HIPPA COMPLIANCE POLICY

PURPOSE: The purpose of this Policy is to ensure the Fire Department ("Department") and members of its workforce comply with the applicable requirements of a health care provider covered entity under the HIPAA Privacy and Security Standards at 45 C.F.R. Parts 160 and 164.

POLICY: It is the Policy of the Fire Department to comply with the requirements of a health care provider HIPAA covered entity in accordance with the Procedure set forth below.

PROCEDURE:

1. HIPAA Administrative Requirements:
   A. Designation of Privacy Officer: The Fire Chief assumes the role of, or shall appoint, the HIPAA Privacy Officer. The HIPAA Privacy Officer and shall be responsible for:
      I. The development, implementation and periodic review of the Fire Department's HIPAA privacy policies and procedures;
      II. Consulting and collaborating with the HIPAA Security Officer in the development and implementation of a security policies and procedures;
      III. Reporting any HIPAA-related compliance issues or concerns to the Fire Chief, and, if the issue or concern relates to the security of a Department patient's electronic protected health information ("ePHI"), to the HIPAA Security Officer.
      IV. Conducting or arranging for HIPAA training for all members of the Fire Department's workforce; and
      V. Other roles and responsibilities specifically assigned to the Privacy Officer under HIPAA, in this Policy, and in any other Department HIPAA policies and procedures.
   B. Designation of Security Officer: The Fire Chief assumes the role of, or shall appoint, the HIPAA Security Officer. The HIPAA Security Officer shall be responsible for the following, in consultation and collaboration with the HIPAA Privacy Officer, and the Fire Chief:
      I. The development and implementation of the Fire Department's HIPAA security policies and procedures;
      II. Reporting any security-related compliance issues or concerns related to Department patients' ePHI to the HIPAA Privacy Officer and to the Fire Chief; and
      III. Other roles and responsibilities specifically assigned to the Security Officer under HIPAA, in this Policy, in any other Department HIPAA policies and procedures.

C. Designation of a Contact Person: The HIPAA Privacy Officer shall also serve as the Department's designated Contact Person responsible for:

   I. Receiving, investigating and responding to HIPAA-related privacy and security complaints from patients and persons involved in their care; and

   II. Providing further information in response to queries about matters covered by the Department's HIPAA Notice of Privacy Practices.

D. Documentation of Designations: The Fire Chief's appointment of HIPAA Privacy Officer, HIPAA Security Officer and HIPAA Contact Person will be recorded by the Department in MEFIRS for six (6) years from (a) the date when such appointments terminate, or (b) the date this policy expires; whichever is first.

E. HIPAA Training: The HIPAA Privacy Officer shall be responsible for providing or arranging for training for all members of the Department's workforce on protecting patients' PHI and on the Department's HIPAA policies and procedures, as necessary and appropriate for the members of the Department's workforce to carry out their job-related functions and responsibilities within the Department. Such training shall be provided as follows:

   I. To each member of the Department's workforce on an annual basis;

   II. To each new member of the Department's workforce (including students, trainees and volunteers) within a reasonable period of time after the person joins the Department's workforce; and

   III. To each member of the Department's workforce whose functions are affected by a material change in the policies or procedures relating to PHI, within a reasonable period after the material change becomes effective.

   IV. The HIPAA Privacy Officer shall be responsible for documenting that such training has been provided to each member of the Department's workforce. HIPPA training is mandatory for all members of the Department's work force.

F. Security and Privacy Safeguards: The HIPAA Privacy Officer and Security Officer shall be responsible for ensuring that the Department (i) has in place appropriate administrative, technical and physical safeguards to protect the privacy of Department patients' PHI, (ii) reasonably safeguards such PHI from any intentional or unintentional use or disclosure that is in violation of HIPAA's requirements, and (iii) reasonably safeguards such PHI to limit incidental uses and disclosures made pursuant to an otherwise permitted or required use or disclosure.

G. HIPAA Complaints: Department patients have the right to make complaints to the Department regarding alleged violations of their privacy rights. The HIPAA Privacy Officer, acting as the HIPAA Contact Person, shall be responsible for responding to individuals who make complaints concerning the Department's HIPAA policies and procedures or the Department's compliance with such policies and procedures. The

Privacy Officer shall document all complaints received, investigate such complaints to determine whether they are substantiated or unsubstantiated, respond in writing to persons making such complaints within a reasonable period of time after receipt of the complaint, and document each complaint's final disposition, if any.

H. Sanctions for Violations of HIPAA and the Department's HIPAA Policies: Any member of the Department's workforce who is determined, following an investigation, to have violated a requirement of the HIPAA Privacy or Security Standards, or a requirement of this Policy or any other Department HIPAA policy or procedure, may be subject to any of the following corrective and disciplinary sanctions, depending on the severity and impact of the violation: (i) remedial training and education on the security, privacy and confidentiality of PHI, (ii) verbal warning, (iii) written warning, (iv) suspension, (v) demotion, (vi) other appropriate discipline, or (vii) termination of membership with the Department. The Department shall investigate and impose sanctions for violations, and document any such sanctions applied against a workforce member in accordance with Department personnel policies and procedures.

I. Mitigation of Effects of Violations: The HIPAA Privacy Officer, in coordination with the Fire Chief, shall be responsible for taking appropriate steps to mitigate, to the extent practicable, any harmful effect that is known to the Department resulting from a use or disclosure of PHI in violation of a requirement of the HIPAA Privacy or Security Standards, this Policy, or any other Department HIPAA policy or procedure, by the Department or a business associate of the Department.

J. Prohibited Acts of Intimidation or Retaliation: Neither the Department nor any member of its workforce shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for (i) exercising a right or participating in a process afforded to such individual under the HIPAA Privacy and Security Standards, (ii) filing a HIPAA complaint with the Secretary of the United States Department of Health and Human Services, (iii) testifying, assisting, or participating in a HIPAA-related investigation, compliance review, proceeding or hearing, or (iv) opposing any act or practice that the individual has a good faith belief is unlawful under the HIPAA Privacy or Security Standards.

K. Prohibited Waivers of Rights: Neither the Department, nor any member of its workforce, will require any individual to waive (i) the individual's right to file a HIPAA complaint with the Secretary of the United States Department of Health and Human Services, or (ii) any other right the individual has under the HIPAA Privacy Standards, as a condition of the Department's provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

L. HIPAA Policies and Procedures: The HIPAA Privacy Officer shall be responsible for:

   I. Developing and implementing the Department's HIPAA policies and procedures, subject to review and approval by the Fire Chief;

II. Periodically reviewing, updating and revising this Policy and any other Department HIPAA policies and procedures as necessary and appropriate to comply with changes in applicable law; and

III. Ensuring that any updates and revisions to the Department's HIPAA policies and procedures are promptly documented, implemented and, as necessary, reflected in the Department's Notice of Privacy Practices, and that affected Department personnel are appropriately informed about any such updates and revisions.

M. Documentation and Retention Requirements: The HIPAA Privacy Officer shall be responsible for ensuring that all Department HIPAA policies, procedures, forms, communications, actions, and activities required by the HIPAA Privacy and Security Standards are maintained in written or electronic form for a period of six (6) years from the date of creation or the date when they last were in effect, whichever is later.

2. HIPAA Notice of Privacy Practices Requirements:

A. The Department will maintain at all times a Notice of Privacy Practices (attached to this Policy as **Attachment A**) that complies with the requirements of 45 C.F.R. §164.520.

B. Department personnel providing treatment to a patient will provide a copy of its Notice of Privacy Practices:

I. To each Department patient (i) no later than the date of the first service delivery, or (ii) in an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation;

II. To any person upon request; and

III. To an individual by email if the individual agrees to electronic notice. However, the individual retains the right to obtain a paper copy of the Notice upon request.

C. Except in an emergency treatment situation, the Department personnel providing treatment to a patient will (i) make a good faith effort to obtain from each Department patient a written acknowledgement of receipt of the Notice of Privacy Practices, and (ii) if not obtained, document its good faith efforts to obtain such acknowledgement and the reason the acknowledgement was not obtained.

D. Whenever the Department's Notice of Privacy Practices is revised, the Department will make the Notice available upon request on or after the effective date of the revision.

E. The Department may make its Notice of Privacy Practices available on its website.

F. The Department will retain copies of all versions of its Notices of Privacy Practices, any written acknowledgements of receipt, and documentation of its good faith efforts to obtain such written acknowledgements, for a period of six (6) years.

3. Patients' HIPAA Rights: The Department will honor its patients' HIPAA rights as follows:

A. Right to Access and Obtain Copies of Protected Health Information:

I. Department patients have a right of access to inspect and obtain a copy of PHI maintained by the Department in the form of a designated record set unless an exception applies under Section 3(A)(V) of this Policy. Patients must make such requests in writing to the Department's Privacy Officer.

a. For purposes of this Policy, a patient's designated record set shall consist of:

(i) Patient care reports

(ii) Billing records; and

(iii) Any other records the Department maintains for a patient that the Department and its personnel use, in whole or in part, to make decisions about a patient.

b. A patient's designated record set shall <u>not</u> include:

(i) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and other documents and records that are subject to the attorney-client privilege, the attorney work product doctrine, or that are subject to any other privilege under federal or state law;

(ii) Peer review records;

(iii) Quality review and quality improvement records;

(iv) Health care provider credentialing records;

(v) Incident/accident reports and related records;

(vi) Internal grievance reports and related records;

(vii) Infection control reports and related records;

(viii) Information contained in Department employee personnel file records;

(ix) Information contained in Maine's state-wide, state-designated health information exchange in which the Department participates that has not been incorporated and integrated into the Department's designated record set for a patient;

(x) Financial, purchasing, and inventory control reports used by the Department for health care operations purposes;

(xi) Internal compliance reports and audits;

(xii) Administrative records;

(xiii) Any records excluded from a designated record set pursuant to 45 C.F.R. §164.524(a)(1)(i)-(iii)(A)-(B);

(xiv) Personal notes maintained by a Department health care practitioner that are not directly related to a patient's past or future treatment; and

(xv) Any other document or record that is not used by the Department and its health care providers to make health care decisions about a patient.

II. The Department will respond to requests for access within 30 days after receipt of the written request, unless the Department requires additional time in which case the Department may extend the time an additional 30 days upon notification of the requester of the reasons for the delay.

III. The Department will provide the patient with access to the PHI in the form and format requested, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format agreed to by the Department and the patient. If the request directs the Department to transmit the copy of the PHI directly to another person designated by the patient, the Department will provide the copy to the designated person in the manner requested.

IV. The Department may provide the patient with a summary of the PHI requested in lieu of providing access to the PHI, or may provide an explanation of the PHI to which the access has been provided, if the patient agrees in advance to such a summary or explanation and to the Department's fees for such summary or explanation.

V. The Department may deny a patient's access if:

a. The PHI was obtained by the Department from someone other than a health care provider under a promise of confidentiality and the requested access would be reasonably likely to reveal the source of the information;

b. A licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to endanger the life or physical safety of the patient or another person;

c. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to such other person; or

d. The requested access is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

VI. If the requested access if denied, the Department will provide the requestor with a written statement of the basis for the denial, a description of the requestor's review rights, a description of how the requestor may exercise such review rights, a description of how the requestor may file a complaint to the Department or to the Secretary of the United States Department of Health and Human Services, and the name (or title) and telephone number of the Department's Privacy Officer.

VII. If the Department denies requested access on any of the grounds described in Section 3(A)(V)(b)-(d), the patient or patient's authorized representative requesting the access has the right to have the denial reviewed within a reasonable period of time by a licensed health care professional designated by the Department to act as a reviewing official who did not participate in the original decision to deny. The Department will provide the requestor with written notification of the review decision.

VIII. The Department may impose a reasonable, cost-based fee for copies of PHI provided to a patient, provided such fees (i) only include the cost of labor for copying the PHI, supplies for creating the copy (including electronic media for electronic copies), postage (when the copy is requested by mail), and labor for preparing an agreed upon summary or explanation of the PHI, and (ii) do not exceed $5.00 for the first page, 45 cents for each additional page, and a maximum of $250.00 for the entire hardcopy, or $150.00 for the entire electronic copy.

B. Right to Amend, Correct and Clarify PHI and Treatment Records:

I. Department patients have the right to request amendments, corrections and clarifications to their PHI and treatment records maintained by the Department in a designated record set (as defined in this Policy). A patient who wishes to amend, correct or clarify PHI documented in the patient's treatment record shall submit to the Department's Privacy Officer a written request that includes the following information:

a. A statement of the information that the patient believes amends, corrects or clarifies the patient's treatment record;

b. A statement of the patient's reason for the requested amendment, correction or clarification;

c. A list of persons or entities to whom the patient wishes the Department to share the patient's amendment, correction or clarification; and

d. The patient's authorization for the Department to share the patient's amendment, correction or clarification with the persons identified by the patient.

II. Upon receipt of the patient's requested amendment, correction or clarification, the requested amendment, correction or clarification will be retained with the patient's treatment record by the Department and the Department's Privacy Officer will notify the patient within 60 days of receipt of the patient's request of the actions taken by the Department to honor the patient's request.

III. Department personnel who provided treatment to the patient that is the subject of the requested amendment, correction or clarification may add to the patient's treatment record a statement in response to the patient's requested amendment, correction or clarification.

IV. If Department personnel who provided treatment to the patient add a supplemental statement in response to the patient's requested amendment, correction or clarification, a copy of such provider's (providers') supplemental statement(s) shall be provided to the patient.

V. Upon receipt of a patient's written request, the Department will make reasonable efforts to inform and provide the patient's amendment, correction or clarification to:

a. Persons identified by the patient as having received protected health information about the patient and needing the amendment, correction or clarification; and

b. Persons, including business associates, that the Department knows has the PHI that is the subject of the amendment and who may have relied, or could foreseeably rely, on such information to the detriment of the patient.

VI. When the Department is required or authorized by law to disclose the patient's PHI or treatment records, any PHI or records required or authorized to be disclosed shall include copies of the patient's written amendments, corrections or clarifications and any supplemental statements added to the patient's treatment record by any Department personnel who provided treatment to the patient if:

a. The patient's amendments, corrections or clarifications relate to diagnosis, treatment or care;

b. The patient requests that the amendments, corrections or clarifications be included in the disclosure, and provides to the Department a signed authorization to that effect; and

c. The patient pays the Department all reasonable copying costs requested by the Department to provide the disclosed records.

C. Right to Request Restrictions on Disclosure of Protected Health Information:

I. Department patients have the right to request that the Department restrict (i) uses and disclosures of PHI to carry out treatment, payment or health care operations, and (ii) disclosures to persons involved in the patient's care and for notification purposes.

II. However, the Department is not required to a requested restriction, unless (ii) the requested restriction on disclosures is to a health plan for the purpose of carrying out payment or health care operations and is not otherwise required by law, and (ii) the PHI pertains solely to a health care item or service for which the patient, or person other than the health plan on behalf of the patient, has paid the Department in full.

III. If the Department agrees to honor a requested restriction, the Department will document the restriction and not use or disclose the patient's PHI in violation of the restriction unless the patient is in need of emergency treatment and the restricted PHI is needed by the Department or another health care provider to provide emergency treatment to the patient. In such circumstances the Department will request that the

health care provider receiving the patient's PHI in the emergency treatment situation not further use or disclose the information.

IV. If the Department agrees to a requested restriction, the Department will not be precluded from using or disclosing the patient's PHI when such use is otherwise permitted or required by (i) the Secretary of the United States Department of Health and Human Services to investigate or determine the Department's compliance with HIPAA, or (ii) any of the purposes set forth in 45 C.F.R. §164.512.

V. The Department or the patient may terminate a requested restriction at any time for any reason upon notice to the other party.

D. Right to Request Confidential Communications:

I. Department patients have the right to request to receive communications of PHI from the Department by alternative means or at alternative locations.

II. The Department will accommodate reasonable requests.

III. The Department may require that the request be made in writing.

IV. The Department may condition the provision of a reasonable accommodation on (i) when appropriate, information as to how payment, if any, will be handled, and (ii) specification of an alternative address or other method of contact.

V. The Department may not require an explanation from the patient as to the basis for the request as a condition of providing communications on a confidential basis.

E. Patient Right to Accounting of Disclosures of Protected Health Information:

I. Department patients have the right to request and obtain an accounting of certain disclosures of their PHI made by the Department.

II. The Department will maintain a log (an "Accounting Log") of all disclosures of a patient's PHI for which an accounting is required ("Accountable Disclosures," as further defined below) containing the information described in Sections 3(E)(4)(a)-(f) below, or documentation of a patient's Accountable Disclosures from which an Accounting Log can be created upon a patient's request for an accounting of such disclosures.

a. Definition of Accountable Disclosures: A disclosure of PHI is the release, transfer, provision of access to, or divulging in any other manner of PHI to any person or entity outside of the Department. An Accountable Disclosure is any disclosure of PHI outside of the Department, including disclosures made to or by Department business associates, except:

(i) Disclosures of PHI to carry out treatment, payment or health care operations, unless the disclosures were made through an electronic health record during the three years prior to the date of the requested accounting, in which case the disclosures are Accountable Disclosures;

(ii) Disclosures of PHI directly to the patient;

(iii) Disclosures of PHI incident to a permitted or required use or disclosure of PHI;

(iv) Disclosures of PHI pursuant to an authorization from the patient or the patient's authorized representative;

(v) Disclosures of PHI to persons involved in the patient's care or for other notification purposes;

(vi) Disclosures of PHI authorized by law to federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities;

(vii) Disclosures of PHI authorized by law to correctional institutions or law enforcement officials having lawful custody of an inmate or other individual;

(viii) Disclosures of PHI as part of a limited data set pursuant to a data use agreement; and

(ix) Disclosures of PHI that occurred more than six years prior to the date of a requested accounting.

b. Examples of Accountable Disclosures: The following disclosures are Accountable Disclosures under this Policy:

(i) Disclosures to carry out treatment, payment or health care operations made through an electronic health record during the three years prior to the date of the requested accounting;

(ii) Disclosures to a Department business associate for a purpose other than those listed in Sections 3(E)(2)(a)(i)-(ix) above;

(iii) Disclosures by a Department business associate for a purpose other than those listed in Sections 3(E)(2)(a)(i)-(ix) above;

(iv) Disclosures required by law not listed as an exception under Sections 3(E)(2)(a)(i)-(ix) above;

(v) Disclosures for public health activities, for example, to comply with communicable disease reporting laws, mandatory gunshot wound reporting laws, vital statistics reporting laws;

(vi) Disclosures about victims of abuse or neglect, for example, to comply with laws mandating the reporting of suspected child abuse and neglect, and suspected abuse, neglect or exploitation of incapacitated or dependent adults;

(vii) Disclosures for health oversight activities, for example, to professional licensing boards in connection with health care professional licensure or disciplinary actions, or to government regulators conducting facility licensing surveys or investigating complaints;

(viii) Disclosures for judicial and administrative proceedings, for example, to comply with a governmental subpoena in connection with a child protection proceeding, or to comply with a court order;

(ix) Disclosures to law enforcement for a purpose not listed in Sections 3(E)(2)(a)(i)-(ix) above, for example, to report a crime committed on Department premises or against a Department health care provider;

(x) Disclosures about decedents to coroners, medical examiners and funeral directors, or to organ procurement organizations for organ, eye or tissue donation purposes;

(xi) Disclosures for research purposes for which a patient's written authorization was not obtained;

(xii) Disclosures to avert serious threats to health or safety, for example, to law enforcement or to a potential victim of the threat;

(xiii) Disclosures for specialized government functions for a purpose other than those listed in Sections 3(E)(2)(a)(i)-(ix) above;

(xiv) Disclosures for workers' compensation purposes to comply with Maine's workers' compensation laws;

(xv) Unauthorized disclosures to persons or entities outside of the Department; and

(xvi) Disclosures to other persons or entities outside of the Department for which an exception does not apply under Sections 3(E)(2)(a)(i)-(ix) above.

III. Department patients may request an accounting of disclosures of PHI that have occurred within six years prior to the date of the request. Patients may be asked to make such a request in writing. Additionally, any person legally authorized to make health care decisions on behalf of a patient (such as a legal guardian, an agent under a durable health care power of attorney, a health care surrogate under the *Maine Uniform Health Care Decisions Act*, or the parent of a minor) is also authorized to request an accounting on behalf of the patient. A personal representative with the authority to act on behalf of a deceased patient or on behalf of a deceased patient's estate is also authorized to request an accounting on behalf of a deceased patient.

IV. Upon receiving a request for an accounting, the Department will provide the patient (or other authorized requestor) with a written accounting of disclosures containing the following information:

a. An itemized list of Accountable Disclosures of PHI that have occurred during the six years (or shorter period of time if specified by the patient) prior to the date of the request. This list will include Accountable Disclosures to or by business associates of the Department, or a list of all business associates of the Department

acting on behalf of the Department, including the mailing addresses, telephone numbers, and email addresses of all such business associates.

b. The date of each Accountable Disclosure.

c. The name of the entity or person who received the PHI for each Accountable Disclosure and, if known, the address of such entity or person.

d. A brief description of the PHI disclosed during each Accountable Disclosure.

e. A brief statement of the purpose of each disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of the written request for the disclosure.

f. If, during the period covered by the accounting, the Department has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required in Sections 3(E)(4)(b)-(e) above for the first disclosure made during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii)The date of the last such disclosure during the accounting period.

V. The Department will act on the patient's request for an accounting no later than 60 days after receipt of the request by either (i) providing the patient with the accounting requested, or (ii) extending the time to provide the accounting by no more than 30 days if the Department cannot provide the accounting within 60 days of the patient's request. In the event that the Department extends the time for providing the accounting, the Department will provide the patient with a written statement of the reasons for the delay and the date by which the Department will provide the accounting. This statement will be provided to the patient within 60 days of the patient's request for an accounting.

VI. The Department will provide the first accounting to a patient in any 12 month period without charge. However, the Department may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the 12 month period. The Department will inform a patient making a subsequent request during a given 12 month period that a fee may be charged for such subsequent requests, and provide the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

VII. The Department will document and maintain copies of all written accountings provided to patients.

VIII. The Department will temporarily suspend a patient's right to receive an accounting of disclosures of PHI upon request from a health oversight agency or a

law enforcement official for the time specified by such agency or official if (i) the health oversight agency or law enforcement official provides the Department with a written statement indicating that the provision of an accounting to the patient would be reasonably likely to impede the agency's or official's activities, and (ii) the statement specifies the time for which the suspension is required. If the agency or official statement is made orally, the Department will:

a. Document the statement, including the identity of the agency or official making the statement;

b. Temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and

c. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted by the agency or official during that time.

F. Right to Make Privacy Complaints: Department patients have the right to make complaints concerning the Department's HIPAA policies and procedures and the Department's compliance with such policies and procedures, in accordance with Section 1(G) of this Policy.

4. Uses and Disclosures of Department Patients' Protected Health Information:

A. A Department patient's PHI is confidential and may not be disclosed by the Department or its workforce members to any person or entity outside of the Department, other than to the patient, except as provided under this Section 4.

I. Any disclosure of PHI to a component of the Town of Harpswell government, including to another health care or HIPAA covered entity component of the TOWN, must meet an applicable exception to patient privacy under this Policy. If a member of the Department workforce also performs duties for the TOWN of Harpswell: Such workforce member is prohibited from using the Department's PHI in connection with the workforce member's duties to the TOWN, and from disclosing the Department's PHI to the TOWN, unless such use or disclosure is permitted under this Policy, HIPAA and applicable Maine law.

B. Minimum Necessary Rule and Related Requirements

I. Whenever using or disclosing a Department patient's PHI or when requesting a Department patient's PHI from another covered entity or business associate, the Department and its workforce members will make reasonable efforts to limit PHI to the minimum necessary reasonably required to accomplish the intended purpose of the use, disclosure or request. For all uses, disclosures, or requests to which the minimum necessary rule applies, the Department and its workforce members may not use, disclose or request an entire medical record, except when the entire medical

record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of that use, disclosure, or request.

II. The Department and its workforce members will identify:

    a. Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and

    b. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

        (i) The Department and its workforce members will make reasonable efforts to limit the access of such persons or classes identified above to PHI consistent with such persons' access needs and conditions of access.

III. For any type of disclosure that the Department and its workforce members make on a routine and recurring basis, the Department and its workforce members will implement standard protocols that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, the Department and its workforce members will:

    a. Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

    b. Review requests for disclosure on an individual basis in accordance with such criteria.

IV. The Department and its workforce members may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

    a. Making disclosures to public officials that are permitted under HIPAA (see 45 C.F.R. § 164.512), if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

    b. The information is requested by another HIPAA covered entity;

    c. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

    d. Documentation or representations that comply with the applicable requirements of 45 C.F.R. § 164.512(i) have been provided by a person requesting the information for research purposes.

V. The Department and its workforce members will limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. For a request that is made on a routine and recurring basis, the Department and its workforce

members will implement standard protocols that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made. For all other requests, the Department and its workforce members will:

a. Develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made; and

b. Review requests for disclosure on an individual basis in accordance with such criteria.

C. Permissible Uses and Disclosures of PHI with Patient's Authorization:

I. The Department and its workforce members may disclose a patient's PHI pursuant to a valid written authorization (*see* **Attachment B**) signed by the patient for the specific purpose stated in the authorization. The Department and its workforce members shall not disclose PHI in excess of the information described in the authorization. In the event that a Department workforce member is unclear as to the validity of an authorization signed by a patient or patient's authorized representative, the workforce member shall notify and consult with the Department's Privacy Officer to determine whether the Department can rely upon and honor the authorization.

II. A Department patient (or patient's authorized representative) may revoke an authorization at any time, provided the revocation is in writing, signed and dated. The Department and its workforce members will honor a written revocation, but such revocation shall be subject to the rights of any person who has already acted in reliance on the authorization prior to receiving notice of the revocation.

D. Permissible Uses and Disclosures of Patients' PHI upon Authorization from an Authorized Representative: In the event that a Department patient lacks the capacity or is otherwise unable to provide a written authorization to disclose the patient's PHI, the Department and its workforce members may disclose the patient's PHI pursuant to a written authorization signed by an authorized representative of the patient, unless the Department determines that the patient has been or may be subjected to domestic violence, abuse, neglect or exploitation by the patient's authorized representative, or treating such person as the authorized representative could otherwise endanger the safety of the patient, and/or that it is not in the best interest of the patient to recognize the authority of the authorized representative, taking into consideration the safety of the patient and any indicators, suspicion or substantiation of abuse. Department workforce members shall identify and verify an authorized representative's authority to act on behalf of the patient in accordance as follows:

I. Identification of Authorized Representative for the Purpose of Authorizing the Disclosure of Protected Health Information: The person authorized to obtain or disclose, or to exercise other rights a Department patient has with respect to, the

patient's PHI on behalf of the patient, will be identified by Department workforce members as follows:

a. The Patient: A competent adult patient with decisional capacity is authorized to make all decisions related to the patient's PHI.

b. Patient's Authorized Representative: In circumstances where the patient lacks decisional capacity, has been adjudicated to be legally incompetent, or is otherwise not legally authorized to access, disclose or exercise the patient's other rights with respect to the patient's PHI, the person authorized to make such decisions related to the patient's PHI on behalf of the patient will be identified in the following order of priority:

(i) The individual's agent under a health care power of attorney, unless the patient also has a court-appointed legal guardian whose health care decisions take precedence over the decisions of the patient's agent pursuant to the court's guardianship order;

(ii) The individual's legal guardian;

(iii) The patient's health care surrogate, in the following order of priority:

(1) The patient's spouse (including a same-sex spouse if the marriage was valid in the jurisdiction in which it was celebrated), unless legally separated;

(2) An adult who shares an emotional, physical and financial relationship with the patient similar to that of a spouse;

(3) An adult child of the patient;

(4) A parent of the patient;

(5) An adult brother or sister of the patient;

(6) An adult grandchild of the patient;

(7) An adult niece or nephew of the patient related by blood or adoption;

(8) An adult aunt or uncle of the patient related by blood or adoption;

(9) Another adult relative of the patient, related by blood or adoption, who is familiar with the patient's personal values; or

(10) An adult who has exhibited special concern for the patient and who is familiar with the individual's personal values.

(iv) If the patient is deceased: The personal representative, executor or administrator of the decedent's estate; if no personal representative, executor or administrator has been appointed, then (*in no order of priority, though consultation with legal counsel is advised*):

(1) The decedent's spouse (including a same-sex spouse if the marriage was valid in the jurisdiction in which it was celebrated);

(2) A parent of the decedent;

(3) An adult who is a child, grandchild or sibling of the decedent;

(4) An adult who is an aunt, uncle, niece or nephew of the decedent, related by blood or adoption;

(5) An adult related to the decedent, by blood or adoption, who is familiar with the decedent's personal values; or

(6) An adult who has exhibited special concern for the decedent and is familiar with the decedent's personal values.

II. Verification and Documentation of Identity and Authority of Authorized Representatives: Where an authorized representative acts on behalf of a patient under Section 4 of this Policy and the identity and authority of the patient's authorized representative are not known to the Department, the identity and authority of the person to act on behalf of the patient will be verified and documented by the Department as follows before allowing the person to assume the duties of an authorized representative:

a. In the case a patient with a health care power of attorney agent, the Department shall request a copy of the patient's health care power of attorney form from the patient or the patient's agent, and place it in the patient's medical record.

b. In the case of a patient with a court-appointed guardian, the Department shall request a copy of the court's guardianship order and place it in the patient's medical record.

c. In the case of an incapacitated patient without a health care power of attorney agent or a court-appointed guardian, the Department shall identify and document in the patient's medical record the patient's health care surrogate (as defined above). If the identity of the patient's health care surrogate is not known to the Department, the Department may require the individual acting as the patient's health care surrogate to complete and sign a Written Declaration of Health Care Surrogate form stating facts and circumstances reasonably sufficient to establish the surrogate's claimed authority.

d. In the case of a deceased patient, the personal representative of the decedent's estate or other person purportedly authorized to access or authorize the disclosure of the decedent's PHI will be required to either:

(i) Provide documentation of the person's status and authority to act as the decedent's personal representative, executor or administrator of the deceased patient's estate, such as a copy of the court order appointing the person to act as the personal representative of the decedent's estate, or a copy of the

patient's will designating the person to act as the administrator or executor of the decedent's estate, prior to disclosing the decedent's PHI to the patient's personal representative; and/or

(ii) Complete and sign the Verification of Authorized Representative's Status and Authority to Access and Authorize the Disclosure of Decedent's Health care Information form prior to disclosing the decedent's PHI to the patient's personal representative.

e. In cases where the identity of the person acting as the patient's authorized representative is not known to the Department, the Department will request documentation sufficient to reasonably verify the identity of the authorized representative, such as a driver's license or other similar identification, and shall maintain a copy of such documentation in the patient's medical record.

III. Verification and Documentation of Identity and Authority of Other Persons Purportedly Authorized to Obtain Patient's Protected Health Information: When a disclosure of PHI is requested by a person other than the patient's authorized representative who purports to have the authority to obtain such information (e.g., by a health oversight agency for health oversight activities, or to a law enforcement official for a law enforcement purpose), and such person is not known to the Department, the Department will obtain from the requesting person documentation, statements, or representations sufficient to reasonably verify the identity and authority of the person requesting the PHI, prior to disclosing such information. Such identification might include presentation of the requesting person's identification badge or credentials, submission of a written request on the requesting agency's official letterhead, written statement of the requesting person's purported legal authority to obtain the information, or other similar documentation.

E. Permissible Uses and Disclosures of Patients' PHI without Patient Authorization: The Department and its workforce members may use or disclose, or when required by law must use or disclose, a patient's PHI without the patient's or the patient's authorized representative's authorization under the following circumstances:

I. To workforce members within the Department for diagnosis, treatment or care of the patient, to provide health care services to the patient, or to coordinate or manage the care of the patient.

II. To health care providers and facilities outside the Department for diagnosis, treatment or care of the patient, to provide health care services to the patient, or to coordinate or manage the care of the patient; provided, however, that if the disclosure is to another health care practitioner or health care facility, or to a payor or a person engaged in payment for health care, for purposes of care management or coordination of care, the Department will make a reasonable effort to notify the patient or the patient's authorized representative of the disclosure.

III. To a business associate of the Department when such PHI is necessary for the business associate to perform services on behalf of the Department, provided such business associate has entered into a HIPAA-compliant written Business Associate Agreement with the Department.

IV. For the Department's own health care operations purposes, including, but not limited to quality assurance, utilization review, peer review, risk management, billing and collection, and similar activities relating to the delivery of health care.

V. For the health care operations purposes of a health care provider or facility receiving the PHI if:

a. Both the Department and the receiving entity either have or had a relationship with the patient who is the subject of the PHI being disclosed;

b. The PHI pertains to such relationship; and

c. The disclosure is for one of the following purposes:

(i) Health care fraud and abuse detection or compliance;

(ii) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

(iii) Reviewing the competence or qualifications of health care professionals; evaluating employee performance; evaluating services; conducting training programs in which students, trainees, and employees in areas of health care learn, under supervision, to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities.

VI. To third-party payors for payment and health care operations purposes, unless the patient has requested a restriction on disclosures to a health plan or third-party payor for a payment or health care operations purpose and the PHI pertains to services for which the patient has paid the Department in full.

VII. In the event of a patient's incapacity, to the patient's health care power-of-attorney agent or court-appointed guardian (unless such disclosure is otherwise limited by the patient's health care power of attorney document or the court's guardianship order), or to the patient's health care surrogate.

VIII. To persons involved in the patient's care and for notification purposes when such information is directly relevant to their involvement in the patient's care or to their

arrangement of payment for the patient's care, unless the patient has objected to such disclosures after being afforded an opportunity to object.

IX. To appropriate persons upon a determination by the Department and the patient's Department provider that (i) in their good faith, reasonable professional judgment the patient poses a direct threat of serious imminent harm to the health or safety of another person or the public, (ii) the disclosure is necessary to prevent, avert or lessen the threat, (iii) the disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat or law enforcement, (iv) the disclosure otherwise protects the confidentiality of the patient's PHI consistent with sound professional judgment, and (v) the disclosure is consistent with standards of ethical conduct applicable to the Department and the patient's Department health care provider.

X. To state and federal governmental entities in order to protect the public health and welfare when reporting is required or authorized by law, including but not limited to mandatory reports of suspected abuse, neglect or exploitation of children and incapacitated and dependent adults under Maine law.

XI. To federal, state or local governmental entities to report a suspected crime against the Department or against a Department health care practitioner, or to report information that the Department or a Department health care practitioner believes in good faith constitutes evidence of criminal conduct that occurred on the Department's premises.

XII. To federal, state or local governmental entities if the Department is providing diagnosis, treatment or care to a patient and has determined in the exercise of sound professional judgment that the following requirements, as applicable, are satisfied:

a. With regard to a disclosure for public health activities, the provisions of 45 C.F.R. §164.512(b) have been met. *Consultation with legal counsel should be considered.*

b. With regard to a disclosure for law enforcement purposes, the provisions of 45 C.F.R. §164.512(f) have been met, including disclosure to law enforcement officers investigating criminal conduct. *Consultation with legal counsel should be considered.*

c. With regard to a disclosure that pertains to victims of abuse, neglect or domestic violence, the provisions of 45 C.F.R. §164.512(c) have been met. *Consultation with legal counsel should be considered.* Additionally, with regard to a disclosure that pertains to a victim of domestic violence or a victim of sexual assault, (i) the Department, in the exercise of professional judgment, must believe that the disclosure is necessary to prevent serious harm to the patient or other potential victims, or (ii) if the patient is unable to agree to the disclosure because of incapacity, a law enforcement or other public official authorized to receive the report must represent that the PHI for which disclosure is sought is not intended

to be used against the patient (or other potential victims) and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

XIII. As directed by an order of a court having jurisdiction over the Department or its workforce members. *Consultation with legal counsel is advised to determine the validity of the court order and whether and how the Department is authorized to disclose PHI pursuant to the court order*.

XIV. To a governmental entity pursuant to a lawful subpoena requesting PHI to which the governmental entity is entitled according to statute or rules of court. *Consultation with legal counsel is advised to determine whether and how the Department is authorized to respond to a subpoena, and whether the Department should seek to quash the subpoena or an appropriate protective order.*

XV. To health oversight agencies engaged in the assessment, evaluation or investigation of the provision of, payment to, or the practices of, the Department pursuant to statutory or professional standards or requirements.

XVI. To health oversight entities engaged in the regulation, accreditation, licensure or certification of the Department or its health care providers.

XVII. To attorneys of the Department as determined by the Department to be required for the Department's own legal representation.

XVIII. In the event of a patient's death:

a. To the personal representative or administrator of the deceased patient's estate or, if no such personal representative or administrator has been appointed, to another authorized representative of the patient;

b. To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties of the recipient as authorized by law;

c. To a funeral director, consistent with Maine law, as necessary to carry out the funeral director's duties with respect to the decedent (PHI may also be disclosed to a funeral director prior to, and in reasonable anticipation of, the patient's death, if necessary for the funeral director to carry out his or her duties); or

d. To a family member or other persons who were involved in the patient's care or payment for health care prior to the patient's death if such information is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed wishes of the patient that are known to the Department.

XIX. When such disclosure is otherwise required or authorized by law. *Consultation with legal counsel should be sought in uncertain circumstances.*

F. Disclosures of Substance Use Disorder Program PHI: To the extent that the Department obtains or maintains Substance Use Disorder Program PHI concerning a patient that is identified as a substance use disorder program patient and that is subject to the confidentiality protections of 42 C.F.R. Part 2, the Department shall maintain the confidentiality of such information and shall not disclose such information except that:

I. The Department may disclose substance use disorder program information to medical personnel outside of the Department to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained, provided that immediately following the disclosure the disclosure is documented by the Department, including the name of the medical personnel to whom the disclosure was made and their affiliation with any health care facility, the name of the Department workforce member making the disclosure, the date and time of the disclosure, and the nature of the emergency; or

II. The Department may disclose substance use disorder program PHI pursuant to a written authorization that specifically authorizes the disclosure of such information.

III. The Department may disclose substance use disorder program PHI as otherwise authorized or required by another exception under 42 C.F.R. Part 2.

G. Disclosures of HIV Information: The Department and its workforce members shall not disclose any information regarding a patient's HIV test results or HIV status unless the patient has specifically authorized the disclosure of HIV information in a written authorization, except to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained. *Legal counsel should be consulted in uncertain circumstances*. Patients authorizing the disclosure of Department records containing HIV infection status information shall be informed of the potential implications of authorizing the disclosure of HIV information prior to the disclosure, and such risks shall be disclosed and documented either in the patient's medical record or on the patient's authorization form. In the event that a Department health care provider has a good faith, reasonable basis to believe that a patient's behavior intentionally or negligently places a third party at serious health risk of exposure to HIV/AIDS, the Department is authorized to report the provider's concerns about the risk of exposure of a communicable disease the patient poses to a third party to the Maine Bureau of Public Health. The Bureau of Public Health is authorized to take any appropriate preventive action deemed necessary to protect the health and safety of third parties at risk, including notification of such third parties of their risk of exposure. The Department health care provider is authorized to cooperate with the Bureau of Public Health in the course of the Bureau's taking preventive action in the case.

H. Verification of Permissible Uses and Disclosures: Department workforce members who use or disclose a patient's PHI under this Policy shall either know or verify that a signed authorization form authorizing the use or disclosure is documented in the patient's medical record or that another exception to confidentiality applies under this Policy, prior

to making such use or disclosure of PHI. In circumstances where a Department workforce member is unsure as to whether a use or disclosure is permissible under this Policy and applicable law, the Department workforce member shall confer with the Department's Privacy Officer for guidance.

I. Disclosure of Partial or Incomplete Information: If the Department discloses partial or incomplete PHI of a patient as compared to the request or directive to disclose under applicable law, the Department will indicate in writing to the recipient of the information that the information is partial or incomplete.

J. Requests for Certified Copies of Medical Records: In responding to requests for certified copies of a patient's Department records, the custodian of medical records at the Department shall certify the authenticity of the records by completing a "Certification of Authenticity of Medical Records" form and ensuring that any records sent in response to the request are accompanied by a completed Certification form.

K. Uses and Disclosures of De-Identified Information: The Department may use PHI to create De-Identified PHI for a use or disclosure other than for research purposes, without patient authorization. De-Identified PHI is not subject to the confidentiality requirements of this Policy.

5. Security Incidents and Breach Notification: The Department will (i) identify, report, investigate, mitigate and document all discovered or reported Security Incidents (as defined herein) in accordance with the requirements set forth below in Section 5, and (ii) following the discovery of a Breach of Unsecured PHI (as defined herein), notify each individual whose Unsecured PHI has been, or is reasonably believed by the Department to have been, accessed, acquired, used, or disclosed as a result of such Breach, in the manner set forth in Section 5 below.

A. For purposes of this Policy, the following terms shall have the following meaning:

I. Breach: The acquisition, access, use, or disclosure of protected health information ("PHI") in a manner not permitted under the HIPAA Privacy Standards which compromises the security or privacy of the PHI.

II. Secured Protected Health Information: PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology that encrypts, clears, purges, or destroys the PHI in accordance with HIPAA.

III. Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in a Department information system.

IV. Unsecured Protected Health Information: PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a

technology or methodology that encrypts, clears, purges, or destroys the PHI in accordance with HIPAA.

B. Any member of the Department workforce who discovers or becomes aware of a Security Incident, or who suspects that a Breach may have occurred, shall immediately report the Security Incident or suspected Breach to the Department Privacy Officer or Security Officer.

C. Upon discovering or being informed of a Security Incident or a suspected Breach, the Department Privacy Officer, or his or her designee, in consultation with the Department's Security Officer (if the suspected Breach involved ePHI) shall promptly conduct an investigation and risk assessment to determine (i) whether any information maintained in a Department information system has been or has attempted to be accessed, used, disclosed, modified or destroyed in an unauthorized manner, (ii) whether a Breach of PHI has occurred, and (iii) whether any system operations within a Department information system have been interfered with in an unauthorized manner. The Department Privacy Officer, in consultation with the Department Security Officer (if ePHI is involved), shall evaluate whether the incident compromises the security or privacy of any individual's PHI, as follows:

   I. The risk assessment shall be fact-specific and take into account at least the following factors:

      a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

      b. The unauthorized person who used the PHI or to whom the disclosure was made;

      c. Whether the PHI was actually acquired or viewed; and

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

   II. The Department Privacy Officer shall presume that an acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Standards is a Breach, unless the Privacy Officer concludes, based on the Risk Assessment above, that the Department can demonstrate that there is a low probability that the PHI has been compromised.

   III. The Department Privacy Officer shall be responsible for ensuring that Security Incidents, Risk Assessments related to suspected Breaches, and outcomes related to such Security Incidents and Breaches, are investigated and appropriately documented.

D. There is no Breach, and the Department has no breach notification obligations under this Policy, if, as a result of the Privacy Officer's investigation and Risk Assessment, the Department determines that the incident involved:

   I. An unintentional acquisition, access, or use of PHI by a Department workforce member or person acting under the authority of the Department or a business associate of the Department, and such acquisition, access, or use was made in good

faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Standards;

II. An inadvertent disclosure by a person who is authorized to access PHI at the Department or a business associate of the Department to another person authorized to access PHI at the Department or the Department business associate, or organized health care arrangement in which the Department participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Standards;

III. A disclosure of PHI where the Department (or a business associate of the Department) has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information;

IV. Secured (encrypted) PHI (*unencrypted PHI breached that is protected by means of firewalls and/or access controls is subject to breach notification*); or

V. An acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Standards that, following a risk assessment undertaken by the Department of the factors described in Sections 5(C)(1)(a)-(d) above, the Department can demonstrate poses a low probability that the PHI has been compromised.

E. Breach Notification: In the event that the Department concludes that a Breach has occurred:

I. The Department shall provide the notification required by this Policy without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach. For purposes of this Policy, a Breach shall be treated as discovered as of the first day on which the Breach is known or, by exercising reasonable diligence would have been known to any person, other than the person committing the Breach, who is a workforce member or agent of the Department.

II. The notification required by this Policy shall include, to the extent possible, the following information:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

b. A description of the types of Unsecured PHI that were involved in the Breach;

c. Any steps individuals affected by the Breach should take to protect themselves from potential harm resulting from the Breach;

d. A brief description of what the Department is doing or has done to investigate the Breach, to mitigate harm to individuals affected by the Breach, and to protect against any further Breaches; and

e. Contact procedures for individuals to ask questions or to obtain additional information, which shall include a toll free telephone number, an e-mail address, Web site, or postal address.

III. Methods of Individual Notification: The notification required by this Section 5 shall be provided in the following form to each affected patient or, if a patient lacks decisional capacity, to the patient's authorized representative:

a. Written Notice:

(i) Written notification by first-class mail will be provided to the individual at the last known address of the individual. The notification may be provided in one or more mailings as information becomes available.

(ii) If the Department knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail will be provided to either the next of kin or personal representative of the individual.

b. Substitute Notice: In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, the Department shall provide a substitute form of notice reasonably calculated to reach the individual. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

(i) In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for ten (10) or more individuals, then such substitute notice shall:

(1) Be in the form of either a conspicuous posting for a period of ninety (90) days on the Department's website home page or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside; and

(2) Include a toll-free phone number that shall remain active for at least ninety (90) days where an individual can learn whether the individual's Unsecured PHI may be included in the Breach.

c. Additional notice in urgent situations may be required in any case deemed by the Department Privacy Officer to require urgency because of possible imminent misuse of Unsecured PHI. Such notice may be provided to individuals by telephone or other means, as appropriate, in addition to the written notice required by this Policy.

IV. For a Breach of Unsecured PHI involving more than five hundred (500) patients, the Department shall, following the discovery of the Breach, notify prominent media outlets serving the State of Maine. The Department shall provide this notification without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the Breach, unless such notification is delayed pursuant to a law enforcement request under Section 5 below. The notification provided under this Section 4(D) shall include the same information described in Sections 5(E)(2)(a)-(e).

V. The Department shall, following the discovery of a Breach of Unsecured PHI, notify the Secretary of the United States Department of Health and Human Services ("DHHS") as follows:

a. For Breaches of Unsecured PHI involving five hundred (500) or more individuals, the Department shall provide the notification required by Section 5(E)(3) contemporaneously with the notice to the Secretary of DHHS, in the manner specified on the DHHS Website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

b. For Breaches of Unsecured PHI involving less than five hundred (500) individuals, the Department shall maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide the notification to the Secretary of DHHS for Breaches discovered during the preceding calendar year, in the manner specified on the DHHS Website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

F. The Department shall require its respective business associate contractors to enter into a written business associate agreement with the Department that includes a provision requiring the business associate to report to the Department any Security Incident of which the business associate becomes aware, including Breaches of Unsecured PHI as required by 45 C.F.R. §164.410.

I. If a law enforcement official represents to the Department that a notification, notice, or posting required under Section 5 of this Policy would impede a criminal investigation or cause damage to national security:

II. If the statement is in writing and specifies the time for which a delay is required, the Department shall delay such notification, notice, or posting for the time period specified by the official; or

III. If the statement is made orally, the Department shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted by law enforcement to the Department during that time.

G. The Department Privacy Officer and, if the Breach involved ePHI, the Department Security Officer, shall be responsible for ensuring that timely measures are taken to mitigate, to the extent practicable, the harmful effects of any identified Security Incidents or suspected Breaches. If steps taken to mitigate the harm stemming from a Security Incident are determined by the Privacy Officer to demonstrate that the probability that the PHI has been compromised is either low or has been eliminated, the Department may conclude that the security and privacy of the PHI has not been compromised and that no Breach has occurred as a result of the Security Incident. Such mitigating measures might include:

   I. Identifying the source of the Security Incident or Breach and, if the source is a member of the Department workforce, taking appropriate corrective or other action against the source. If the source is a business associate contractor of the Department, determining whether termination of the business associate relationship, or other appropriate action, is warranted under the circumstances.

   II. Contacting the recipient of the information that was the subject of a Breach, requesting that the recipient make no further disclosures of the information, requesting that the recipient either return or destroy the information, and obtaining the recipient's satisfactory assurances that the information has not been and will not be further used or disclosed (through a confidentiality agreement or similar means), and has been or will be destroyed.

   III. Notifying affected patients whose PHI may have been placed at risk as a result of the Security Incident or Breach.

   IV. Reviewing Department policies and procedures to determine whether changes are necessary to prevent or reduce the risk of a recurrence of the Security Incident or Breach.

H. The Department shall be responsible for ensuring that any incident involving a suspected or actual Breach under this Policy that constitutes an Accountable Disclosure under this Policy, is properly documented on affected patients' Accounting Logs in accordance with this Policy.

I. Notifications Required by Other Laws:

   I. Personal Data Breach Notification: The Department Privacy Officer shall be responsible for determining whether any suspected or actual Breach under this Policy also involved a use or disclosure of "personal information" that triggers a breach notification obligation under Maine's Notice of Risk to Personal Data Act.

   II. Notification Required by Other State Laws: In the event that a suspected or actual Breach involved a breach of information concerning a patient of another state, the Department Privacy Officer shall confer with legal counsel to determine whether the Department has any breach notification obligations under the laws of the state of any such non-Maine patient.

J. In the event that the Department Privacy Officer determines, after conducting an appropriate investigation and Risk Assessment of a suspected Breach, that the Department has no breach notification obligations under this Policy, the Privacy Officer, in consultation with the Department Chief and/or the Department's legal counsel, may elect, in their discretion, to notify affected patients of the incident even though the Department may be under no legal obligation to provide such notification.

K. Only the Department Privacy Officer and Department Chief, or a designee thereof, shall be authorized to provide the notifications required by this Policy.

L. Any member of the Department workforce who is determined, following an investigation, to have intentionally or knowingly caused a Security Incident or breached the security or privacy of a Department patient's PHI or personal information, may be subject to corrective and disciplinary actions, up to and including termination of membership or contractual or other relationship with the Department, depending on the facts and circumstances, severity and impact of the Security Incident or Breach.

M. Any unauthorized member of the Department's workforce acquiring any Department patient's PHI or personal information through a Breach or as a result of a Security Incident is strictly prohibited from using or redisclosing such information to any unauthorized person.

6. HIPAA Security Safeguards to Protect Electronic Health Care Information: PHI and electronic PHI ("ePHI") maintained by the Department in any Department information system, or in any Department information system maintained by a business associate of the Department, shall be maintained, stored and transmitted in a secure manner in accordance with the Department's "HIPAA Security Policy."

7. Business Associates: The Department will ensure that Department patient's PHI is not disclosed to a Department contractor that provides services to or on behalf of the Department other than in a capacity of a member of the Department's, unless (i) the services involve the use or disclosure of PHI, and (ii) such contractor has entered into a Business Associate Agreement with the Department that meets the applicable business associate requirements of the HIPAA Privacy and Security Standards set forth at 45 C.F.R. §164.314(a) and §164.504(e). For purposes of this Section 7, a "business associate" means a person or entity that:

   A. On behalf of the Department, but other than in the capacity of a member of the Department's workforce, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, and repricing; or

   B. Provides, other than in the capacity of a member of the Department's workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative,

accreditation, or financial services to or for the Department, where the provision of the service involves the disclosure of PHI from the Department or from another business associate of the Department, to the person or entity.

A person or entity is not a business associate of the Department if he/she/it is:

(i) An employee of the Department;

(ii) A health care provider to which the Department discloses PHI in connection with the treatment of a Department patient; or

(iii) A vendor that places its employees on the Department's premises to the extent that the vendor's employees perform a substantial proportion of their activities at such location and the Department treats such vendor's employees as members of the Department's workforce for the purpose of complying with the Privacy Rule and the Department's HIPAA policies and procedures.

This policy applies to the following organizations:

Cundy's Harbor Volunteer Fire Department
837 Cundy's Harbor Rd
PO Box 948
Harpswell, ME 04079

Orr's & Bailey Islands Fire Department
1600 Harpswell Islands Rd
PO Box 177
Harpswell, ME 04066

Reviewed and Approved By:

_____ Fire Chief

08 October 8, 2021
Date