatment, health plan enrollment, the determination of eligibility for benefits, or the provision of health care that is solely for the purpose of creating confidential health information for disclosure to a third party may be conditioned on signing an Authorization Form.
5	Verify that the Authorization Form is not incorrectly combined with another Authorization Form. An example of an incorrect combination is psychotherapy notes or a precondition -- circumstances requiring separate Authorization Forms (see Part IV E and F).
6	Verify that the Authorization Form is properly signed by the data subject or his/her Authorized Representative.
7	Verify that the Authorization Form does not contain any information that is known to be false.
8	Release only the information requested on the Authorization Form.
9	Document the release in accordance with Bureau/Program procedures and keep a copy of the Authorization Form.

B. Non-Covered Component Release Process

Non-covered components are strongly encouraged to require Authorization Forms that contain the core elements. They do, however, retain the discretion to release confidential information in response to an Authorization Form that does not meet this standard. The Bureau/Program director must review and approve these requests for the release of confidential information. Non-Covered Components should follow the process outlined in table 4.3 when presented with a request to release confidential information

Table 4.3: Non-Covered Component Release Request Protocol

Step	Action
1	The Bureau/Program adopts guidelines for the release of confidential information which are consistent with FIPA. FIPA requires that the data subject approves the release. No further standards are specified. These guidelines are made available to the Privacy & Data Access Office upon request.
2	These guidelines are made available to the Privacy & Data Access Office upon request.
3	The Bureau/Program receives an Authorization Form from a requestor.
4	Does the Bureau/Program director or designee decide to honor the Authorization Form? Yes? Go to Step 5. No? End of process.
5	The identity of the requesting individual is verified as described in Procedure 9, Verification of Individuals or Entities Requesting Disclosure of Confidential Information.
6	The Bureau/Program releases only the information requested on the

	Authorization Form.
7	The rationale for honoring the Authorization Form is documented in writing and maintained with a copy of the Authorization Form.
8	Document the release in accordance with Bureau/Program procedures.

C. Requests for Information Held by Multiple Programs

When requests for Information held by multiple Bureaus are received, Bureaus shall follow the process outlined in table 4.4.

Table 4.4: Multiple Bureau Release Request Protocol

If the Information Involves…	Coordinates the Release
Information held by multiple Bureaus/Programs	The Bureau/Program maintaining the most records, with coordination at times through the Office of the General Counsel
Both MDPH Covered and non-covered Components	The Privacy & Data Access Office, with coordination at times through the Office of the General Counsel
Department-wide	The Office of the General Counsel

PART V. Special Rules Governing Authorizations & Authorization Forms

A. Research

An Authorization Form for a research study may be combined with an informed consent form for the same research study.

B. HIV/AIDS Records

Information regarding the release of HIV/AIDS diagnosis or HIV/AIDS treatment is protected by M.G.L. c 111, Section 70F. No healthcare facility may release such records without separate informed consent that must be distinguished from the Authorization Form for the release of any other medical information. HIV/AIDS diagnosis and treatment information cannot be released without a specific Authorization, separately acknowledged, or the use of a separate Authorization Form.

C. Genetic Information

Information regarding the release of genetic information is protected by M.G.L. c 111, Section 70G. No healthcare facility may release such records without separate informed consent that must be distinguished from the Authorization Form for the release of any other medical information. Genetic information cannot be released without a specific Authorization, separately acknowledged, or the use of a separate Authorization Form.

D. Substance Abuse Information

Records that contain information about alcohol and drug treatment are protected by 42 C.F.R. Part 2. The federal standards for the release of records containing information about alcohol or drug treatment are very specific. Such information shall not be released without specific Authorization, separately acknowledged, or the use of a separate Authorization Form. Any Authorization Form for information

concerning alcohol or drug treatment must also include a separate notice prohibiting the redisclosure of confidential information.

E. Psychotherapy Notes

A separate Authorization Form is required for the Use and Disclosure of Psychotherapy Notes.

F. Pre-Conditions

An Authorization Form that a covered entity has required as a condition for treatment, payment, eligibility, or enrollment in a health plan cannot be combined with another Authorization Form.

Authority:

45 C.F.R §§ 164.508 and 164.532 (a) - (c)
M.G.L. c 66A § 2 (c)

Procedure 5 Subpoenas or Court Orders

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure establishes uniform standards for responding to subpoenas[1] and court orders and ensuring that confidential information/personal data related to data subjects is not released without the authorization of the data subject when sought pursuant to a subpoena or court order.[2]

As described in section IV, the Fair Information Practices Act (FIPA) establishes a stricter standard for the release of information pursuant to a subpoena than does the Health Insurance Portability and Accountability Act (HIPAA). The FIPA standard will be followed by all parts of the Department responding to subpoenas, regardless of whether the Bureau or program is a covered health care component under HIPAA.

Procedure 5 applies to both covered and non-covered components of the Department and all Department workforce members.

PART II. Procedure for Responding to Subpoenas and Court Orders

A. Model letters available on Healthnet

Sample letters referenced in this procedure may be found on HealthNet. If a sample letter corresponds to a particular section of this procedure it will be referenced as "Sample Letter #___." (http://healthnet.dph.state.ma.us/privsec/forms/forms.htm - *Available to MDPH Intranet users only*)

B. Contact the Office of General Counsel

Upon receipt of a subpoena or court order for DPH data, notify the MDPH attorney assigned to the program that received the subpoena. The only exception to this rule is if there is an established protocol, described in section III.

C. Determine if the Subpoena or Court Order Seeks Personal Data

With the assistance of the Office of General Counsel determine whether the subpoena or court order seeks personal data subject to FIPA or whether the information constitutes a public record. Information that constitutes a public record may be released see *Sample-Letter 1*. The keeper of the records from the DPH program should certify the records, either using *Sample-Letter 1* or the certification provided by the attorney.

D. Determine if the Subpoena includes an Appropriate Authorization from Data Subject

If the subpoena seeks personal data, determine if it is accompanied by an authorization for the release of personal data that complies with Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information. If there is a

[1] Subpoena means a formal request to compel the Department to produce an individual to testify or to produce documents in relation to a proceeding in which the Department may or may not be a party to the action. A subpoena is issued most often by an attorney or, in some instances, by the court. It is often accompanied by a witness fee. Failure to respond to a subpoena may result in legal sanctions.

[2] M.G.L. c. 66A, § 2(k) provides that holders of personal data are required to "maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed."

compliant authorization, the information specified in the authorization may be released, see *Sample-Letter 1*. The keeper of the records from the DPH program should certify the records, either using *Sample-Letter 1* or the certification provided by the attorney.

E. Determine if the Subpoena or Court Order Seeks Non-medical or Medical Data

If the subpoena or court order is for documents that contain personal data and there is no authorization from the data subject allowing the disclosure, determine whether the requested personal data is medical information.

1. Non-Medical and De-identified

If the **subpoena or court order** is for non-medical information and it can be de-identified in compliance with Confidentiality Procedure # 7: De-Identification, Limited Data Sets and Aggregate Data, and still be responsive to the request, the documents may be released after they are fully de-identified, using *Sample-Letter 1*. The keeper of the records from the DPH program should certify the records, either using *Sample-Letter 1* or the certification provided by the attorney.

2. Medical or Non-medical but Identifiable

a. Subpoena

If the subpoena is for medical information, or non-medical information that cannot be de-identified, and there is no authorization from the data subject allowing the disclosure of information, then the documents cannot be released, and two further steps must be taken:

(1) Rule 45 Objections

File objections to the production of documents pursuant to Massachusetts Rules of Civil Procedure, Rule 45, because information sought is subject to FIPA and cannot be released without consent of data subject, (see Sample-Letter 2). MDPH must serve a "written objection" on the attorney designated in the subpoena within 10 days of service of the subpoena (if the subpoena requires production of documents in fewer than 10 days, then the objection must be filed prior to that date). Once an objection is sent, the requesting party is not entitled to the documents without a court order unless the data subject provides an authorization for the requested data.

In some instances the subpoena demands the production of some records that can be disclosed and others that cannot. In these circumstances, the letter to the attorney (see, Sample-Letter 3) should include a certification of what is being released as well as the Rule 45 objection and explanation related to those documents which are not released. The letter to the data subject should inform the data subject of the documents that were released and the documents for which an authorization is requested.

(2) Contact the Data Subject

Contact the data subject(s) regarding the subpoena. Give notice that the Department received a subpoena requesting personal data about the data subject, see Sample-Letter 4. Also, include:

- An authorization to release the information (use the MDPH Model Authorization form); and

- The date by which the data subject should either respond with the authorization, move to quash the subpoena, or seek a limiting or protective order from the court. This should be at a minimum 7 business days.
- If the data subject authorizes the release in writing, the documents referenced in the authorization may be released, see *Sample-Letter 1*. The keeper of the records from the DPH program should certify the records, either using *Sample-Letter 1* or the certification provided by the attorney. If the data subject fails to respond or refuses to authorize the release, then no documents may be released and the attorney who issued the subpoena and was served with a Rule 45 objection must seek a court order. Contact attorney using *Sample-Letter 5*.

If the attorney moves to compel, contact the Attorney General's Office for representation.

b. Court Order

If the court order is for medical information or non-medical information that cannot be de-identified then documents shall not be released and:

(1) Notify data subject

Notice of the court order and request for personal data shall be sent to the data subject as soon as possible, including an authorization form to allow for the release of the data. The letter shall provide the data subject with fourteen days to respond unless the return date in court is earlier. The letter shall also indicate that after the date set in the letter the Department will release the subject's personal data in compliance with the court order. Use Sample-letter 6.

(2) Release of records

If the data subject fails to respond within the time period set, the Department shall release the information requested in the court order, with notice to the data subject. The keeper of the records from the DPH program should certify the records, using Sample-Letter 1.

PART III. Establishing Protocols

Programs that handle many subpoenas should work with their program's attorney to decide if they should establish a protocol of how to process routine subpoenas including when the program should contact the attorney.

PART IV. HIPAA: Subpoena Requirements

A. General Requirements

Under HIPAA, a covered entity may release information pursuant to a subpoena that is *not* authorized or accompanied by a court order if it receives a "satisfactory assurance"[3] as described below. FIPA has a more restrictive standard, requiring the data subject's authorization or a court order, with notice to the data subject before the Department may release information pursuant to a subpoena. The FIPA standard will be followed by all parts of the Department when **responding** to subpoenas regardless of whether the Center or program is a covered health care component under HIPAA. As described in section IV.B, however, the Department

[3] 45 C.F.R. § 164.512(e)(1)

must follow the requirements of HIPAA when **issuing** a subpoena to a HIPAA covered entity.

1. **Satisfactory Assurance from the individual-HIPAA Standard**

   a. **Written notice**
   The party issuing the subpoena made a good faith attempt to provide written notice to the subject of the PHI, sufficient to permit the individual to raise an objection (mailing to individual's last know address is deemed sufficient); and

   b. **Sufficient time to respond**
   The time to raise objections has elapsed, and

   No objections were filed; or

   All objections filed were resolved by the court or administrative tribunal, and disclosures are consistent with the resolution.

2. **Satisfactory Assurance that steps were taken to secure a qualified protective order**[4]
   - The parties have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
   - Party seeking PHI requested a qualified protective order from such court or tribunal.

B. Subpoenas Issued by the Department

1. **Authority as Health Oversight Agency**
   If the Department issues a subpoena for documents to be used in an administrative hearing, no certification of satisfactory assurance is required if the Department is serving in a health oversight capacity. Entities covered by HIPAA are authorized to release protected health information without the authorization of the individual provided that the Department is authorized by law as a health oversight agency to oversee the healthcare system (45 CFR Section 164.512 (d)). This includes oversight activities authorized by law such as administrative investigations, inspections, and licensure or disciplinary actions. The body of the subpoena should reference the authority for the health oversight function and cite 45 CFR Section 164.512 (d) in place of the satisfactory assurance. Programs may also choose to attach a letter that explains the authority: *Sample-Letter 7*

   If the Department is not otherwise authorized to receive the information under the HIPAA Privacy Rule without the individual's authorization, the subpoena must be fully compliant with the HIPAA Privacy Rule and be accompanied by a certification of satisfactory assurance.

2. **Documenting Satisfactory Assurance Process**
   An attorney in the OGC will prepare the required documentation depending on the circumstances. Proof of steps taken in the satisfactory assurance process, as described above, shall be kept in the file, including for example:

[4] An order of a court or an administrative tribunal or a stipulation by the parties to the litigation that (a) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which it was requested; and (b) requires the return to the covered entity or destruction of the PHI at the end of the litigation or proceeding.

- Written notice to the data subject;
- Proof of mailing, including the date of mailing (certificate of mailing or certified mailing receipt) to the data subject; and
- Qualified protective order submitted to court.

C. Subpoenas Received by the Department

If a subpoena is accompanied by a "satisfactory assurance," which meets only the HIPAA, and not the FIPA standard, notify the attorney using *Sample-Letter 8* that the Department is subject to FIPA and cannot release the information without an authorization from the data subject or a proper court order. This letter also contains the required M.R.C.P. Rule 45 (d) objection, explained in Part II E.2.a.i above.

Authority:

M.G.L. c. 66A § 2(k)

45 C.F.R. § 164.512(e)

For a suggested model-letters: See Healthnet, look under the Privacy & Data Access pages, Subpoena Sample-Letters may be found under “Model Forms.” (Available to MDPH Intranet users only)

(Page intentionally blank)

Return to table of contents

Procedure 6 Research Requirements (under construction)

Version: 4 Effective Date: October 1, 2012

Procedure 6 has been removed
This procedure will be rewritten.

Research Requirement questions may be directed to the
DPH Confidential Data Officer: telephone 617-624-5229

(Page intentionally blank)

Procedure 7 De-Identification, Limited Data Sets, and Aggregate Data

Version: 6 Effective Date: October 1, 2012

PART I. Purpose and Scope

This procedure specifies standards under which individual-level or aggregate data can be disclosed if information that can identify a person has been removed or limited as in a limited data set. This procedure applies to both covered and non-covered components of the Department and to all Department workforce members unless otherwise stated.[1] Individual-level data are considered de-identified provided that they meet the standards established in this procedure. A Bureau, however, retains the discretion not to release data that it believes risk identification of the data subject. Bureaus may adopt different aggregate data release standards provided they are at least as protective as one of the standards described in this procedure. The decision to be more protective or to suppress or not release portions of particular aggregate data remains with the custodian of the data.

PART II. Standards for Disclosure of Individual-Level Data

A. De-Identification Standard

Individual-level data are sufficiently de-identified and do not constitute confidential information if one of the following de-identification methods is satisfied.

1. Statistical De-Identification

A qualified statistician using accepted analytic techniques concludes that the risk is very small that the individual-level data could be used alone or in combination with other reasonably available information to identify the subject of those data.

- For purposes of this procedure, a qualified statistician shall mean a member of the MDPH workforce who is identified by the Bureau Director for this purpose and is approved by the Privacy & Data Access Office.
- The process for making this determination must be documented in writing and approved by the Privacy & Data Access Office.
- The documentation shall be maintained with the file including the individual-level data and record of disclosure.

or

2. Safe Harbor Method (Covered components, see footnotes)

Individual-level data are considered de-identified under the safe-harbor method if

All of the identifiers listed in this subsection are removed and the Department workforce member who discloses the de-identified information does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information. If the holder of the data is not the custodian, the holder must confirm with the custodian prior to release that the data are appropriately de-identified.

[1] This procedure does not apply to disclosures of unrestricted, identifiable vital record information made by the Registry of Vital Records and Statistics in accordance with applicable laws.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 7

NOTE: Even if the identifiers listed are removed, there may be situations in which unique characteristics still make the data identifiable, and the data holder must group data elements or combine years in order to create appropriately de-identified information or must not disclose the information.

To create de-identified data, all of the following identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

- Names;
- All geographic subdivisions[2] of a state including:
  - street address
  - city/town
  - precinct
  - Zip Code
  - census tract and geocodes equivalent to the above

  Exceptions: the following geographic information may be included:
    - EOHHS regions
    - CHNAs
    - Counties, provided that Dukes and Nantucket Counties are combined.
- Dates[3]:
  - Month and day of Birth and Death must be removed. Note: depending on the population, it may be necessary to aggregate year of birth or death and age for persons 90 years of age and older, and in some cases, for other age groups as well;
  - Day must be removed for all other dates relating to an individual (for example, dates of admission and discharge from a health care facility, dates of service).
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate or license numbers;
- Vehicle identification and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;

---

[2] Covered components must follow the HIPAA safe harbor standard: All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes. However, the initial three digits of a zip code may remain in the information if, according to current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000.

[3] Covered components must follow the HIPAA safe harbor standard: All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older."

- Biometric identifiers, including finger prints and voiceprints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted under section II.A.3.

3. Re-Identification of De-Identified Data

The Department may assign a code or other means of data identification to allow information that has been de-identified to be re-identified provided that:

- The code or other means of data identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and
- The Department does not disclose the code or other means of data identification for any other purpose and does not disclose the mechanism for re-identification.

B. Limited Data Set Standard

Confidential Information which is sufficiently de-identified so that it no longer can be readily associated with an individual may be disclosed with certain indirect identifiers with authorization of a project in accordance with MGL c.111, §24A.

1. Content of Limited Data Sets

a. Identifiers That Must be Removed

A limited data set is confidential information that ***excludes*** the following direct identifiers of the individual or of his/her relatives, employers, or household members:

- Names;
- Postal address information (street name and number, 4-digit zip code extension)
- Latitude, longitude, census block;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

b. Permissible Identifiers

A limited data set ***may*** include the following information:

- Admission, discharge, service, and incident dates;
- Dates of birth or death;

- Five-digit zip code or any other geographic subdivision, such as state, county, city, town, precinct, census tract, block group and their equivalent codes, (except for street name and number, 4-digit zip code extension, latitude and longitude, or census block);
- Unique Identification Codes that allow information that has been de-identified to be re-identified, including those that are derived from or related to information about the individual provided that the mechanism for re-identification is not disclosed; and
- Any other information that is not specified in section II.B.1.a.

2. Authorization to access a limited data set

a. By DPH Workforce.
A DPH workforce member may access a limited data set as permitted in Procedure 3, section III.B.

b. By Outside Applicants.
Individuals or entities outside the Department may apply for access to use a limited data set that meets the standard described in section II.B.1.[4] Release of a limited data set may be authorized at the discretion of MDPH. The application is reviewed and approved by the confidential data officer in conjunction with an epidemiologist or content expert within the bureau from which the data are requested. Criteria for approval include:

- The application is complete;
- The release of the requested data is not otherwise restricted by law;
- The request is for public health purposes and may lead to reduction of morbidity and mortality in the Commonwealth;
- The request is for data elements reasonably related to the public health purpose;
- The requested data elements meet the standard for a limited data set; and
- The request includes appropriate plans for secure storage and use.

3. Bureau Requirements Related to Limited Data Set Agreements

- Bureaus shall make a content expert available to work with the confidential data officer to ensure that the data requested are reasonably related to conducting the analyses or activities described in the application, and that the information provided is clear and complete.
- The application for access must be approved by the confidential data officer prior to the release of any data to which it pertains and the bureau releasing the limited data set shall maintain a copy of the approval.

PART III. Standards for Disclosure of Aggregate Data

A. General Requirements

[4] Although the HIPAA Privacy Rule provides that a covered entity may disclose a limited data set for the purposes of research, public health, or operations pursuant to a Limited Data Set Agreement this is generally not used by the Department. For specific instances where it may be appropriate inquiries should be directed to the confidential data officer.

Aggregate data are data collected from individual-level data that have been combined for statistical or analytical purposes. Data that satisfy the aggregate data release standards outlined in this section are considered de-identified and may be released.

The aggregate data release standards below are a minimum standard. Any Bureau may adopt more restrictive standards for disclosure of aggregate data. Regardless of whether a Bureau follows the Department standards specified below or its own more restrictive standards, each Bureau that discloses aggregate data must ensure that there is no reasonable basis to believe that any identifying information could be derived from disclosure of the aggregate data.

When multiple data sets are combined, the standard for the data set with the most restrictive rules must be followed. When utilizing data from other agencies, workforce members using the data are responsible for complying with the standard for aggregate data release for that agency and to ensure that it is followed if it is more restrictive than the MDPH standard.

Each Bureau privacy liaison shall document and provide to the Privacy & Data Access Office the aggregate data release standard or standards adopted by the Bureau.

All MDPH publications (all public releases including publications and web releases) containing aggregate data shall be reviewed through the MDPH Peer Review Process or a comparable committee or process to verify that the Department or Bureau aggregate data release standard is met prior to release.

B. De-identification Methods

To de-identify aggregate data, bureaus should select one of the following standards.

Even after applying one of these de-identification standards, the data should not be released if there is a reasonable risk that an individual could be identified.

1. Numerator/Denominator-Based Suppression

Cell sizes based on a combination of denominator[5] (population or group from which the health events arise) and numerator[6] (health event) are suppressed in accordance with the table below. Aggregate data with denominator and numerator values greater than those indicated in the table may be considered sufficiently de-identified so as not to constitute confidential information, and may be disclosed. Cell suppression requirements are explained further in table 7.1.

[5] Population or denominator means: For counts of health events (cases, diagnoses, births, discharges, etc.), the population or denominator is defined as the number of people who live in a particular community, are clients of a particular program, or patients in a particular facility. The population or denominator may be further delineated by demographic information (e.g., race, age, gender, etc.). For additional cross-classifications, the denominator is defined as the number of events or the numerator for the preceding cross-classification or the population.

[6] Numerator means: The number health events (cases, diagnoses, clients, discharges, encounters, visits, etc.) being considered for release for a particular population or cross-classification.

Table 7.1: Cell suppression requirements

DENOMINATOR (D)	NUMERATOR (N)	STANDARD
10-29	1-4	Suppress numerator and any other cells[5] that would allow for the calculation of any other cells with values of 1-4
10-29	5-29	Suppress any cells that would allow for the calculation of any other cells[6] with values of 1-4
0-9	0-9	Suppress numerator
= N	= D	Suppress numerator unless privacy risk is minimal

2. **Numerator Based Cell Suppression**
   - Suppress all statistical cells with one to five subjects; and
   - Suppress all other cells that would allow for the calculation of the values of cells that have been suppressed in the first bullet.[7]

   or

3. **Alternative Suppression Standards**
   Any Bureau may develop an alternative aggregate data release standard if it decides not to follow any of the standards above, provided that:
   - The standard is at least as restrictive as the above stated standards; and
   - Any alternative standard is documented by the Bureau and approved by the Privacy & Data Access Office prior to implementation.

4. **Statistical De-Identification:**
   Any bureau may rely on a qualified statistician using accepted analytic techniques to conclude that the aggregate data are de-identified as described above in Section II.A. 1. on Statistical De-identification.

Authority:

M.G.L. c. 66A

45 C.F.R §§ 164.514

For a Limited Data Set Agreement form: See Healthnet, look under the Privacy & Data Access pages, forms may be found under "Model Forms."
(Available to MDPH Intranet users only)

[7] Because it is possible to figure out a suppressed value from column and row totals when only one value is suppressed, it may also be necessary to either suppress the column and row totals or suppress other cells so that no column or row has only one suppressed value.

Procedure 8 Public Records Release Standards for Documents Containing Medical Information

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes how to protect the privacy of individuals whose medical information is contained in DPH reports and documents requested as public records.

This procedure applies to all documents containing medical files or medical information [hereinafter referenced as medical information] including, but not limited to, Statements of Deficiencies (SOD), complaint and incident investigation reports, licensure or inspection reports, external review documents, and records relating to disease investigations. All Department workforce members in both covered and non-covered components of the Department must comply with this procedure.

Table 8.1 is a decision tree to aid MDPH employees answering a public records request.

PART II. General Requirements

Before releasing any reports and documents containing medical information pursuant to a public records request, workforce members should engage in the following process:

1. Determine if the requested materials contain any one of the following three categories of information:
   - Direct identifiers;
   - Medical information related to an individual; or
   - Indirect identifiers.
2. Redact or withhold any information falling within one of the three categories; and
3. Release the materials as a public record unless another Public Records Law exemption prohibits the release.

PART III. Redaction Standards Applicable to all Documents

The standards for redacting identifiers and medical information under this part apply to all Department documents and reports. As discussed in part IV, Bureaus are responsible for developing standards for redacting indirect identifiers specific to Bureau needs.

A. Direct Identifiers

Workforce members shall redact all direct personal identifiers from all documents that include medical information prior to public release including, but not limited to:

1. Patient names

All names[1] of individuals who received medical care, resided in the facility, or filed a complaint;[2]

[1] To the extent that reports are drafted with a generic reference (i.e., patient A) rather than an individual name, no redaction for this item would be required.

[2] Exemption (f) of the Public Records Law (M.G.L. c. 4, §7(26)) permits the agency to withhold the name of the complainant without having to show prejudice to an ongoing investigation.

2. **Dates:**
   Month and day of birth and death. Depending on the population, it may be necessary to aggregate year of birth or death and age for persons 90 years of age and older, and in some cases for other age groups as well, if it could serve to identify an individual.

   Day for all other dates directly related to an individual shall be redacted. Redact the day (but may include the month and year) for the following dates:

   - Admission date;
   - Discharge date;
   - Date of incident; and
   - Date of service;

3. **Address and contact information**
   The home address (including street, town, county, state, country, and zip code) and phone number of any individual included in the document. This does not include the address of a residential facility including, but not limited to, a hospital, long-term care facility, rest-home, substance abuse facility, or other community-based facility; and

4. **Personal ID Numbers**
   All personal identification numbers including a social security number; medical record number; and health plan number.

B. Medical Information

Bureaus shall not release any medical information that relates to an individual with the exception of the general medical condition or category of complaint that some programs may determine is necessary to retain, as described in part IV.

Medical information is not necessarily determined by whether it is physically located in a single file, but turns on the nature or character of the documents and their label or location. This includes medical information lacking direct identifiers that could be used to identify an individual,[3] as opposed to aggregate medical information[4] from more than one individual's file.

Medical information includes the nature and extent of a person's medical condition. This includes medical statements, for example, such as a bad back, heart problems, and hypertension if related to a specific person. It also includes autopsies and blood tests, as well as information that is diagnostic in nature and that yields detailed, intimate information about the subject's body and medical condition.

C. Medical Records and Abstracts

Medical records and abstracts are a subset of medical information. A medical record is an independent document created by the provider as part of providing health care,

[3] The release of medical information, even without other particular identifying details, creates a serious risk of identification by those who are familiar with the individual. The risk of identification is enhanced in those instances that relate to surveys, inspections, complaints, or investigations of particular licensed, identified facilities at a particular point in time. Moreover, the ability to link information electronically and to tie it to other information in the public domain has greatly increased the risk of identifying individuals from limited information.

[4] Release of aggregate information must comply with Procedure # 7: De-Identification, Limited Data Sets, and Aggregate Data.

which a Bureau is given or collects in the process of its oversight functions. Medical abstracts are also independent documents, created by a DPH investigator from the medical record and include only medical information taken directly from the medical records of a provider. Medical records and abstracts are wholly exempt from release.

D. Non-Segregable Materials

Sections of reports or documents containing non-segregable medical information may be redacted in their entirely. Material is considered non-segregable if redacting the medical information from the section leaves information with no independent meaning. For example, the redaction of the medical information in a section of a document might leave only conjunctions such as "and," "but," and "or." This section should be redacted in its entirety because the string of conjunctions has no independent meaning.

PART IV. Bureau-Specific Redaction Standards[5]

A. Indirect Identifiers

Indirect identifiers are elements in documents and records which implicate privacy interests by increasing the likelihood of identifying an individual, but do not involve direct identifiers or medical information.

The indirect identifiers left in any specific document may vary from program to program and depend on whether the indirect identifier serves to increase the likelihood of identifying the individual and whether the privacy interest of the individual outweighs the public interest in releasing the indirect identifier. For example, Health Care Quality will release the name of the facility in a hospital or nursing home inspection report since the performance of the facility is precisely what is at issue in the report, the likelihood of increasing the chance of identifying the individual is limited, and there is a strong public interest in its release. On the other hand, the Office of Patient Protection will redact references to a specific facility, but not to the health plan, since it is the health plan and not the facility that is at issue in the matter on appeal. Moreover, the name of a facility coupled with the health plan could serve to identify the individual in an OPP decision and therefore, should be redacted.

Each Bureau that releases such documents as public records shall formulate its own protocol for redaction of indirect identifiers commonly found in their documents including, but not limited to:

- The name of a facility, provided that it is not the subject of the incident, investigation or case in review;
- The name(s) of medical provider(s), employee(s) of the facility or a witness(es) to events provided that they are not the subject of the incident, investigation, or case in review;
- Age of individual: exact age, age range, or age category (e.g., adult, child, infant);
- General medical condition or subject of incident, investigation, or case under review (e.g., OPP may release a decision that states that the appeal relates to a denial of coverage for a breast reduction. HCQ may identify the category of

[5] It is recommended that these redaction standards be set at the program level, if they are likely to differ from program to program within a Bureau.

complaints as those relating to gastric bypass surgery. The inclusion of this information is necessary to identify the incident, investigation, or case under review. No other medical information should be included) and;,

- Other personal information (e.g., marital status; paternity; government assistance; family disputes; and reputation).

Copies of program-specific redaction standards shall be made available to the Privacy Officer.

B. Report-Writing Considerations

Each Bureau[6] shall review this procedure and the associated Bureau-specific protocol to determine, to the extent possible, how to modify its report-writing requirements to accommodate these standards without the need for redaction. If certain information, which must be redacted prior to public release, is required to be included in the reports/documents, programs should set standards for writing and formatting the reports to ensure their readability. If identifying information is not required, it should not be included in the report.

Each Bureau should also review its report-writing requirements and decide whether to add a report summary of the report, either as an executive summary or a separate document, which includes no identifiers or medical information. This may be particularly important if the program deems it necessary to provide a context for its findings or to provide the public with sufficient information to fulfill its health oversight functions. The decision to issue a summary is within the discretion of the Department and shall be made by the Bureau director or designee.

Authority:

M.G.L. c. 4, § 7(26) and M.G.L. c. 66A

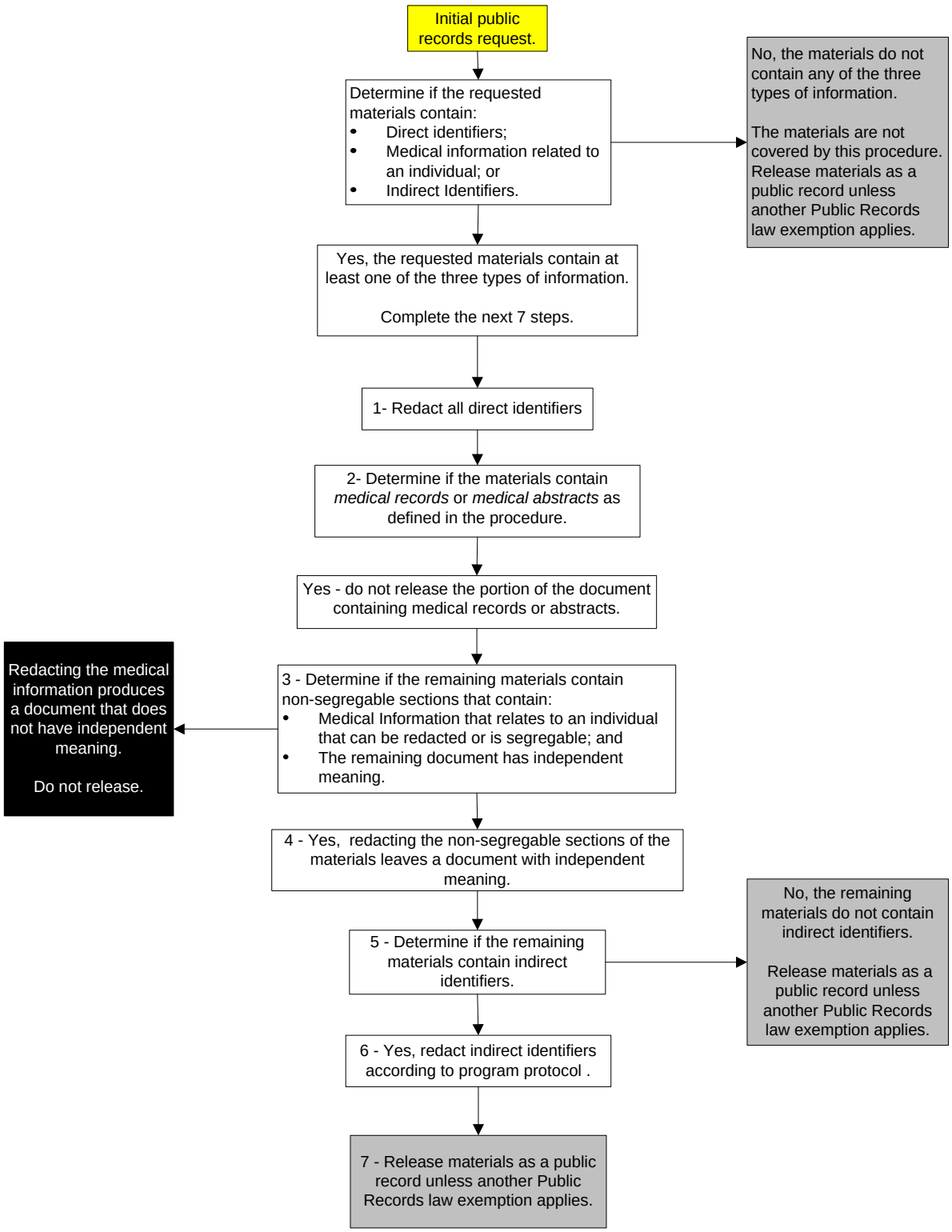
45 C.F.R. § 164.514

[6] These considerations should be coordinated at a Bureau level, but again may differ from program to program.

Return to table of contents

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 8

Table 8.1: Determining response to public records request for documents containing medical information.



(Page intentionally blank)

Procedure 9 Verification of Individuals or Entities Requesting Disclosure of Confidential Information

Version: 4 Effective Date: April 21, 2008

PART I. Purpose and Scope

In the absence of a statute or regulation that defines the verification standard for a particular program, this procedure describes how a Bureau or Program determines whether it is permitted to release confidential information to the individual or entity making the request. As needed, a Bureaus or Program should establish additional specific protocols that correspond to its internal operations. Bureau or Program-specific protocols shall be available to the Privacy Officer upon request.

This procedure applies to both covered and non-covered components of the Department and all Department workforce members.

Graphical guidance is provided in table 9.1 showing steps in the verification process.

PART II. General Requirements

Prior to disclosing confidential information, Department workforce members shall follow a four-step process:

1. Verify the authority of the individual or entity to receive access to the confidential information that is requested as discussed in section III;
2. Classify the type of requestor (i.e., data subject requesting their own confidential information; an attorney for the data subject; or the legal representative of the data subject);
3. Verify the identity of the individual or entity requesting access to the information as discussed in section IV and the verification chart; and
4. Verify the records requested as discussed in section V.

PART III. Verification of the Requestor's Authority

Determine whether the individual or entity requesting the disclosure of confidential information is permitted to have access to the information. The best method for determining this is by considering whether the disclosure is permissible under Procedure # 3: Use and Disclosure of Confidential Information. For example, consider whether:

- The request is from the data subject for his or her own confidential information;
- The request is from the data subject's personal representative for the data subject's confidential information, and is accompanied by the appropriate documentation;
- The request is accompanied by an authorization and the authorization meets the requirements of Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information;

PART IV. Verification of the Requestor's Identity

Make sure that the individual requesting the information is who he or she claims to be. If the person is known to you from prior experience, no further verification is required. If the individual is not known to you, refer to the chart below for details on identity verification. A DPH workforce member should use common sense when

verifying identity. For example, if reasonable under the circumstances, a workforce member may rely on documents, statements, or representations that on their face meet applicable requirements.

The verification standard is a minimum standard. Any program may implement enhanced measures.

PART V. Waiver

Any Bureau that believes compliance with the verification procedure is a hardship for the individual making the request, may apply to the Privacy Officer for a waiver of the standard for the verification of the requestor's identity. No waiver will be granted unless the Bureau demonstrates that the requirement is a hardship and that it has taken necessary precautions to ensure the protection of confidential information against unauthorized release.

PART VI. Verification of the Record Requested

After determining that the disclosure is permitted and verifying the identity of the requestor, workforce members must take steps to verify that the record requested is the appropriate record. The steps taken by each Bureau to verify the record may differ depending on the type of information held with respect to the individuals served. Among the data elements that may be used to verify the record are the individual's full name, social security number, date of birth, address at the date of service, or name of parents or guardians.

Authority:

M.G.L. c. 66A

45 C.F.R. § 164.514(h)

Table 9.1: Steps in the verification process

Individual Requesting Information	Authorization required to Release Information to Individual Requesting Information	Verification Of Identity Individual Required to Present to Obtain Information	Verification of the Release of the Appropriate Records
The data subject (DS)	None required	Identification can be verified by one of the following methods: 1) presentation or copy of a photo identification; 2) provision of information that only that person would know; 3) recognition of the individual by a DPH workforce member; 4) comparison of an individual's signature with a copy of the person's signature in an existing DPH file; or 5) a notarized signature.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of Birth of DS • Address of DS at the date of service • Name of parents or guardian
The DS, if the DS has a different last name	None required	Verify that it is the same individual as DS • documentation showing the same address; or, • documentation showing maiden name or name change Use common sense. Workforce may reasonably rely on documents, statements, or representations that, on their face, meet the applicable requirements.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at the date of service • Name of parents or guardian
Attorney for DS Legislator of DS	Authorization from DS and statement from attorney or DS that the attorney is representing the DS. Authorization from DS and statement from legislator or DS that the legislator is acting on behalf of the DS.	Attorney's request must be on letterhead identifying the name and address of law firm or attorney identified as representing the DS. The Legislator's request must be on letterhead identifying the name and address of legislator identified as acting on behalf of the DS.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at the date or service • Name of parents or guardian
Guardian Treatment Monitor/Rogers Guardian Custody of the State (DSS/DYS) Executor or administrator of DS estate Conservator	Copy of the relevant court appointment. Verify that the court appointment does not limit a guardian from obtaining the information requested. Note: Some authority may change. It should be checked periodically.	Verify requestor's identify in the same way that one verifies the DS's identity.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at date of service • Name of parents or guardian

Individual Requesting Information	Authorization required to Release Information to Individual Requesting Information	Verification Of Identity Individual Required to Present to Obtain Information	Verification of the Release of the Appropriate Records
Health Care Agent	Copy of the Health Care Proxy signed by the DS and documentation of the individual's incapacity. Note: Designation as the Health Care Agent alone is insufficient authority.	Verify requestor's identify in the same way that one verifies the DS's identity.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at the date of service • Name of parents or guardian
Requests from third parties, e.g., spouse, relative, friend, or other person when the DS when the DS is present	None required. It is the same as the DS above. Since the DS is present and gives verbal consent for MDPH to speak to or give documentation to the other individual and indicates the scope of the information, it is permissible to disclose information to the other person. This can only be done in person with the DS present. .	Verify the identity of the DS in the same manner that you would if the DS were alone. It is not necessary to verify the identity of the other person identified by the DS. You should note the name of the other person in the file.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, for example: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at the date of service • Name of` parents or guardian
Requests from third parties, e.g., spouse, relative, friend, or other person when the DS is not present.	Since the DS is not present, a written authorization in compliance with Procedure #4 is required. Use professional judgment in reviewing the documents. It is appropriate to rely on an authorization for authority to release information to the individual or institution named in the authorization, unless there is something about the authorization that raises questions about its authenticity.	Verify requestor's identify in the same way that one verifies the DS's identity.	Assure that the written authorization provides sufficient information to show that the information on the records relates to the information provided on the authorization form, including the elements listed above.

Table 9.1: Steps in the verification process

Procedure 10 Security of Confidential Information

Version: 4 Effective Date: June 1, 2009

PART I. Purpose and definitions

This procedure describes the standards for ensuring the security of the Confidential Information collected, maintained, used, and discarded by the Department.

This Procedure applies to both covered and non-covered components of the Department and to all Department workforce members.

A. Definitions

1. Confidential Information
Unless otherwise defined by law, any individually identifiable information, including, but not limited to, medical and demographic information, that:

- Reveals the identity of the data subject or is readily identified with the data subject, such as 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 data subject.

2. Portable Device
Includes any non-fixed device that contains an operating system that may be used to create, access, or store Confidential Information (e.g., laptop computers, wireless email devices [e.g., BlackBerry], tablet computers, personal digital assistants [PDAs], smart phones, etc.).

3. Removable Media
Includes, but is not limited to, CDs, DVDs, MP3 players, removable memory including external hard disk drives, and USB flash drives (thumb drives).

PART II. Transmission of Confidential Information

Department workforce members must take steps to ensure the security of Confidential Information transmitted within the Department and to non-DPH entities. Workforce members shall disclose Confidential Information only when the disclosure is permissible under Procedure # 3: Use and Disclosure of Confidential Information.

A. Disclosures Made by U.S. Mail

When sending Confidential Information by U.S. mail workforce members must

1. Verify that the correct Confidential Information is being mailed to the correct individual(s);
2. Send the information in a security envelope marked “Confidential,”
3. Include their name and a return address;
4. Verify that the recipient’s address is correct; and
5. Whenever feasible, send the information by registered or certified mail, or another method that provides delivery tracking.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 10

B. Disclosures Made by Delivery or Courier Service

When sending Confidential Information by hand delivery or courier service, workforce members must:

1. Verify that the correct Confidential Information is being delivered to the correct individual(s);
2. Verify the name and address of the intended recipient;;
3. Seal the information under protective cover (e.g., a folder or envelope) and mark the package “Confidential,”
4. Use a reputable courier service known to the Department;
5. Verify the identity of the individual who will be delivering the package.. Workforce members should also record the courier’s name, time of pick-up, and other identifying information such as employee number available from the identification presented by the courier; and
6. Retain a tracking number so that in the event the intended recipient informs you that the package was not received, you are able to track the item with the delivery service.

C. Disclosures Made by Facsimile Machine

When sending Confidential Information by facsimile machine, workforce members must:

1. Verify the fax number of the intended recipient.
2. Telephone the recipient to alert him/her that a fax containing Confidential Information is to be transmitted.
3. Transmit the fax using either DPH’s standard fax cover sheet (See Healthnet, look under the Privacy & Data Access pages, forms may be found under “Model Forms.” Available to DPH Intranet users only) or a Bureau-specific cover sheet that contains:
   - A confidentiality statement; and
   - Instructions directing the unauthorized recipient of a misdirected fax to contact the sender. In the event of a misdirected fax, the unauthorized recipient should be directed to immediately destroy the fax or return the information to the sender, as directed by the sender.
4. If the recipient does not confirm receipt within a reasonable period of time, call the recipient to confirm receipt.
5. Remove the faxed documents from the vicinity of the fax machine, including the fax activity confirmation sheet after transmission. Keep fax activity confirmation sheets with original documents.

It is considered a best practice to locate fax machines in a secure area to which only authorized workforce members have access, ideally in a locked room.

D. Disclosures Made by Telephone

When transmitting Confidential Information by telephone, workforce members must take the following steps:

1. Verify the identity of all requestor's seeking the disclosure of Confidential Information over the telephone.
2. Whether using landlines, cellular telephones, or public telephones, disclose Confidential Information by telephone only from a secure or private area whenever feasible.
3. Never leave messages with Confidential Information on voicemail, answering machines or with individuals other than the data subject or their personal representative. Information left in messages shall be generic in nature and not indicate services being performed or provider of such services, unless the data subject has directly requested otherwise and is documented in the data subject's record. An example of a generic message is, "My name is Emily Smith. Please return my call at 617.624.5200."

E. Restrictions on Email, Email Attachments, and File Transfers

No Confidential Information shall be transmitted electronically unless compliant with the requirements of Procedure 10A.

PART III. Workstation Security

To minimize the opportunity for DPH workforce members and worksite visitors to inadvertently view Confidential Information to which they should not have access, DPH workforce members shall adhere to the following guidelines at all times:

- Workstations at which Confidential Information is handled are to be located in secure areas of DPH property.
- Terminals should be turned so that they are not facing hallways or other heavily trafficked areas.
- Passwords must not be shared.
- No one should use a computer while it is operating under another person's password.
- Passwords should not be displayed in the work area.
- Documents containing Confidential Information should be turned face-down when the workstation is unattended; these documents should be locked before leaving for extended periods of time and at the end of day.
- Workforce members must log off or lock their computers when stepping away from their desks for an extended period or leaving at the end of the day.
- Work should not be saved to individual computer hard drives (c drives) but rather to shared network drives.

PART IV. Storage of Confidential Information

Confidential Information shall be stored and maintained by the data custodian in a manner that protects the confidentiality, integrity, and availability of the information. Access to the Confidential Information must meet the Department's minimum necessary and role-based access standards as described in Procedure # 3.

A. Paper-Based Confidential Information

Improper storage of on-site paper-based files including the storage of files in unlocked file cabinets may result in the improper disclosure of or access to Confidential Information. Bureaus shall take steps to secure paper-based Confidential Information, including:

1. Move Confidential Information to locked files or purchase and install locks on existing non-locked cabinets;
2. Move file cabinets or other storage sites from public areas to low-traffic areas;
3. Move workforce members and storage so that those workforce members who need access to the materials are located near the storage area, and those not requiring access are relocated away from the area; and
4. Move file cabinets without locks into rooms that can be locked or otherwise secured; limit access to rooms with unlocked cabinets based on need–to-know, role-based access.

B. Printers and Copiers

Improper disclosures of Confidential Information can occur by means of unsecured printers and copiers. Examples of unsecured printers or copiers are those located in unmonitored or high-traffic areas that allow unauthorized individuals to search through documents left at the printer or copier. Bureaus shall take steps to secure these devices, including:

1. Move printers to enclosed areas to which only authorized personnel have access;
2. Designate dedicated printers and copiers to be used only for printing and copying Confidential Information; and
3. Train staff to immediately retrieve papers that contain Confidential Information from printers and copy machines.

C. Electronic Confidential Information

1. Electronic Confidential Information shall be maintained by the data custodian in a manner that protects the confidentiality, integrity, and availability of the information.
2. Confidential Information stored on desktop computers must be encrypted.
3. Confidential Information stored on any removable media and portable devices must be password-protected and stored in an encrypted volume or file using DPH-approved encryption products (refer to the ITS Procedure on Portable Devices and Removable Media).
4. Passwords must contain, at minimum, eight characters, and the following characteristics:
    a. At least one uppercase character

b. At least one lowercase character; and

c. At least one numeric digit.

Workforce members should not use such obvious choices as children's names, repeating numbers, birthdays, and telephone numbers.

5. Workforce member's access rights must meet the Department's role-based access and minimum necessary standards as described in Procedure # 3. Workforce members shall not circumvent prescribed access rights by sharing their passwords or utilizing another workforce member's password to access Confidential Information beyond the scope of their authority.

6. ITS must be immediately notified when workforce members are terminated so that the workforce member's access rights can be terminated immediately.

7. Program management, Human Resources, and ITS should coordinate the date and time of a workforce member's transfer or resignation so that computer network access is altered or terminated as required under the circumstances.

PART V. Removal of Confidential Information from the Worksite

Workforce members shall not remove Confidential Information, including paper or electronic information, from the work site unless it is required for a field visit, meeting, or otherwise necessary for work-related purposes and only with supervisor permission and pursuant to Bureau procedures. Appropriate measures shall be taken in each instance to ensure that Confidential Information removed from the building is secured from unauthorized access.

A. Paper Records & Removable Media

Only workforce members that are authorized to do so may remove paper records and removable media from worksite premises. Confidential Information shall not be left unattended in an unsecured area or container. Records and files shall be transported in containers (e.g., locked briefcases, sealed boxes, or sealed envelopes) that are not easily opened by unauthorized individuals.

B. Portable Devices

Laptop computers, PDAs, and other portable devices on which Confidential Information is stored should be protected at all times and should not be left unattended. In automobiles, laptops, PDAs, and other portable devices should be kept out of sight and locked when the car is unattended. Laptops, PDAs, and other portable devices on which Confidential Information is stored should not be loaned to any unauthorized person including family members.

Note: The Executive Office of Health and Human Services Laptop Computer Security Policy and Procedures are available on the Public Health Confidentiality Policy and Procedures page within the DPH Privacy and Confidentiality Internet page.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 10

PART VI. Disposal of Confidential Information

First, determine if you are authorized and have permission to destroy the information under the Statewide Records Retention Schedule. A description of this process can be found at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm. If you have permission to destroy the information, or don't need permission, destroy the information according to the minimum standards set out below. In all cases, contact the Help Desk for assistance should you have questions.

A. Paper-Based Records

Bureaus shall take steps to ensure the proper destruction of paper records containing Confidential Information. This includes purchasing:

- Shredders and place them near recycling and trash bins; or
- Secure bins with locked tops and contracting with vendors to ensure secure disposal.

Redaction of Confidential Information so that it can no longer be read is also an acceptable method of disposal.

B. Electronic Records

Confidential information stored on portable devices must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software implementing at a minimum D.D.5200.28-STD (7) disk wiping, and the degaussing of backup tapes.

C. Removable Media

Confidential information stored on removable media must be destroyed so that it cannot be recovered. Removable Media must be made unusable by physical destruction such as shredding or the data must be permanently destroyed through the use of file wiping software implementing at a minimum DoD.5200 disk wiping.

The Help Desk at 250 Washington Street has a CD shredder that is available for staff use.

D. Portable Devices

Confidential information stored on portable devices must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software implementing at a minimum D.D.5200.28-STD (7) disk wiping, and the degaussing of backup tapes.

Authority:

M.G.L. c. 66A, § 2

M.G.L. c. 93 I

45 C.F.R. § 164.530(c)

Procedure 10A The Electronic Transmission of Confidential Information

Version: 5 Effective Date: June 1, 2009

PART I. Policy & Definitions

A. Policy

The Massachusetts Department of Public Health (DPH) prohibits the electronic transmission of Confidential Information whether within the body of an Email, as an Attachment, or as a File Transfer unless the Bureau or workforce member has received a waiver from the Privacy & Data Access Office. An electronic transmission that includes an individual's name or address without any other Confidential Information is not included in this policy unless the sender's signature includes the name of his/her bureau or program.

Exemptions to this policy are named below. All other electronic transmissions require the approval of the DPH Privacy & Data Access Office.

Due to the identity theft risk associated with their loss, DPH prohibits the electronic transmission the following except under extraordinary circumstances:

- Social Security Numbers
- Driver's license numbers
- State-issued identification card numbers
- Financial account numbers
- Credit or debit card numbers
- Personal identification number or passwords.

Bureaus and programs seeking approval to transmit this information will be required to demonstrate that their electronic transmission is required to accomplish the business requirement.

B. Rationale

All information transmitted electronically is at risk of tampering or disclosure whether inadvertently, maliciously, or through human error. The use of encryption technology and attention to process mitigates the risk associated with the electronic transmission of information.

C. Purpose

This procedure describes:

- The Department of Public Health's policy prohibiting the electronic transmission, including File Transfers, of Confidential Information;
- The Bureaus and circumstances which are exempt from this policy;
- The framework within which a DPH Bureau may seek a waiver from the prohibition against the electronic transmission of Confidential Information;
- Guidelines for the electronic transmission of Confidential Information within the state domain; and
- Guidelines for the electronic transmission of Confidential Information between external entities, e.g., third parties such as contractors or health care facilities.

D. Definitions

1. Confidential Information
For the purposes of this policy, any individually identifiable information, including, but not limited to, medical and demographic information that:

- Reveals the identity of the subject or is readily identified with the data subject such as name, address, telephone number, social security number, health identification number, or date of birth;
- Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a data subject;
- Includes any protected health information as defined by HIPAA and any personal data, as defined by FIPA. See http://healthnet.dph.state.ma.us/privsec/glossary.htm#C; or
- Includes health information or reference to an application to, enrollment or participation in any DPH or EOHHS program.

2. Electronic Transmission
For the purposes of this policy, the use of Email and File Transfer protocols such as SFTP, SFED, and NDM to exchange information over a computer network.

3. Email
A system for sending and receiving messages electronically over a computer network, as between personal computers.

4. MAGnet
The Commonwealth's wide area network (MAGNet). Not all state agencies' operations are located on MAGnet.

5. Secure File and Email Delivery System (SFED)
A system used by Commonwealth governmental agencies to ensure the security of electronic transmission of Confidential Information. The SFED system uses encryption to protect data during transmission.

6. State Domain
The Commonwealth of Massachusetts' wide area network (WAN). The Email system operates in this network. Email users are assigned an address ending in "state.ma.us."

PART II. Exemptions & Waivers

A. Exemptions

The Bureau and Individuals identified in table 10A.1 are exempt from the general policy prohibition against the electronic transmission of Confidential Information when using DPH computers. Exempt Bureaus or individuals are still required to follow the protocols for sending Emails with Confidential Information outlined in Part III of this procedure.

Table 10A.1: Exemptions & Waivers

Bureau/Individual	Circumstances
DPH Hospitals	• When emailing within or between DPH hospitals • When emailing between a DPH hospital and the Bureau of Public Health Hospitals • When emailing between a DPH hospital and the DPH Office of General Counsel • When emailing between a DPH hospital and representatives of the Department of Mental Health with respect to common clients • When emailing between a DPH Hospital and representatives of the Department of Corrections with respect to common clients. • When emailing between a DPH Hospital and representatives of UMass Medical School with respect to common clients
DPH Workforce Members	Between DPH workforce members and Human Resources when using Email to conduct personnel matters.
DPH Workforce Members	When an email is misdirected to a DPH workforce member, it may be forwarded to the appropriate DPH workforce member if the original email comes from an address outside state.ma.us and it is from the individual about whom the information relates or is from an advocate for that individual with the consent or implied consent of that individual.

All other electronic transmissions of Confidential Information require the approval of the DPH Privacy & Data Access Office.

B. Obtaining Approval to Transmit Confidential Information Electronically

DPH Bureaus may apply to the Privacy and Data Access Office for approval to transmit Confidential Information electronically using the "Application to Transmit Confidential Information Electronically." The application must include:

- A description of the business justification (see "Business justification" below);
- A description of the Confidential Information that the Bureau proposes to transmit electronically. This should contain only the minimum necessary data elements required to accomplish the intended purpose of the transmission. Social Security Numbers and other personal identification numbers as described in Part I.A. may not be included unless the Bureau or Program is required to transmit them and the business need is essential.

- The name of each state agency workforce member for whom you are requesting approval to transmit Confidential Information;
- The name of each external user (individuals not within the state.ma.us domain) for whom you are requesting approval to transmit Confidential Information; and
- The Bureau director's signature.

The signed application should be submitted to the Privacy Officer, c/o the Privacy & Data Access Office, 250 Washington Street. An electronic copy of the application should be forwarded to the Privacy Officer's attention as well.

Note: Applications for approval are transaction-specific. Additions or modifications to approved transmissions require the submission of a new or amended application for approval. Bureaus and Programs are expected to inform the Privacy & Data Access Office of changes and additions to application contacts, state agency workforce members, and external users involved in transmitting Confidential Information on a monthly basis.

C. Business Justification and the Application Evaluation

Applications will be evaluated by the Privacy & Data Access Office based on a review of:

- The Bureau's business justification;
- Adherence to disclosure requirements as described in Confidentiality Procedure #3
- Adherence to standards for the disclosure of the minimum amount of Confidential Information necessary to achieve the business requirement; and
- The existence, if necessary, of any data-sharing agreements.

PART III. Transmitting Confidential Information Electronically

The required procedures below apply only to Bureaus that are exempt from the policy prohibiting the electronic transmission of Confidential Information or to Bureaus that have applied for and received a waiver from this policy from the Privacy & Data Access Office.

A. Email Conventions

- Use this or similar language as a Header or Footer: "This mail [and attachment] is intended for authorized individuals and contains confidential information. If you have received this message in error and are not the intended recipient, please notify the sender."
- Do not use any Confidential Information in the subject line of the Email.
- Verify the intended recipients (the individuals included in the "TO" field) prior to sending the message. Use prepared contact lists whenever possible.

B. Determination of the Technology Solution

Upon receipt of the "Application to Transmit Confidential Information Electronically," the Privacy Officer will confer with ITS as necessary to determine the most appropriate technology solution. Solutions are based on volume, user types, and the nature of the transaction.

C. Technical Notes

1. MAGnet Email System
Type "Confidential" in the subject line of the Email to be sent. It is not case-sensitive and does not need to be boldfaced.

2. SFED

c. Request Process
SFED accounts are obtained from the DPH Help Desk.

d. SFED Account Management
SFED users will be assigned a special SFED account that will end "eohhs-sfed.state.ma.us."

Example: emily.publichealth@eohhs-sfed.state.ma.us

SFED users should be sure to direct all their SFED incoming and outgoing Email to their SFED accounts and not to their regular work Email (i.e., the account ending "state.ma.us").

PART IV. Administrative Requirements

A. Training Requirements

It is the responsibility of each DPH Bureau to ensure that each workforce member completes the appropriate training prior to transmitting Emails containing Confidential Information. Completion of the training must be documented.

If SFED is identified as the technology solution for transmitting Confidential Information electronically, it is the responsibility of the approved Bureau to train any individuals (either state agency workforce members or external users) who will be using SFED (either as a sender or as a receiver) in this application.

This requirement applies to both exempt Bureaus and Programs and those who are approved to email Confidential Information by means of a waiver.

Table 10A.3: Available Privacy and Confidentiality Training

If you will be using	You must take training located on HEALTHNET *
The MAGnet Email System	http://healthnet.dph.state.ma.us/privsec/training/email/email01.htm
SFED	http://healthnet.dph.state.ma.us/privsec/training.htm
* Available to DPH Intranet users only.	

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 10A

B. Self-Audit Requirements

Bureaus receiving a waiver authorizing them to transmit individual-level Confidential Information electronically must conduct an annual self-audit to ensure that:

1. The list of approved workforce members is current;
2. All approved workforce members have completed training;
3. Only the minimum necessary Confidential Information is being sent;
4. The electronic transmission of Confidential Information is used only for the purpose(s) identified in the original application;
5. Appropriate headers or footers are included in the Emails and/or File Transfers;
6. Confidential Information is not written in the subject line of the Emails;
7. The word, “Confidential” is typed in the subject line of the Emails;
8. Prepared contact lists are used whenever possible; and
9. Emails are appropriately saved.
10. A copy of this self-audit may be requested by the Privacy & Data Access Office.

C. Record Retention

In accordance with the Public Records Law, all substantive Emails must be preserved. While portions of any Emails sent pursuant to this procedure are likely exempt from disclosure because they contain Confidential Information identifying an individual, they still must be saved pursuant to the statewide Retention Schedule. The Bureau should either print a copy for inclusion in the individual’s file or save the message in an Outlook archive file backed up to network storage. Email containing Confidential Information may only be saved on DPH-owned computers unless the computer is otherwise approved by ITS Services for use with DPH Confidential Information. Emails containing Confidential Information should not remain in the workforce member’s inbox.

D. Security Incidents

Any privacy or security incidents, including unauthorized transmissions, should be immediately reported to the reporting workforce member’s supervisor (see Procedure #2, Breaches of Confidential Information) and the Help Desk. A Privacy Incident Report should be submitted to the Privacy and Data Access Office.

Important Note: Recipients of Emails containing Confidential Information, including SFED users, may not open SFED incoming Email in public areas on Personal Digital Assistants (e.g., blackberries) or laptop computers.

Procedure 11 Individual Rights Related to Confidential Information

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes the rights of data subjects[1] relating to the confidential information collected, used, and disclosed by the Department. These include the right to request:

- Access to confidential information;
- Amendment of confidential information;
- Communication with the Department through alternative means; and
- Restrictions on the use and disclosure of confidential information.

This procedure applies to both covered and non-covered components of the Department and all Department workforce members. As described below, there are certain limitations on these rights imposed by state and federal laws as well as certain requirements that relate only to covered components.

PART II. Access to Confidential Health Information

Generally, the Department must inform a requesting data subject if it maintains any confidential information relating to the data subject, and must subsequently make the confidential information available to the data subject. As described in section II.C below, the right of access is restricted in limited situations. Sample letters referenced in this procedure may be found on HealthNet (http://healthnet.dph.state.ma.us/privsec/forms/forms.htm - *Available to MDPH Intranet users only*)

A. Request in Writing

A data subject's request for access must be made in writing, preferably using the form *Request for Access to Confidential Information*. The request must:

- Provide sufficient information to identify the information sought;
- Specify whether the data subject wants either to inspect or receive a copy of his or her confidential information; and
- The data subject's contact information.

B. Granting Access

1. Provide information to data subject

Unless access is restricted as described in section II.2, MDPH must provide the data subject with access to confidential information in:

- The form or format requested if it can be produced in such form or format;
- A readable hard copy or other form or format as mutually agreed to by MDPH and the data subject; or

[1] All rights in this procedure may be exercised by a data subject's personal representative, provided that the personal representative is authorized for that purpose, as described in Procedure # 9: Verification of Individuals or Entities Requesting Access to Confidential Information.

- A summary of the requested information instead of the actual information if the data subject agrees in advance to the summary and to any fees associated with the summary.

2. Explain request process to the data subject

- The Bureau may discuss with the data subject the scope, format, time, and location for review, and other aspects of the request to facilitate access;
- Only one copy is required if the same information is maintained in more than one place;
- The identity of the data subject must be verified prior to granting access as described in Procedure # 9: Verification of Individuals or Entities Requesting Confidential Information;
- When providing the data subject access to his or her confidential information, MDPH shall remove personal identifiers relating to third-parties, except where a third-party is an officer or employee of the government acting in an official role.

C. Denying Access

1. Notice

If access to confidential information is denied in whole or in part, MDPH will provide the data subject:

- Access to any other confidential information that is not subject to the exceptions to access listed below;
- A timely written denial including the basis for the denial; and
- A statement of the data subject's right for review of the denial as described below.

2. Grounds for Denying Access

A data subject shall be denied access to confidential information in the following circumstances:

(1) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. This information may be withheld until the holder completes its investigation and commences an administrative or judicial proceeding, or for one year from the commencement of the investigation, whichever is first.

(2) When access to confidential information is restricted by law, including but not limited to information subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), and confidential statistical birth information.

(3) Confidential information contained in psychotherapy notes.

(4) Confidential information created or obtained by MDPH in the course of research currently in progress, provided that:

- The data subject agreed to the temporary denial of access when consenting to participate in the research that includes treatment; and
- MDPH informed the data subject that the right of access will be reinstated upon completion of research.

(5) When a licensed health care professional determines in the exercise of professional judgment that the requested access is:

- Reasonably likely to endanger the life or physical safety of the data subject or another individual; or
- Reasonably likely to cause substantial harm to the data subject or another individual.

3. Right of Review

The MDPH Privacy and Data Access Office will process a data subject's request for a review. If the denial was based on any reason other than a restriction by statute, the request for review of the denial of access will be assigned to an MDPH manager who did not participate in the decision under review.

PART III. Amendment of Confidential Information

A data subject has the right to request that MDPH amend his or her confidential information maintained by the Department if the data subject believes the information is incorrect or incomplete. MDPH may deny a requested amendment for the reasons described in part II,A,3,b. In addition, the right to request amendment of confidential information does not apply to the amendment of any personal data for which the process for amendment is established in statute or regulation. For covered components, this also includes the right to amend confidential information held by a business associate.

A. Request in Writing

Requests must be made in writing, preferably using the form *Request for Amendment of Confidential Information*. The request must include:

- Sufficient information to identify the requested amendment;
- The reason(s) to support the amendment;
- Any individuals or entities identified by the data subject as having a need to know of the amendment; and
- The data subject's contact information.

B. Granting an Amendment

1. Document amendments

If there is no disagreement about the requested amendment, a signed and dated notation will be made in the appropriate file. The amendment form should be attached to the information that was amended. Bureaus may develop alternative means of recording amendments to confidential information for both electronic and paper-based records.

2. Completed amendments distribution:

- The data subject, indicating that an amendment was made;
- Individuals identified by the data subject as having a need to know; and
- Any other individuals who reasonably can be identified as having received the confidential information, including business associates of covered components, that may have relied or may rely on the information to the detriment of the data subject.

C. Denying the Amendment

1. Notice

MDPH may deny a requested amendment for the reasons described in part II,A,3,b. If the amendment is denied, MDPH must provide the data subject with a timely written denial including:

- The basis for the denial;
- A statement that the request for amendment will be included in any subsequent disclosure of the disputed information;
- The data subject's right to submit a written statement disagreeing with the denial and a description of how a statement may be filed; and
- A statement that the data subject's disagreement, along with any MDPH rebuttal, will be included in any subsequent disclosure of the disputed information. Any rebuttal will be provided to the data subject.

2. Grounds for Denial

Acceptable reasons for denying a requested amendment include:

- The information was not created by MDPH;
- The information is subject to specific amendment procedures pursuant to statute or regulation;
- The information is not part of the data subject's record as maintained by MDPH;
- The information is not available for inspection pursuant to MDPH's policy regarding access; or
- The information is accurate and complete.

D. Amendment of Confidential Information by Non-MDPH Entities

A Bureau that is informed by another entity about an amendment to confidential information held by, but not created by the Bureau, shall amend the information by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.

PART IV. Communications by Alternate Means

A data subject has the right to request that he or she receive correspondence from MDPH at an address, telephone number, or by means other than those associated with the subject's home address.

A. Request in Writing

The request must be made in writing, preferably using the *form Request for Alternative Means of Communications*. While a Bureau shall not require an explanation, the data subject must identify:

- The specific communications for which the data subject is making the request;
- A clear alternative means of communication; and
- The data subject's contact information.

B. Granting or Denying the Request

- MDPH is not required to agree to communicate by the requested means; all reasonable requests, however, should be granted. In making this determination, Bureaus may consider, for example, the expense and administrative burden involved with compliance and whether the alternative means is sufficiently effective in communicating with the data subject.
- If the request is granted, the Bureau will notify the data subject that the alternate address and/or telephone number will be used for the specified communications between MDPH and the data subject. The alternate address and/or telephone number will remain in place until changed by the data subject.
- The Bureau granting the request must clearly identify the alternative means of communication on the individual's record(s), whether it is paper or electronic.
- The Bureau must also provide notice of the data subject's alternate means of communication to the billing department and/or any other departments, providers, and business associates as applicable, who may be sending communications on behalf of the Bureau.
- If the request is denied, the Bureau making the determination should send the denial to the requested alternative means of communication. The data subject should be informed that all future communications will be directed to the previously listed means of communication.

PART V. Restrictions on the Use and Disclosure of Confidential Information

A data subject has the right to request restrictions on the use and disclosure of his or her confidential information. Such a restriction, however, does not restrict the following uses or disclosures:

- To the data subject;
- To those otherwise permitted or required by law;
- For public health activities; and
- For health oversight activities.

A. Request in Writing

All requests must be made in writing, preferably using the form *Request for Restrictions on Use and Disclosures of Confidential Information*. The request must identify:

- The data subject and the specific confidential information to be restricted;
- To whom the restriction applies; and
- The data subject’s contact information.

B. Granting or Denying the Request

MDPH is not required to agree to a restriction. Bureaus should consider whether the request is reasonable. In making this determination, Centers may consider, for example, the expense and administrative burden involved with compliance. If the Bureau does not agree to the request for restriction, the data subject shall be notified in writing. If the Bureau agrees to the request for a restriction, it agrees to the following:

- MDPH may not use or disclose confidential information in violation of the restriction, except to a health care provider when the individual who requested the restriction is in need of emergency treatment and the restricted confidential information is needed to provide the emergency treatment.
- If restricted confidential information is disclosed to a health care provider for emergency treatment, MDPH must request that such health care provider not further use or disclose the information.
- The subject of the confidential information must be given notice of such access upon termination of the emergency.

C. Terminating a Restriction

A restriction on the use and disclosure of confidential information may be terminated if:

- The data subject agrees to or requests the termination in writing;
- The data subject orally agrees to the termination and it is documented; or
- MDPH informs the data subject that it is terminating its agreement to a restriction and the termination is effective with respect to protected health information created or received after the individual is informed.

PART VI. Bureau Requirements: Administration and Documentation

A. Designations and Procedures

Each Bureau must designate an individual(s) responsible for receiving and processing requests related to data subjects' individual rights. Bureaus must also develop internal procedures to comply with the requirements of this procedure.

B. Submission and Coordination of Requests

- All individual rights requests must be made to the Bureau maintaining the data subject's confidential information. All Bureaus must keep a log of all requests for individual rights made under this procedure.
- All responses to requests should be made on the back of a copy of the original request, or on a page attached to a copy of the request.
- All original request forms and responses will remain a part of the data subject's record and shall be maintained as long as the underlying record is required to be maintained by the Commonwealth's record retention policies, or for six years, whichever is longer.
- If the request involves confidential information maintained by more than one Bureau or by a covered and non-covered component of the same Bureau, the Bureau that received the request should forward a copy of the request to the Privacy and Data Access Office, which will coordinate the processing of the request.

C. Email or Telephone Requests by Data Subjects

Data subjects making a request by telephone or e-mail to exercise their individual rights should be sent a copy of the applicable form.

D. Timely Review

Bureaus shall respond to all requests within thirty days of receipt of the written request. For request for access to information that is not maintained or accessible

on-site, the response shall be no later than sixty days. One thirty-day extension is allowed provided that the data subject is notified of 1) the reason for the delay and 2) the date the Department will comply with the request.

E. Fees

Bureaus may charge data subjects for the cost of postage, $0.20 a page for photocopies, and the actual cost incurred for the duplication costs associated with non-paper records, e.g., CDs. If a summary of the confidential information was agreed to by the data subject, the agreed-upon cost of the summary should be charged. MDPH Hospitals shall follow established hospital fee schedules..

F. Covered and Non-Covered Component Response Forms

All forms are specific to covered and non-covered components:

- Covered Components (labeled with the prefix CC): reflects the ability of data subjects to file complaints with MDPH's Privacy and Data Access Office or to the Secretary of Health and Human Services.
- Non-Covered Components (labeled with the prefix NCC): reflects that data subjects may file a complaint only with MDPH's Privacy and Data Access Office.

G. Documentation

Bureaus must document the designations and procedures required under this procedure. This documentation must be maintained for a minimum of six years or as required by the Massachusetts Records Conservation Board.[2]

Authority:

M.G.L. c. M.G.L. c.66A, §§ 2(i) and (j);

45 C.F.R. §§ 164.522, 164.524, and 164.526.

Recommended forms:

Request for Access to Confidential Information
Request for Amendment of Confidential Information
Request for Alternative Means of Communication
Request for Restrictions on Use and Disclosures of Confidential Information

For recommended forms: See Healthnet, look under the Privacy & Data Access pages, forms may be found under “Model Forms.” (Available to MDPH Intranet users only)

[2] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

(Page intentionally blank)

Procedure 12 Accounting of Disclosures

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes the procedures Bureaus should follow in response to requests by data subjects for an accounting of the disclosures of their confidential information.

This procedure applies to both covered and non-covered components of the Department and all Department workforce members. As described below, there are specific requirements that relate only to covered components and their workforce members.

PART II. General Requirements

Generally, each data subject has a right to request and receive a descriptive list, known as an accounting, of all the disclosures of his or her confidential information made by the Department.[1] However, Bureaus are not required to account for disclosures made:

- Directly to the data subject or the data subject's personal representative;
- Pursuant to an authorization;
- Related to treatment, payment, and operations;
- Pursuant to national security or intelligence purposes;
- To correctional institutions or law enforcement officials as permitted under law;
- Incident to a disclosure that is otherwise not required to be included in the accounting;
- As part of a limited data set as described in Procedure #7: Requirements for De-Identification, Limited Data Sets and Aggregate Data;
- Limited to information that is de-identified in accordance with consistent with Procedure #7;
- In response to a public records request that have been redacted in accordance with Procedure # 8: Public Records Release Standards for MDPH Documents Containing Medical Information; and
- Made prior to April 14, 2003.

Questions about whether a particular disclosure must be included in an accounting of disclosures should be referred to the Bureau privacy liaison first and then the Privacy Officer.

[1] The accounting requirements apply only to the release of confidential information that is defined as a disclosure under Procedure # 3: Use and Disclosure of Confidential Information. Since unrestricted identifiable vital record information disclosed by the Registry of Vital Records and Statistics is not considered confidential information, no accounting is required for such disclosures.

PART III. Accounting Requirements for Covered Components

Covered components must also account to the data subject for disclosures made:

- By business associates as described in Procedure # CC-2: Business Associate Agreements; and
- To another covered or non-covered component of the Department as described in Procedure # 3.

PART IV. Implementation: Bureau Responsibilities

DPH Bureaus shall develop procedures for maintaining the record of disclosures necessary to produce an accounting. This record may be combined with the Record of Disclosure required in Procedure # 3. This requirement can be met by:

- Maintaining a paper or electronic disclosure log which tracks each disclosure required in an accounting as they are made; or
- Compiling the required accounting upon receipt of a data subject's request utilizing existing Bureau records.

A. Submission of the Request

A data subject's request for an accounting must be made in writing, and if possible, using the form, *Request for Access to Confidential Information*.[2] Any request for an accounting of disclosures shall include the following:

1. The name of the data subject making the request;
2. Identification of programs or records for which the data subject is seeking an accounting; and
3. The time period, for which the accounting is based, not to exceed six years prior to the date of the request, or for disclosures made prior to April 14, 2003.

B. Review of Requests

Upon receipt of a request for an accounting of disclosures, DPH Bureau shall review the request and prepare the accounting. If the accounting is for confidential information from more than one Bureau, or for covered and non-covered components within the same Bureau, the Bureau receiving the request should contact the Privacy Officer, who will coordinate the response. The Privacy Officer shall also process requests for Department-wide accountings.

C. Temporary Suspension of Accounting

In limited circumstances, there may be a temporary suspension of a data subject's right to receive an accounting due to a request from a health oversight agency or a law enforcement official. All requests to suspend an accounting of a data subject's confidential information should be referred directly to the Office of General Counsel or the Privacy & Data Access Office. If the request is deemed valid, the accounting will be temporarily suspended.

1. Requests in Writing

If the request for the temporary suspension of the individual's right to receive an accounting is in writing and includes a statement of the reasons that an accounting would likely impede the requestor's activities and includes the time

[2] Versions of the form specific to covered and non-covered components are available at http://healthnet.dph.state.ma.us/privsec/forms/forms.htm (available to MDPH Intranet users only).

period for such a suspension, the Department will grant the request for the suspension. The suspension shall not exceed one year from the initiation date of the requestor's investigation.

2. Oral Requests
If the request is made orally, Bureaus shall attempt to obtain it in writing. If this is not possible, the oral request should be documented by the Bureau, listing the verified identity[3] of the individual making the request for suspension, and the reasons for the request. If the request is deemed valid, the data subject's right to an accounting will be suspended for no more than thirty days unless a written request submitted during that time frame specifies the time frame required for the suspension.

D. Content of Accounting: General Requirements

The accounting provided for each data subject's request must include the following information for each disclosure made during the time period requested:

1. The date of the disclosure;
2. The name of the entity or person who received the confidential information and, if known, the address of such entity or person;
3. A brief description of the confidential information disclosed; and
4. A brief statement of the purpose of the disclosure that reasonably informs the data subject of the basis for the disclosure. In lieu of such a statement, a copy of the written request for the disclosure made can be provided.

E. Accounting for Multiple Disclosures

If during the requested period for accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting does not need to list each disclosure in detail. Rather, the accounting may list:

- The first and last dates of the series of disclosures,
- The frequency or number of disclosures, and
- Elements 2, 3, and 4 listed in section IV.D.

F. Accounting for Research

Unless the information disclosed is de-identified or constitutes a limited data set, Bureaus must account for disclosures made for research purposes. The content of the accounting for research depends on the number of participants in the research study.

1. 50 or fewer Participants
Each Bureau that discloses confidential information for a research study involving 50 or fewer participants must provide an accounting of each disclosure in accordance with the requirements of section IV.D and section IV.E.

2. 50 or more Participants
If confidential information about the individual requesting the accounting may have been disclosed as part of a research study involving more than 50 participants, the following information must be included in the accounting:

[3] The requestor's identity should be verified in accordance with Procedure # 9: Verification of Individuals or Entities Requesting Confidential Information.

- The name of the protocol or research activity;
- A description, in plain language, of the protocol or activity including its purpose and the criteria for selecting particular records;
- A brief description of the type of confidential information disclosed;
- The date or time period during which the disclosures occurred or may have occurred, including the last disclosure date;
- The name, address, and phone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
- A statement that the confidential information may or may not have been disclosed for a particular protocol or other research activity.

G. Bureau Designations

All Bureaus shall designate one or more individuals to be responsible for maintaining the log of disclosures required by Procedure # 3, as well as responding to requests for an accounting of disclosures. Bureaus may choose to do this at the Bureau or program level.

H. Documentation

Bureaus must maintain the following documentation for a minimum of six (6) years, or longer if required by the Commonwealth's Records Conservation Board:[4]

- A copy of the current and previous versions of the procedures necessary to produce an accounting;
- A list of the designated individual(s) responsible for implementing the procedures for accounting; and
- A record of all requests for an accounting and all responses to these requests.

The documentation must be made accessible to the Privacy & Data Access Office upon request.

I. Fees

The first request for an accounting within a 12-month period is free. The following is the fee structure for subsequent requests:

1 year of accounting $2.00	4 years of accounting $5.00
2 years of accounting $3.00	5 years of accounting $6.00
3 years of accounting $4.00	6 years of accounting $7.00

Authority:

M.G.L. c. 66A, §§ 2(f), (g) and (i)

45 C.F.R. § 164.528

For a suggested Accounting of Disclosure form: See Healthnet, look under the Privacy & Data Access pages, forms may be found under "Model Forms." (available to MDPH Intranet users only)

[4] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Procedure 13 Complaints Regarding the Use and Disclosure of Confidential Information

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes a data subject's right to file a complaint if he or she believes his or her rights under the Department's Confidentiality Policy and Procedures have been violated.

This procedure applies to both covered and non-covered components of the Department.

PART II. Process for Filing a Complaint[1]

A. General Requirements

1. When feasible, all complaints must be filed in writing on the Department's privacy complaint form[2] and sent to:

   Massachusetts Department of Public Health
   Privacy & Data Access Office
   250 Washington St., 2nd Floor
   Boston, MA 02108

2. All complaints must be filed within 180 days of when the individual knew or should have known of the alleged violation.

3. Questions about filing complaints should be referred to (617) 624-5194.

B. Requirements for Covered Components

In addition to registering complaints with MDPH, individuals may register a complaint with the U.S. Department of Health and Human Services at:

Office for Civil Rights
US Dept. of Health and Human Services
J.F. Kennedy Federal Building-Room 1875
Boston, MA 02203
Telephone (617) 565-1340
Fax (617) 565-3809; TDD (617) 565-1343

PART III. Investigation of Complaints

Upon receipt of a complaint, the Privacy Officer, in consultation with the Director of the Bureau involved in the complaint, shall take the following steps:

1. Consult with the Bureau Director or Hospital Director, if necessary, and determine whether the complaint should be investigated by the Center's privacy liaison, the Hospital privacy officer, or the DPH Privacy Officer, based on the nature of the alleged facts. In most instances, the complaint will be investigated by the Bureau or the Hospital;

[1] Complaints relating to DPH Hospitals or the State Office of Pharmacy Services, and all questions regarding their respective complaint procedures must be submitted to their respective privacy offices.
[2] The Privacy Complaint forms for both covered and non-covered components are available at: http://healthnet.dph.state.ma.us/privsec/forms/forms.htm.

2. Interview the individual who filed the complaint to ensure a full understanding of the alleged violation;
3. Meet with workforce members, as applicable, who have knowledge of the complaint or issues associated with it;
4. Complete a draft response containing proposed findings, and forward it to the appropriate Bureau or Hospital director, or his/her designee, for review and approval;
5. Send the final response to the complainant and maintain a copy in the Privacy & Data Access Office's files for six years or longer if required by the Records Conservation Board.[3]
6. Maintain a log that documents all complaints received, the disposition, and the date of disposition.

Authority:

M.G.L. c. 66A, § 2

45 C.F.R. § 164.530(d)

For covered and non-covered components forms: See Healthnet, look under the Privacy & Data Access pages, forms may be found under "Model Forms." (available to MDPH Intranet users only)

[3] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Procedure 14 Confidentiality Agreements

Version: 1 Effective Date: June 1, 2009

PART I. Purpose & definitions

A. Introduction

This procedure provides instructions regarding the use and construction of confidentiality agreements.

B. Purpose

Bureaus and programs that contract with individuals or entities that receive or create Confidential Information on behalf of DPH are responsible for ensuring that Confidentiality Agreements are executed. This includes the Standard Terms & Conditions Agreement, the Human Services Terms & Conditions Agreement, Statewide Master Agreements, and Statements of Work.

Templates are available for bureau convenience. Where appropriate bureaus should add language to address their specific privacy and security concerns, but the core language in the templates may not be deleted. Bureaus and programs are encouraged to work with privacy liaisons, attorneys, or the Privacy and Data Access Office in the development of Confidentiality Agreements.

C. Definitions

1. Confidential Information

Any individually identifiable information, including, but not limited to, medical and demographic information, that:

- Reveals the identity of the data subject or is readily identified with the data subject, such as 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 data subject.

2. Confidentiality Agreements

Legal documents that establish privacy and security protections that must be put in place with a Vendor that receives Confidential Information from or creates Confidential Information on behalf of DPH pursuant to a contract. They include provisions on how the Confidential information must be protected, who owns the data, whether the data may be disclosed, and limitations on publication and research.

3. Vendor

For the purposes of this procedure, Vendors include, unless otherwise specified, all DPH consultants, contractors, providers, and vendors. Contracted employees are excluded from this procedure.

Massachusetts Department of Public Health
Confidentiality Procedures – Procedure 14

PART II. Which Form to Use

Agreement templates are available on the Privacy & Data Access Office page (available to DPH intranet users only). Follow this algorithm to determine which form to use:

If …	Then …
Your Vendor is not receiving or creating confidential information on your behalf pursuant to the contract.	You do not need to execute a Confidentiality Agreement or a Business Associate Agreement.
You are a DPH Hospital and the contract involves the receipt or creation of confidential information.	Use the form, BAA Hospitals – Standard Terms & Conditions. Additional procedural information is found in Procedure CC 2, Business Associate Agreements.
You are another DPH covered entity and the contract involves the receipt or creation of confidential information.	Use the form, BAA Non-Hospital – Standard Terms & Conditions. Additional procedural information is found in Procedure CC 2, Business Associate Agreements.
Your Bureau/Program's contract is written using the Commonwealth's Terms & Conditions and the contract involves the receipt or creation of confidential information.	Use the form, Confidentiality Agreement – Standard Terms & Conditions and the appended Confidentiality Pledge. One pledge should be signed for each individual authorized to access confidential information.
Your Bureau/Program's contract is written using the Commonwealth's Human & Social Services Terms & Conditions and the contract involves the receipt or creation of confidential information.	Use the form, Confidentiality Agreement – Human Services Terms & Conditions.
Your Bureau/Program's contract is written using the Statement of Work and the contract involves the receipt or creation of confidential information.	Use the form, Confidentiality Agreement – Standard Terms & Conditions and the appended Confidentiality Pledge.

PART III. Completing the Confidentiality Agreement

A. Bureau/Program Initiation.

The following sections of the Confidentiality Agreement must be completed by the contracting Bureau/Program before providing it to the Vendor:

1. Section I. General Provisions

Indicate the RFR number or some other reference to the RFR or state-wide contract that will connect it to the underlying RFR or contract

- The name of the contracting DPH program or bureau
- The name of the Vendor

If the underlying contract does not clearly describe the work of the vendor that relates to its receipt or creation of confidential information, the program or bureau must clearly describe what the vendor will be doing for the Department. This is

particularly important when the Vendor is engaged from a state-wide contract or a master service agreement.

2. **Section 1 A. Permitted Uses and Disclosures**
   Select whether the Vendor is authorized under the terms of the contract to disclose Confidential Information or not. This is an essential provision of the agreement. If you have any question about how to respond to this section, contact the PDAO.

3. **Vendor Signature.**
   The Vendor completes the appropriate sections of the Confidentiality Agreement and returns it to the Department. Although it is the Contractor's decision who signs the Confidentiality Agreement, DPH staff are encouraged to ensure that the signing individual ahs sufficient authority to enforce the agreement.

4. **Department Signature**
   The Department does not need to sign this document, since only the Vendor incurs obligations under this agreement. If a Business Associate Agreement is signed, the Department is required to sign the agreement. See Procedure CC2.

B. The Confidentiality Agreement Paper Flow

Type of RFR	Provide the Confidentiality Agreement to Vendor	Bidder should submit the signed Confidentiality Agreement to DPH …
DPH Individual Bureau RFR	With the RFR at the time of procurement	As part of the Vendor response to the RFR
DPH Master Agreement RFR	Single Confidentiality Agreement at the time of procurement	At time of Vendor hire or commencement of services with DPH
DPH Master Agreement	At time of engagement	Before Vendor has access to Confidential Information
OSD state-wide master agreement contract	At time of engagement at DPH	Before Vendor has access to Confidential Information
OSD master agreement that changes to require use of Confidential Information	At time when scope of work changes to require collection of confidential data	Before Vendor has access to Confidential Information

C. Confidentiality Pledges

Confidentiality Pledges are used only in conjunction with Standard Terms and Conditions Contracts (not Human Service Contracts). Any member of the Vendor's staff who will access Confidential Information must sign a Confidentiality Pledge before accessing such information.

The individual signing the Confidentiality Agreement on behalf of the Vendor is responsible for obtaining Confidentiality Pledges signed by his/her employees and making them available to DPH upon request. The DPH contract manager can and should also collect them as part of the contract management process.

The Confidentiality Pledge is appended to the Standard Terms and Conditions Confidentiality Template. This template is on the Privacy & Data Access Office web

page (available to DPH intranet users only). Bureaus may add language to address their specific privacy and security requirements for specific projects.

D. Resources Available

Bureau/Program Privacy Liaison; Program Attorney; Privacy and Data Access; Office; POS Office

Procedure CC-1 Notice of Privacy Practices

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure describes the requirements related to the provision of a Notice of Privacy Practices (Notice) by the Department's covered components. Specific requirements related to providing and distributing the Notice depend on the type of covered component as described in section V. All workforce members in the Department's covered components must comply with this procedure.

PART II. General Requirements

Under the Privacy Rule, a data subject has a right to adequate notice of:

- The uses and disclosures of his or her confidential health information that may be made by or on behalf of the covered component; and,
- The data subject's rights and the covered component's legal duties with respect to the data subject's confidential health information.

There is no model Notice for the Department. Rather, each component must create its own Notice incorporating the requirements listed below.

PART III. Required Content

The Notice must be written in plain language and include the following heading:

> "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

The Notice must include the following content:

A. Uses and Disclosures

The Notice must include descriptions of the following elements written in sufficient detail to describe the uses and disclosures of confidential information that may be made by the covered entity and of the individual's rights and the covered entity's legal duties with respect to confidential information.

1. A description of the types of uses and disclosures that the covered component is permitted to make for purposes of treatment, payment, and health care operations, including at least one example for each;
2. A description of each of the other purposes for which the covered component is permitted or required to use or disclose confidential health information without a data subject's authorization;
3. A description of any restrictions on the use and disclosure of confidential information limited by any state or federal laws, which are not preempted by HIPAA and which are more stringent than HIPAA;
4. A statement that other uses or disclosures will be made only with the data subject's written authorization, and that an individual's authorization may be revoked as provided for in the Privacy Rule;

5. A separate statement describing if a provider intends to contact the data subject for appointment reminders, treatment alternatives, or other health-related benefits; and

6. Although not mandated, a description that confidential health information may be disclosed to business associates is recommended.

B. Rights of the Data Subject

1. A statement of the data subject's rights with respect to confidential health information and a description of how the data subject may exercise these rights must be included in the Privacy Notice including:

   - The right to restrictions on certain uses/disclosures of confidential health information, including a statement that the covered component is not required to agree to a requested restriction;
   - The right to receive confidential communications of confidential health information;
   - The right to inspect and copy confidential health information;
   - The right to amend confidential health information;
   - The right to receive an accounting of disclosures of confidential health information; and,
   - The right to receive a paper copy of the Notice of Privacy Practices.

2. A statement that data subjects may complain to the covered component and to the Secretary of U.S. Department of Health and Human Services about privacy violations, including a brief description of how a complaint may be filed and a statement that the data subject will not be retaliated against for filing a complaint; and

3. The name or title and the telephone number of the person or office for further information related to the covered component's complaint process.

C. Obligations of the Covered Component

1. A statement that the covered component is required by law to maintain the privacy of confidential health information and to provide data subjects with notice of its legal duties and privacy practices with respect to protected health information;

2. A statement that the covered component is required to abide by the terms of the Notice currently in effect; and

3. A statement that the covered component reserves the right to change the terms of the Notice and to make the new Notice provisions effective for all confidential health information that it maintains and a description of how the covered component will provide data subjects with a revised Notice.

D. Effective Date

The Notice must include the effective date, which may not be earlier than the date on which it is first printed or published.

PART IV. Revisions

The covered component must promptly revise and distribute the Notice when there is a material change to its uses or disclosures of confidential information, the data subject's rights, the covered components legal duties, or other privacy practices described in the Notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the Notice reflecting the change.

PART V. Provision and Distribution of the Notice

A. Covered component health plans

Covered component health plans need only provide their Notice to the data subject who is the named insured. The Notice must be distributed as follows:

1. No later than April 14, 2003, for data subjects covered by the plan at that time;
2. For new enrollees, at the time of enrollment;
3. Within 60 days of a material revision to the Notice, to data subjects then covered by the plan; and
4. At least once every 3 years, data subjects covered by the plan must be notified of the availability of the Notice and how to obtain the Notice.

B. Direct health care providers

Covered component direct health care providers are required to affirmatively provide the Notice only when there is a direct treatment relationship with the data subject. The Notice must be distributed as follows:

1. No later than the date of the first service delivery, after April 14, 2003, or as soon as reasonably practicable in an emergency situation;
2. The covered component provider shall make a good faith effort to obtain a written acknowledgement of receipt of the Notice from the data subject or document why acknowledgment was not obtained;
3. Post the current Notice in effect, and make copies available, at the service delivery site;
4. Post the current Notice in effect on the covered component's web site; and
5. Upon revision, make the revised Notice available upon request and prominently post the Notice at the site of service delivery.

C. Indirect health care providers

Covered component indirect health care providers such as clinical laboratories, are only required to distribute a Notice upon request.

D. Distribution by Business Associates[1]

A covered health care component can make arrangements with a business associate (BA) to distribute its Notice. However, the covered component remains responsible for the Notice.

[1] Procedure # CC-2: Business Associate Agreements describes the contractual requirements between programs and their BAs in detail.

If a MDPH covered component arranges for its BA to distribute the Notice, this must be explicitly stated in the BA agreement, along with a requirement that the BA demonstrate full compliance with this obligation. If the BA is a provider on the covered component's behalf, it will need to make a good faith effort to obtain an acknowledgement of receipt of the Notice and maintain or provide to the covered component the acknowledgement documentation.

PART VI. Documentation Requirements

The covered component must retain the following documentation for six (6) years, or longer if required by the Commonwealth's Records Conservation Board[2]:

- Copies of all Notices issued, including those no longer in effect; and
- Copies of written acknowledgments or the documentation of good faith efforts to obtain acknowledgment.

Authority:

45 C.F.R. § 164.520

[2] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Procedure CC-2 Business Associate Agreements

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure provides instructions to all covered components regarding the necessity for and the required content of agreements with a business associate (BA). It pertains to the BA's receipt, use and development of confidential information from or on behalf of the MDPH covered component.

Programs that are not covered components are not required to enter into business associate agreements; however, if they contract with a vendor or provider to share or create confidential information on behalf of the Department, they must ensure that the contractor or vendor signs a confidentiality agreement as part of the contract. While both the BA and the confidentiality agreements are designed to protect the privacy and security of the Department's data, the main difference is that only the BA ties into the HIPAA Privacy Rule.

PART II. General Requirements

The covered component may disclose confidential information to a BA or allow a BA to create or receive confidential information on the covered component's behalf if the covered component obtains adequate assurance that the BA will appropriately safeguard the confidential information. Such assurances shall be included in the underlying contract, an amendment to the underlying contract, or a separate Business Associate Agreement (BAA).

- Each covered component should evaluate every contract it maintains where there is access to confidential health information utilizing the Department's BA decision-tree.
- Once a BA is identified, the covered component should work with the Office of the General Counsel to adapt the Department's model business associate agreement for the particular BA relationship.
- Each BA agreement, along with the underlying contract, should be maintained by the covered component for six years, or longer if required by the Commonwealth's Records Conservation Board.[1]

PART III. Exceptions to the BAA Requirements

The BAA requirements do not apply to:

1. Disclosures by a covered entity to a health care provider for treatment of an individual;
2. Uses or disclosures made to another governmental agency for purposes of public health eligibility or enrollment determinations where such agency is authorized by law to make these determinations;
3. Contracts with persons or organizations whose functions do not involve the use of confidential information; or

[1] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

4. The disclosure of confidential information to a researcher for research purposes either with an authorization, pursuant to a waiver, or as a limited data set.

PART IV. Required Content

The agreement between the covered component and the BA must include language that provides the business associate will:

1. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
2. Use appropriate safeguards to prevent unauthorized use or disclosure of the information;
3. Report unauthorized uses or disclosures or security breaches to the covered component;
4. Ensure that any agents, including a subcontractor, agree to the same restrictions and conditions that apply to the BA with respect to the confidential information and security protections;
5. Make confidential information available for access by the data subject or his/her personal representative within time frames established in the agreement;
6. Make confidential information available for amendment, and incorporate any approved amendments to confidential information, within time frames established in the agreement;
7. Make available the information required to provide a full accounting of disclosures, except for disclosures to the data subject, to his/her personal representative, or
8. Make its internal practices, books, and records relating to the use and disclosure of individually identifiable health information received from, or created by or on behalf of the organization, available to the U.S. Secretary of Health and Human Services for purposes of determining the covered component's compliance with HIPAA;
9. Return or destroy all confidential information received from, created by, or on behalf of the covered component at termination of the contract, if feasible. If such return or destruction is not feasible and any confidential information is retained, extend the full protections in the BA agreement as long as the confidential information is maintained and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
10. Be subject to termination of the agreement upon the BA's violation of a material term of the agreement.

PART V. BA Agreements When Both Entities are Governmental Agencies

The covered component may comply with this procedure by entering into a Memorandum of Understanding (MOU) or Interagency Service Agreement (ISA) that contains terms that accomplishes the BA agreement objectives.

The covered component may comply with this procedure, without entering into an agreement if other law (including regulations adopted by MDPH or the governmental agency that is the BA) contains requirements applicable to the BA that accomplish the objectives of a BA agreement.

The covered component may omit a termination procedure from the agreement if it is inconsistent with the statutory obligations of the covered component of the agency that is the BA.

PART VI. BA Oversight Responsibility

There is no affirmative responsibility imposed by HIPAA to monitor the BA. If, however, a covered component knows of a pattern or practice of the BA that amounts to a material violation of the BA agreement, the entity must attempt to mitigate the breach or end the violation. If the attempted mitigation is unsuccessful, the covered component shall terminate the agreement if feasible. If termination is not feasible, the covered component must report the problem to the Office of the U.S. Secretary of Health and Human Services.

Authority:

45 C.F.R. § 164.502(e)(1)(ii);
45 C.F.R. § 164.504(e)(2) and (3);
45 C.F.R. § 164.532(e)

For a suggested forms and resources;

Business Associate Agreement Model Forms & Business Associate Decision Tree
See Healthnet, look under the Privacy & Data Access pages, forms may be found under “Model Forms.” (available to MDPH Intranet users only)

(Page intentionally blank)

Procedure CC-3 Designated Record Sets

Version: 3 Effective Date: April 21, 2008

PART I. Purpose and Scope

This procedure defines the Designated Record Set (DRS) for covered components that are health care providers and health plans. The procedure also provides a checklist for covered components to use when determining which part of their confidential health information constitutes the Designated Record Set (DRS). All workforce members in the Department's covered components must comply with this procedure.

Unless otherwise limited, HIPAA requires that a covered component provide an individual, upon request, access to certain health information that constitutes a designated record set as defined below. State law requirements under FIPA may require broader access to records than the HIPAA requirements. A covered component is required to comply with both statutes.

PART II. Definitions

A. DRS for Health Care Providers

A group of records[1] maintained by the provider or for the provider that includes:

1. The records about data subjects maintained by the provider or by a third party for the provider; or
2. Used, in whole or in part, by the provider or by a third party on behalf of provider to make decisions about data subjects.

B. DRS for Health Plans

A group of records maintained by the plan or for the plan that includes:

1. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by the plan, or maintained by a third party for the plan; or
2. Used, in whole or in part, by the plan, or by a third party for the plan, to make decisions about data subjects.

PART III. DRS Checklist

Workforce members should follow the steps in this checklist, which will enable the covered component to identify its DRS.

A. Identify storage sites

Identify the "storage sites" where confidential health information is stored:

- Include both paper and electronic systems;
- Include network and desktop systems;
- Include current files and archived files;2

[1] A record is any item, collection, or grouping of information that includes confidential health information and is maintained, collected, used, or disseminated by or for a covered component.

- Include all sites; and
- Include all record systems in the possession of business associates and other agents.

B. Identify covered components DRS

Identify the following elements of the records that are included in the covered component's applicable DRS as defined in part II.

1. Health Care Providers

For each confidential health information "storage site" identified in part III.A.1, identify those that contain in whole or in part:

- Medical record(s) as defined by the covered component; and
- Billing record(s), including any records that might be developed by contracted vendors, Medicare maximization projects, etc.

2. Health Plans

For each confidential health information "storage site" identified in part III.A.1, identify those that contain in whole or in part:

- Enrollment record(s);
- Payment record(s);
- Claim adjudication record(s); and
- Case or medical management record(s).

3. Identify additional data subject records

Identify any additional records for each storage site which are used to make decisions about the data subject that are not included in part III.A.2.

1. Records which are used in making "decisions" about a data subject. For example, records regarding eligibility for a service, need for intervention, outcome of an appeal, need for medical supervision, or appropriateness for release. *These records are included in a DRS.*
2. Records not used to make decisions about a data subject. For example, records used for such things as tracking utilization, budget reporting, program assessment, "bed check" records, attendance reports, or billing back-up. *These records are not included in a DRS.*

4. Eliminate duplicate records

Sort the records identified in subparts III.A.2 and 3(a), eliminating any duplicate records or redundancies. For example, if all of the information in one record is included in one or more other records, the first record can be eliminated as long as the other record or records remain as part of the DRS.

---

[2] The DRS must go back six years. The time begins "running" as of April 14, 2003. For requests received on or after that date, it is likely the elements of the DRS are not archived. Prospectively, the location of records that are archived more frequently than every six years must be noted so they can be accessed if there is a request for the DRS that reaches back the full six years.

Massachusetts Department of Public Health
Confidentiality Procedures –
Procedure CC-3 Designated Record Sets

5. **Document work**
   Document your DRS as containing all records remaining after step 4.

6. **Determine access exceptions**
   Determine if any part of the DRS meets any of the access exceptions:

   (a) Psychotherapy notes which are defined as those clinical notes maintained by a therapist separately from the medical record, sometimes referred to as "desk drawer notes;"

   (b) Information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding; and

   (c) Confidential health information maintained by the covered component that is:

   - Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 263(a) to the extent the provision of access to the individual would be prohibited by law; or
   - Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 C.F.R. § 493.3(a)(2).

7. **Create business process**
   Create a business process to provide the data subject with access to his or her DRS.

   (a) Determine the process for setting apart records or parts of records, which are exempted from the access requirements.

   (b) If parts of the DRS are maintained at various sites, determine the most efficient manner of collecting them in one location if an access request is made.

   (c) Determine the preferred means of handling access requests made directly to a business associate. For example, should all requests be forwarded to and handled at a central location? Should the business associate be required to have a process for providing access to the records maintained by the business associate? If so, what reporting mechanism is needed to provide a record of those requests and the materials provided?

8. **Provide access as allowed by law**
   If the request for access is limited to a DRS, then the workforce member is only required to provide the DRS. If the data subject requests information outside of the DRS, under state law this should also be provided to the data subject unless there are limits on such access as described to Procedure # 11.

9. **Business process update**
   Create a business process to update the DRS when new confidential health information "storage sites" are created or existing ones are modified or deleted.

Massachusetts Department of Public Health
Confidentiality Procedures –
Procedure CC-3 Designated Record Sets

PART IV. Documentation

A covered component must document and retain the following for six (6) years, or longer if required by the Commonwealth's Records Conservation Board:[3]

- The designated record sets that are subject to access by data subjects; and
- The titles of persons or offices responsible for receiving and processing requests for access by data subjects.

Authority:

45 C.F.R. §§ 164.524; 164.530

[3] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.