CANTON CITY PUBLIC HEALTH

HIPAA Privacy and Security Policies

HITECH ACT, Omnibus Rule Compliant, Version 4.0

Updated April 2022

Policies governing confidentiality of the information regarding the patients we serve, their privacy rights, and our computer security.

Table of Contents

This document was created using Microsoft Word. When updating, note the following conventions:

1) Policy titles and headings are created using styles Heading 1, Heading 2 and Heading 3
2) The Table of Contents is a field and can be updated based on revised policy titles and headings by pressing the F9 key.
3) Bookmarks are used in front of Policy titles and are used for hyperlinks.
4) Microsoft Word can create an HTML version of this document for use on your internal system to facilitate ready access by your employees.

CONFIDENTIALITY & PRIVACY POLICIES
POLICIES FOR ALL STAFF

1000 Confidentiality, Privacy and Computer Security Definitions

POLICY
The following definitions shall apply to all Confidentiality, Privacy, and Computer Security Policies, numbered 1000 through 4000.

AUDIENCE
All Staff

AUTHORITY
The definitions below are adapted from the federal HIPAA regulations. The HIPAA Privacy regulations are at 45 CFR Part 160 and 45 CFR Part 164 Subpart E. The HIPAA Security regulations are at 45 CFR Part 160 and 45 CFR Part 164 Subparts C and D. Subpart D is the Breach Notification rule created by the HITECH Act. See:
45 CFR 164.103 Definitions
45 CFR 164.304 Definitions
45 CFR 164.402 Definitions
45 CFR 164.501 Definitions

DEFINITIONS
1) **Access –** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
2) **Administrative safeguards –** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
3) **Applicable Requirements –** Applicable requirements mean applicable federal law and the contracts between the department and other persons or entities which conform to federal law.
4) **Authentication –** means the corroboration that a person is the one claimed.
5) **Availability –** means the property that data or information is accessible and useable upon demand by an authorized person.
6) **Breach –** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information. Breach *excludes*:
   A) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if 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 by the HIPAA privacy rules.
   B) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.
   C) A disclosure of protected health information where a covered entity or business associate 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.

   Except for the two exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:

A) The nature and extent of the protected health information 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.

7) Business Associate (BA) – A Business Associate, basically, is a person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. The complete definition and other information is included in Appendix A - Identifying Business Associates**.**

8) **Confidentiality –** means the property that data or information is not made available or disclosed to unauthorized persons or processes.

9) **Covered Entity –** means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA privacy rules.

10) **Destruction –** means physical destruction of a record or removal of personal identifiers from information so that the information is no longer personally identifiable.

11) **Designated Record Set –** Designated record set means:
A group of records maintained by or for a covered entity that is:
A) The medical records and billing records about patients maintained by or for a covered health care provider;
B) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
C) Used, in whole or in part, by or for the covered entity to make decisions about patients.
For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

12) **Disclosure –** means the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the entity holding the information.

13) **Employee –** means any person employed by the department, volunteers, interns, board members and other persons whose conduct, in the performance of work for the department, is under the direct control of the department, whether or not they are paid by the department.

14) **Encryption –** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

15) **Facility –** means the physical premises and the interior and exterior of a building(s).

16) **Family Member –** means, with respect to an individual:
A) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
B) Any other person who is a first-degree, second-degree, third-degree, or fourth- degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
C) First-degree relatives include parents, spouses, siblings, and children.
D) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
E) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
F) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

17) **Genetic Information –** means:
A) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
i) The individual's genetic tests;
ii) The genetic tests of family members of the individual;
iii) The manifestation of a disease or disorder in family members of such individual; or
iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
B) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:
i) A fetus carried by the individual or family member who is a pregnant woman; and
ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive

technology.

C) Genetic information excludes information about the sex or age of any individual.

18) **Genetic Services –** means:
   A) A genetic test;
   B) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
   C) Genetic education.

19) **Health Care Clearinghouse –** A Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system or community health information system that does either of the following functions:
   A) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
   B) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

20) **Health Care Operations –** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
   A) 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; patient safety activities (as defined in 42 CFR 3.20); 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;
   B) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners 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;
   C) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;
   D) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
   E) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
   F) Business management and general administrative activities of the entity, including, but not limited to:
      i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
      ii) Resolution of internal grievances;
      iii) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
      iv) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity,

21) **Health Oversight Agency –** 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 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.

22) **Health Plan –** Health plan means an individual or group plan that provides, or pays the cost of medical care. A partial list of entities that are health plans includes the following, singly or in combination:
   A) A group health plan, health insurance issuer or HMO
   B) Part A or Part B of the Medicare Program
   C) The Medicaid program under title XIX of the Act, 42 U.S.C. § 1396, et seq.

D) The Medicare Part D Prescription Drug Benefit Program
E) An issuer of a Medicare Supplemental Policy
F) The health program for uniformed services
G) The veterans health care program
H) The Indian Health Service
I) The Federal Employees Health Benefits Program
J) Any other individual or group plan that provides or pays for the cost of medical care

23) **HIPAA –** HIPAA means the Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 - 1320d-8.
24) **Incidental Disclosure** – An unintentional disclosure of PHI, that occurs as a result of a use or disclosure otherwise permitted by the HIPAA Privacy rule. An Incidental Disclosure is NOT a violation of the Privacy rule. However, in order for incidental disclosures to not be a violation, the covered entity must be in compliance with the requirement for implementation of the minimum necessary principle, and also in compliance with the requirement to implement physical, technical, and administrative safeguards to limit incidental disclosures.
25) **Individually identifiable health information –** means the subset of health information, including demographic information collected from an individual, and
    A) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
    B) 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
        i. That identifies the individual; or
        ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
26) **Information system –** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
27) **Integrity –** means the property that data or information have not been altered or destroyed in an unauthorized manner.
28) **Malicious software –** means software, for example, a virus, designed to damage or disrupt a system.
29) **Manifestation or manifested –** means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information
30) **Marketing** - means
    A) Except as provided in paragraph (B) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
    B) Marketing does not include a communication made:
        i. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.
        ii. For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:
            1. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
            2. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
            3. For case management or care coordination, contacting of individuals with information about

treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

31) **Parent –** Parent means either parent. If the parents are separated or divorced, "parent" means the parent with legal custody of the child. "Parent" also includes a child's guardian, custodian, or parent surrogate. At age eighteen, the participant must act in his or her own behalf, unless he/she has a court-appointed guardian
32) **Password –** means confidential authentication information composed of a string of characters.
33) **Patient –** Means a person who receives services from the department. In the event that the patient is a minor, the term "patient" in these policies may also include the parent or guardian of the patient. In addition, in regard to any privacy rights, patient may also mean an individual's "personal representative" as it is defined under HIPAA regulations.
34) **Personal Representative –** means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco parentis has assented to an agreement of confidentiality between the department and the minor.
35) **PHI** – PHI, short for "Protected Health Information" means individually identifiable information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. PHI does not include (i) information in employment records held by a covered entity in its role as an employer or (ii) Records of individuals deceased for more than 50 years. CCPH is a hybrid entity and certain PHI is protected by HIPAA and State law, and other PHI is protected only by State law. These policies apply in both cases.
36) **Physical safeguards –** are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
37) **Protected Health Information –** See **PHI** above.
38) **Provider –** means a person or entity which is licensed or certified to provide services, including but not limited to health care services. This includes physicians, hospitals, home health agencies, ambulance companies, physical therapists, nurses, and any other licensed patient or entity who provides "health care". A Covered Provider is a Health Care Provider who transmits any health information in electronic form.
39) **Public Health Authority – means** an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
40) **Security or Security measures –** encompass all of the administrative, physical, and technical safeguards in an information system.
41) **Security incident –** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
42) **Social Engineering – "**an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). . . .. Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
43) **Subcontractor –** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
44) **Technical safeguards –** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
45) **TPO –** TPO means treatment, payment or health care operations under HIPAA rules.
46) **Treatment –** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual; or the referral of an individual for health care from one health care provider to another.
47) **Unsecured protected health information –** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized patients through the use of a technology or methodology in

guidance specified by the Secretary of the Department of HHS in guidance published on the HHS Web site.

48) **Use –** means, with respect to patiently identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
49) **User –** means a person or entity with authorized access.
50) **Violation**. There are different types of violations, with different contexts:
    A) **Privacy Violation.** Allowed uses and disclosures of PHI are described in considerable detail in policies and procedures in this manual. For the purposes of this policy, a "privacy violation" is any use or disclosure which is not explicitly allowed in these policies.

    B) **Employee Security Procedure Violation**. The failure of an employee to comply with one or more of the policies and procedures described in the HIPAA Security Policies section of the policies and procedures manual.

51) **Workforce Member –** means the same as employee. See definition above.
52) **Workstation –** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

1010 HIPAA – General Rules

POLICY

All employees are required to maintain the confidentiality of patients. This confidentiality encompasses information about patients whether it is spoken, written or in computer systems.

The department shall conform to all requirements for privacy and confidentiality set forth federal HIPAA regulations, and any other applicable law. The employees of the department shall not use or disclose PHI except in accordance with these policies.

Further, all employees will learn and follow all policies regarding the computer equipment at CANTON CITY PUBLIC HEALTH as well as any computer equipment they own, if they are authorized to use it for business purposes.

The Health Commissioner and/or supervisors will follow additional policies that detail administrative duties relating to the HIPAA requirements.

AUDIENCE

All Staff

AUTHORITY

45 CFR Part 160 and 164
45 CFR 164.504(g) for entities with multiple functions
45 CFR 164.502(a)(1)(iii) incidental uses and disclosures

PROCEDURES

1) Staff of the department may use or disclose PHI only as follows:
   A) For treatment, payment or health care operations. An employee may only use or disclose PHI for a patient when they are involved in the treatment of the patient, obtaining payment for services for the patient, or with administrative functions included in "health care operations".
   B) In accordance with an authorization to release information of the patient in accordance with policy and procedure set forth in Policy 1050 Authorizations.
   C) As permitted in Policy 1040 Speaking with the Family or Friends of a Patient Receiving Services.
   D) As permitted by in Policy 1090 Disclosures that do Not Require an Authorization.
2) For all of the above, the minimum amount of information should be disclosed, and specific procedures followed as detailed in Policy 1020 Minimum Necessary Policy.
3) All employees are responsible for safeguarding the information regarding patients we serve, as detailed in
   A) Policy 1030 Confidentiality Safeguards (Oral & Written)
   B) Policy 3080 Computer Usage
   C) Policy 3082 Use of Social Media
   D) Policy 3085 Portable Computing Devices and Home Computer Use
4) Rights of patients served by CANTON CITY PUBLIC HEALTH may be exercised by parents, guardians and personal representatives as detailed in Policy1070 Minors, Personal Representatives and Deceased Patients.
5) Confidentiality and Computer Security are everyone's responsibility – all staff must understand and follow procedures detailed in Policy 1080 Duty to Report Violations and Security Incidents.
6) Supervisors, managers and certain staff have specific duties, rights, and obligations as specified elsewhere in these policies.
7) CANTON CITY PUBLIC HEALTH policy is not to use PHI for marketing purposes or to sell PHI to 3rd parties.

1015 Clinical Data Collection

POLICY
Clinical documentation shall be limited to information needed for patient care, shall be gathered in a confidential manner, and shall be gathered according to accepted medical/legal standards.

AUDIENCE
All Staff

PROCEDURES
1) The types and amount of PHI gathered and recorded should be limited to that information needed for patient care. Supplementary data for research, education, or epidemiology purposes may be recorded with the permission of the patient following an explanation of the purpose for which the information is requested.
2) All individuals engaged in the collection, handling or dissemination of PHI shall be specifically informed of their responsibility to protect patient data and of the penalty for violation of that trust. Details are further specified in Policy 1350 Policy Updating and Staff Training.
3) The collection of any data relative to a patient, whether by interview, observation, or review of documents shall be conducted in a setting which provides maximum privacy and protects the information from unauthorized individuals to the greatest extent possible.
4) All entries in the health record are dated and signed by the health care professional who makes the entry.

1020 Minimum Necessary Policy

POLICY

For purposes other than those listed below, the use and disclosure of PHI must be limited to the minimum necessary to satisfy the request or to complete the task. This minimum necessary provision shall **NOT APPLY** to the following outlined uses and disclosures of PHI:

- For treatment purposes;
- For information requested by the patient (or the patient's personal representative);
- For information requested pursuant to a valid authorization by the patient;
- For compliance with standardized Health Insurance Portability and Accountability Act (HIPAA) transactions; or
- Disclosures required by law or shall be made in accordance with the authority seeking the information.

AUDIENCE

All Staff

AUTHORITY

45 CFR 164.502(b)(1) minimum necessary standard

PROCEDURES

FOR ALL STAFF

1) **General Principles**. For all uses and disclosures of PHI, staff must limit the information used or disclosed to the minimum amount necessary for the purpose. Minimum necessary DOES NOT APPLY to uses and disclosures for treatment, disclosures to the patient or his/her personal representative, for information disclosed pursuant to an authorization, for compliance with standard transactions under HIPAA, or for disclosures required by law.
2) **Limit Uses, Disclosures and Requests of Entire Medical Records** – All personnel should take care to avoid using, disclosing, and requesting the entire record of patients we serve unless this is absolutely necessary.
3) **Procedures for Routine Disclosures and Requests.** Protocols for routine disclosures, and for routine requests for PHI, will be developed by the Privacy Officer. These protocols will be developed for conformance with the minimum necessary principle, and are detailed in Appendix F – Minimum Necessary – Procedures for Routine Disclosures and Requests. The Privacy officer will update these protocols as necessary.
4) **Non-Routine Disclosures or Requests**
   A) For non-routine disclosures, when subject to the minimum necessary provision, the patient making the disclosure must seek guidance and approval of the Privacy Officer (or his/her designee) to review the request for compliance with the minimum necessary requirements.
   B) For non-routine requests, the requesting party will utilize the minimum necessary principle.
5) **Good Faith Reliance** – The department staff may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the request when:
   A) The disclosure is made to a **public official**, permitted to receive information, and the public official represents that the request is for the minimum necessary information
   B) The request is from another **covered entity**;
   C) The request is from a **professional** at another health care provider, or a business associate, and the professional or business associate asserts that the request is for the minimum necessary

FOR THE HIPAA SECURITY OFFICER

1) **Implementation Approach**. The department will systematically examine its operations and enact protocols in order to use or disclose the minimum amount of information necessary to accomplish its work. This examination will focus on implementing minimum necessary for
   A) Uses of PHI – limiting workforce access to the minimum necessary for specific patient's jobs
   B) Disclosures of PHI
   C) Requests for PHI

Further, department personnel will be familiar with procedures for routine disclosures and requests.

2) **Limiting Workforce Access to PHI**: Access to the PHI will be granted based on the employee's role and determined by the Privacy Officer of the department. The department will identify:
   A) Those persons or classes of persons (including Business Associates), who require access to PHI to carry out their duties, in the workforce, including interns and trainees, will be listed according to job classification with the necessary minimal necessary PHI required for successful job performance to serve the patients, 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.
   C) Safeguards will be developed, documented and implemented to restrict workforce access to the minimum necessary, especially as detailed in Policy 2030 Facility Security and Access Control.

   The Privacy Officer will document the results of this analysis. See the Appendix E Workforce Access to PHI and Safeguards

1030 Confidentiality Safeguards (Oral & Written)

POLICY
The department shall maintain appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

AUDIENCE
All Staff

REFERENCES
45 CFR 164.530(c) – Administrative, Technical, and Physical Safeguards

PROCEDURES:

1) **General Procedures**
   A) Employees shall be familiar with Appendix D Facility Security and Safeguards for Oral and Written PHI regarding staff, patients, parent and other visitor access to the facility.
   B) Employees shall escort visitors through the premises. On days when public meetings are held, access to the department is left open for anyone to walk through unescorted. Signage is placed to direct the public to the appropriate meeting room.
2) **Safeguards for Electronic PHI**. The HIPAA Security policies detail physical, technical and administrative safeguards to protect electronic PHI. In addition, these policies detail some of the physical security measures for paper records.
3) **Enforcement**. The Privacy Officer, Health Commissioner and/or Designated Manager are responsible for enforcing this policy. Employees who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.
4) **Compliance Audits/Facility Review/Policy Update**. At least annually the HIPAA Privacy Officer shall audit staff compliance with these guidelines. The audit shall consist of a walk-through of the facility, with observations recorded, such as placement of desks, location of computer equipment, any papers with PHI that would be visible to a visitor, etc. The results shall be discussed with the Health Commissioner, and any appropriate actions taken. Also, the Privacy Officer shall update Appendix G annually or as necessary.

1040 Speaking with the Family and Friends of a Patient Receiving Services

POLICY
Department personnel are allowed to disclose protected health information to family, friends and other individuals involved with the care of a patient, in specific situations, after giving the patient the opportunity to either agree to or object to the disclosure.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.510(b)

PROCEDURES
1) If the patient is present
   A) If a family member, or friend of the patient is present while services are being rendered, an employee serving the patient may disclose PHI after one of the following
      i) verbally seeking permission for the disclosure, and the patient agrees, or
      ii) giving the Patient the opportunity to object to the disclosure, and the patient does not express an objection, or
      iii) the staff member reasonably infers from the circumstances, based on the exercise of professional judgment, that the patient does not object to the disclosure.
2) If the patient is not present
   A) Communications about the patient's care or payment for the patient's care
      i) In the event of a phone call or other discussion with a family member or one involved with the care of the patient being served by the department, where the patient is not present, the employee may use their professional judgment to determine if the disclosure is in the best interests of the patient. If the employee judges that the disclosure is in the best interest of the patient, the employee may disclose only the PHI that is directly relevant to the person's involvement with the patient's care or payment for care.
   B) Notifications regarding patient's location or general condition
      i) If the employee judges that it is in the patient's best interest, the employee may disclose PHI to notify a family member, a personal representative of the patient, or another person responsible for the care of the patient of the patient's location or general condition.

1050 Authorizations

POLICY
All disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization. The department will use an authorization form that conforms to the federal HIPAA regulations.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.508 – HIPAA requirements for authorizations

PROCEDURES
GENERAL PROCEDURES/GUIDELINES

1) All requests for release of information shall be directed to and approved by the Health Records Release Officer, or if they are absent, by a designated alternate. These officers are identified in Appendix G.
2) Unless otherwise authorized by these policies and/or state or federal law, disclosure requires specific authorization by the patient or his/her legal representative. A Standard Authorization Form is included as an Appendix. Authorizations may be accepted on other forms, as long as they contain all of the following:
   A) Full Name of the patient
   B) A specific description of the information to be released. For example, a range of dates, or category of record.
   C) The purpose or need for the disclosure
   D) The name of the individual, person, or agency disclosing the information
   E) Names of the individual, person, or agency to whom the disclosure is to be made
   F) The date, event, or condition upon which the authorization expires (which can be no longer than 180 days from the date of signing)
   G) Statement of the patient's right to revoke the authorization, an explanation of how to revoke it, and any exceptions to the right to revoke;
   H) Statement that the department may not condition treatment on whether the patient signs the authorization.
   I) A statement informing the patient of the potential that information disclosed could be redisclosed if the recipient is not subject to federal or state confidentiality restrictions.
   J) Signature and date of the patient or personal representative
   K) If the authorization is signed by a guardian or personal representative, a description of that person's relationship to the patient and authority to sign the authorization.
   L) Written in plain language.
2) A PHI authorization is considered invalid if authorization has the following defects:
   A) Authorization is incomplete
   B) Authorization is not dated or time has elapsed
   C) Authorization does not contain required elements as explained above
   D) The department is aware authorization has been revoked
   E) The department is aware information is false.
   F) Authorizations to release PHI cannot be combined with other documents
5) The department must retain the written or electronic copy of the authorization for a period of six (6) years from the later of the date of execution or the last effective date. This shall be included in the paper or electronic chart.
6) Upon instructions of revocation of authorization, department employees shall locate the original authorization form, annotate it as revoked, and take appropriate steps to prevent any further disclosure.
7) Note that information from other service providers contained in the Patient's record may be released with the patient's written authorization.
8) Fee Policy.
   A) No charge for processing requests from other healthcare providers.

B) Fees for photocopy requests made by the patient or the patient's personal representative or by other authorized individuals shall not be higher than the fees specified in ORC 3701.741, or the cost of providing the records, including postage, whichever is lower.

ADDITIONAL PROCEDURES FOR REQUESTS RECEIVED VIA FAX OR VIA MAIL

1) If a request for health records does not meet the standards of a valid authorization (see GENERAL PROCEDURES/GUIDELINES above), a Letter for Non-Conforming Requests for PHI shall be sent.
2) If no record is found, the request will be sent back to the Health Records Release Officer with a notation that no record was found.
   A) The Health Records Release Officer will send the requesting party a letter stating that CCPH does not have a record on the designated person;
   B) A photocopy of the authorization form will also be sent to the requesting party;
   C) The original authorization form and the photocopy of the letter will be filed in the Health Records' Correspondence File;
   D) A letter indicating no record on the designated person may either be faxed or mailed.
3) The Health Records Release Officer will process routine releases within two (2) business days.
4) All records shall be reviewed prior to release by the appropriate medical or nursing personnel for accuracy, completeness and adherence to appropriate standards of care. If there are any potential liability issues identified, then the record shall be reviewed by the Canton City Law Department before completing the release.
5) Record requests from an attorney or requested by a subpoena will be reviewed by the appropriate coordinator and by the Canton City Law Department. The coordinator and Canton City Law Department will date and initial the release. These requests will usually be processed within 15 working days.
6) A copy of the Authorization form will be sent along with a copy of the requested records to the individual/organization designated in the request and will be sent via mail unless determined to be an emergent need.
7) The original Authorization form will be filed in the health record.

ADDITIONAL PROCEDURES FOR REQUESTS PRESENTED IN PERSON

1) For authorizations presented in person for immediate release, the staff member shall verify the identity of the recipient according to Policy 1060 Verification, after which the information may be released.

ADDITIONAL PROCEDURES FOR REQUESTS MADE VIA TELEPHONE

1) Health information will not be given over the telephone, except for urgent medical care or other situations specified in Policy 1090 Disclosures that do Not Require an Authorization.
2) Urgent requests for information will be directed to the appropriate clinical staff.
3) For a confirmed urgent medical care, the record will be pulled from file and the needed information given over the phone. A note will be added into the record detailing the release of information.
4) If a faxed copy of records is requested, the requesting party will fax a Release of Information Request signed by the patient.
5) Non-urgent requests will not be handled by telephone. It will be explained to the requesting party that in order to release any information, a Release of Information Request must be signed by the patient. The requesting party will be instructed to fax or mail the Release of Information Request to the appropriate Health Records Release Officer before any action can be taken.

ADDITIONAL PROCEDURES FOR DISCLOSURE OF HIV/AIDS TEST RESULTS

1) Any disclosure of the results of HIV testing or clinical information pertaining to a diagnosis of HIV/AIDS shall be in writing and accompanied by a written statement as follows: "This information has been disclosed to you from confidential records protected from disclosure by state law. You shall make no further disclosure of this

information without the specific, written, and informed release of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is not sufficient for the purpose of the release of HIV test results or diagnoses."

2) Client must complete a separate authorization form (see Attachment 5 - Authorization for Confidential HIV Test Results)

1060 Verification

POLICY
The department will take reasonable steps to verify the identity and/or the authority of the person requesting protected health information (PHI) of a patient.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
164.514(h)(1) Verification Requirements

PROCEDURES

REQUESTS FROM A PUBLIC OFFICIAL OR AUTHORITY

1) In verifying the identity and legal authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI, department personnel may rely on the following, if such reliance is reasonable under the circumstances, when disclosing PHI:
   A) Documentation, statements, or representations that, on their face, meet the applicable requirements for a disclosure of PHI
   B) Presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person
   C) A written statement on appropriate government letterhead that the person is acting under the government's authority
   D) Other evidence of documentation from an agency, such as a contract for services memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official
   E) A written statement of the legal authority under which the information is requested
   F) If a written statement would be impracticable, an oral statement of such legal authority
   G) A request that is made pursuant to a court order and subpoena or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority
2) The following issues should be addressed before releasing PHI once a request is received:
   A) Is the requestor who she/he claims to be
   B) Does the requestor have the authority to request PHI. If the request involves a court order, subpoena, or other legal request, follow the procedures outlined in the Policy 1090 Disclosures that do Not Require an Authorization.

REQUESTS FROM A PATIENT, PARENT, GUARDIAN OR PERSONAL REPRESENTATIVE

1) A properly completed, valid Authorization per the specifications in Policy 1050 Authorizations is sufficient verification of the identity and authority of the individual requesting information.
2) For requests for information other than formal record releases, staff must first verify both the identity and the authority of the individual prior to releasing PHI:
   A) If the individual is known to the staff person, this is sufficient verification of identity.
   B) If the individual is requesting information in person, identity should be verified by reviewing a State issued photo ID or other photo ID that includes birthdate.
   C) Identity can be verified by questioning the individual regarding their knowledge of information in the record of the patient being served, such as birth date, previous dates of service, etc., which only an authorized person would typically know.
   D) For requests from someone other than the patient or parent, the person's authority to obtain information must also be verified. For example, a healthcare Power of Attorney and/or statement from the patient that the requestor is a HIPAA Personal Representative would demonstrate proper authority. See also Policy 1040 Speaking with Family and Friends of a Patient Receiving Services for situations where it may be permissible to give information to a family member.

1070 Minors, Personal Representatives and Deceased Patients

POLICY
All staff will follow appropriate guidelines, set forth in this policy, in situations with patients who are minors or are deceased, and when dealing with their "Personal Representatives", to permit release of PHI and to provide for patients and their personal representatives to exercise the patient's HIPAA rights.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.502(f) & (g)

PROCEDURES:
1) Patients, who are minors, and who are legally allowed to consent to treatment under state law may exercise all rights regarding access to, requests for amendment to, and release of their PHI pursuant to a written authorization. The department will follow all other state laws regarding a minor's control over disclosure of his/her records, including any restrictions on disclosure to parents.
2) The department recognizes a patient's personal representative as a person authorized to exercise rights of access and/or inspection of PHI, rights to request amendment of PHI, and the right to sign the CCPH Standard Authorization Form which permits release of PHI.
3) The department recognizes the following persons to be personal representatives:
   A) The parent of a child younger than 18 years old
   B) The non-custodial parent of a child younger than 18 years old,
   C) An individual who is recognized through durable power of attorney to have authority to act on the behalf of the Patient
   D) The legal guardian of the patient
   E) Any other person authorized by law
   except in Abuse, Neglect, Human Trafficking, and/or Endangerment situations, or where the department has received a court order or other documentation limiting privileges of a non-custodial parent as provided below.
      i) Abuse, Neglect, Human Trafficking, and/or Endangerment Situations. Notwithstanding a state law of any requirement of this paragraph to the contrary, the department may elect not to recognize a person as a personal representative of a patient. In order for the department to choose not to recognize a person as a personal representative, the department must decide that it is not in the best interest of the patient to treat the person as the patient's personal representative and must believe that one of the following conditions exist:
         1) The patient has been or may be subjected to domestic violence, abuse, or neglect by a parent, guardian, or personal representative.
         2) Treating such person as the personal representative could endanger the patient.
      ii) Receipt of a court order limiting privileges of a non-custodial parent. In the event that the department receives from the custodial parent a court order limiting the privileges of the non-custodial parent to act in the capacity of the child's personal representative, the department shall adhere to the restrictions in the court order.
4) **Deceased Patients**
   A) For deceased patients, employees may disclose to a family member, other relative, a close personal friend of the individual, or to the patient's personal representative, who was involved in the deceased individual's care or payment for health care prior to death, PHI that is relevant to that person's involvement, unless doing so is inconsistent with any prior expressed preference of the deceased person.
   B) Other than provided above, PHI generated during the life of an individual is protected from disclosure after death unless disclosure is for treatment or payment, quality assurance or other auditing or program review functions. The department and its employees cannot release PHI regarding a deceased patient unless a valid personal representative has been established and has requested the PHI through the proper authorization process.

C) PHI may be disclosed to the executor or administrator of the estate when the information is necessary to administer the estate.

D) Absent an executor, administrator, or other court-appointed representative for the deceased patient's estate, the following persons listed below may authorize the release of PHI in order of priority. An entire category must be exhausted (i.e., no people in the category exist or are still alive) before moving to the next category.
   i) Spouse (if married)
   ii) The person's children
   iii) The Person's parents
   iv) The Person's brothers or sisters
   v) The person's uncles or aunts;
   vi) The person's closest relative by blood or adoption
   vii) The person's closest relative by marriage

E) Note that the definition of PHI excludes information about people deceased for more than 50 years. With approval of the Health Commissioner, information about individuals deceased for more than 50 years may be released.

F) PHI may be released to coroners, medical examiners, and funeral directors as provided in Policy 1090.

1080 Duty to Report Violations and Security Incidents

POLICY
Confidentiality of patient information, and the computer security required to protect information regarding patients is taken very seriously at the department. Employees are required to follow all rules in these policies. Any employee who becomes aware of a violation of either confidentiality or computer security rules is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

AUDIENCE
All Staff

REFERENCES:
164.530(e)(1) –Sanctions

PROCEDURES:
1) Any employee observing a violation of any of the HIPAA policies is to report the violation to his/her supervisor. Failure to report a Privacy or Security Violation is in itself a disciplinable offense.
2) The supervisor should refer the incident to the Privacy Officer and/or the Security Officer. The Privacy and/or Security Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, patients, or others, and/or review of computer or paper audit trails.
3) For security breaches, the Privacy and/or Security Officer will follow any procedures detailed in Policy 2100 Breach Reporting.
4) For Privacy Violations, the Privacy Officer will follow procedures in Policy 1300 Mitigation.
5) A written incident report will be written by the Privacy and/or Security Officer. It will be filed
   A) in the Privacy Officer's Privacy Violations file
   B) in the employee's personnel file
6) Employee Discipline. The Privacy and/or Security Officer, in conjunction with the Health Commissioner, shall take appropriate disciplinary action as detailed in Policy 1360 Sanctions for Staff Violations of Privacy/Security Policies, and document this action in the employees personnel file.
7) A post-incident review will be conducted by the Privacy and/or Security Officer, with any corrective action taken, such as a change in policy, additional training, or other appropriate action.

1090 Disclosures that do Not Require an Authorization

POLICY
Department employees may use and disclose PHI in specific situations authorized by state and federal statute. In these cases, the patient's authorization is not required. Staff will carefully follow specific requirements for these unusual and infrequent disclosures. These disclosures include:

- For public health purposes such as reporting communicable diseases, work-related illnesses, or other diseases and injuries permitted by law; reporting births and deaths, and reporting reactions to drugs and problems with medical devices.
- To schools, regarding proof of immunization, if given permission from parent.
- To protect victims of abuse, neglect, or domestic violence.
- For health oversight activities such as investigations, audits, and inspections.
- For judicial and administrative proceedings.
- For law enforcement purposes.
- To coroners, medical examiners, and funeral directors.
- For organ, eye or tissue donation.
- Research.
- To reduce or prevent a serious threat to public health and safety.
- Specialized government functions.
- For workers' compensation or other similar programs if applicable.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR § 164.512

PROCEDURES
Department employees will follow the indicated procedures for the various special circumstances detailed below:

1) **Authority to Release.** All requests for release of information shall be directed to the Health Records Release Officer indicated in Appendix G. Non-routine releases of information shall also be reviewed and approved by the Canton City Law Department. The Health Records Release Officer and Law Department will date and initial the release.
2) **Relevant Law.** The procedures below are based on the federal HIPAA regulations. Any release of information not regulated by the HIPAA, which include information from the Non-Health Care Component of CCPH as detailed in Appendix G, are governed by Ohio Revised Code 3701.17, which must be followed instead of HIPAA.
3) **Recordkeeping**. For all of the disclosures authorized below, the employee handling the disclosure will document the details of the disclosure on the Disclosure Log. Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.
4) **When required by law**
   A) The department may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
5) **For public health purposes** PHI may be used or disclosed to:
   A) A **school**, regarding their student or prospective student, if
      i) the school is required by law to have such proof of immunization prior to admitting the individual; and
      ii) the department has obtained permission from the parent, guardian, or other person acting in loco parentis of the individual. The permission need not be in writing and the department must document that they received permission.
   B) A public health authority authorized by law to collect or receive information for the purpose of preventing

or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions;

C) A public health or other government authority authorized by law to receive reports of child abuse or neglect;

D) A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance;

E) A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.

6) **To protect victims of abuse, neglect, or domestic violence**

A) Reports of child abuse

i) Reports of child abuse shall be made in accordance with state law

ii) The department may disclose PHI related to the report of abuse to the extent required by applicable law. Such reports shall be made to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

B) Reports of abuse and neglect other than reports of child abuse or neglect.

i) The department may disclose PHI about a patient believed to be a victim of abuse, neglect, or domestic violence to a governmental authority authorized to receive such reports if:

1) the patient agrees; or

2) the department believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm.

If the patient lacks the capacity to agree, disclosure may be made if not intended for use against the patient and delaying disclosure would materially hinder law enforcement activity.

ii) The department staff member making the disclosure must promptly inform the patient whose PHI has been released unless:

1) doing so would place the patient at risk of serious harm; or

2) the department would be informing a personal representative, and the department reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient as determined by the department, in the exercise of professional judgment.

7) **For health oversight activities such as investigations, audits, and inspections**

A) PHI may be used or disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.

B) Specifically excluded from this category are investigations of a patient that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

8) **For judicial and administrative proceedings**

A) The rules and laws regarding disclosure which are discussed by this policy are complex. The HIPAA Privacy Officer may request permission from the Health Commissioner to consult with an attorney if he/she has any uncertainty about disclosures detailed in this policy.

B) The department must always comply with a **court order**, but only in accordance with the express terms of the order.

C) For a **subpoena, discovery request** or **other lawful process**: the department may comply with such legal requests only if:

i) The department receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the patient who is the subject of the requested PHI has been given notice of the request; or

ii) The department receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.

9) **For law enforcement purposes**

A) PHI may be disclosed for the following law enforcement purposes and under the specified conditions:

i) Pursuant to court order or as otherwise required by law, i.e., laws requiring the reporting of certain types of wounds or injuries; or commission of a felony, subject to any exceptions set forth in applicable law.

ii) Decedent's PHI may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct.
iii) The department may disclose to a law enforcement official protected health information that the department believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the department.
iv) If the department is providing emergency health care in response to a medical emergency, other than such emergency on the premises of the department, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

If the department believes that a medical emergency is the result of abuse, neglect, or domestic violence of the patient in need of emergency health care, the limitations in the previous section above does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject the last condition above, "To protect victims of abuse, neglect, or domestic violence"

B) PHI may be disclosed to law enforcement personnel to report the commission and nature of a crime; The location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime. When responding to requests about the location of a suspect, fugitive, material witness, or missing person, the following PHI may be released:
i) Name and address
ii) Date and place of birth
iii) ABO blood type and RH factor
iv) Type of injury
v) Date and time of treatment
vi) Date and time of death, if applicable,
vii) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair scars, and tattoos

C) Compliance/Enforcement of privacy regulations: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

10) **To coroners, medical examiners, and funeral directors**
A) PHI may be disclosed to coroners, medical examiners and funeral directors, as necessary for carrying out their duties.

11) **Organ, eye or tissue donation**
A) PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.

12) **To reduce or prevent a serious threat to public health and safety**
A) The department may disclose PHI as follows, to the extent permitted by applicable law and ethical standards:
B) PHI may be used or disclosed if the entity believes in good faith
i) that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or
ii) the disclosure is to law enforcement authorities to identify or apprehend a patient who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.
C) Disclosures of admitted participation in a violent crime are limited to the patient's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.
D) Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the patient to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

13) **Specialized government functions**
A) National Security and Intelligence: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, Counterintelligence, and other activities authorized by the National Security Act.
B) Protective services: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
C) The department may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other patient protected health information about such inmate or patient, if the

correctional institution or such law enforcement official represents that such protected health information is necessary for:

i) The provision of health care to such patients;
ii) The health and safety of such patient or other inmates;
iii) The health and safety of the officers or employees of or others at the correctional institution;
iv) The health and safety of such patients and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
v) Law enforcement on the premises of the correctional institution; and
vi) The administration and maintenance of the safety, security, and good order of the correctional institution.

The provisions of this section do not apply after the patient is released from custody.

D) Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

14) **In connection with "whistleblowing"**. In connection with "whistleblowing", or reporting of a violation of law or ethics, an employee of department may disclose PHI to his/her attorney.

15) **For workers' compensation or other similar programs if applicable**.

A) PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

PATIENT RIGHTS

1200 Patient's Right to Access Records

POLICY
Patients, served by CANTON CITY PUBLIC HEALTH, and their personal representatives, have the right to access and/or inspect the PHI contained in the designated record set, subject to any limitations imposed by law.

AUDIENCE
Privacy Officer, Supervisors of Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.524(e) patient's right to access PHI and (b) Time limits on response to access and (c) Form of access

PROCEDURES
1) Who May Access Records
   A) A patient served by CANTON CITY PUBLIC HEALTH above the age of 18, the parent/guardian of a child, the guardian of an adult not able to act on their own behalf, or any "personal representative", of any of those patients may access the records. See Policy 1070 Minors, Personal Representatives and Deceased Patients.
   B) A patient or parent may include any 3rd party of their choosing, including an attorney, to review the records.
   C) CANTON CITY PUBLIC HEALTH may presume that either parent of a minor may have access unless presented with documentation that the parent does not have authority under applicable state law governing such matters as guardianship, separation, or divorce.
2) Procedure, form and method of access
   A) Requests for access to records shall be directed to the Privacy Officer or his/her designee
   B) The Privacy Officer shall follow the procedures in Policy 1060 Verification to verify the identity of the requestor. Any grant of access to someone other than the parent
   C) CANTON CITY PUBLIC HEALTH shall provide the patient with access to their records in any of the following ways requested by the patient:
      i) By inspection. CANTON CITY PUBLIC HEALTH shall provide a private room for the patient to review the records under the supervision of a CANTON CITY PUBLIC HEALTH staff member who will ensure that the record is not altered, or
      ii) Photocopy. CANTON CITY PUBLIC HEALTH shall provide a photocopy of the entire record or portion of the record requested.
      iii) Electronic format. For any records stored by the department electronically, CANTON CITY PUBLIC HEALTH shall provide an electronic copy to a patient upon request. The format shall be negotiated with the patient and reasonable requests must be honored. Possible formats include USB Flash drives, email, or patient portal. Prior to sending any record via unsecured email, the office staff must inform the patient that unsecure email could be intercepted by a 3rd party. If the patient has been informed of the risks and desires email transmission, this request must be honored. The department may charge a fee for materials, for example, for a USB Flash drive.
   D) The Privacy Officer or his/her designee shall maintain a record of parties accessing records (except the access by the patient or their parent) including the name of the party, the date access was given, and the purpose of access.
3) Other services/rights of patients, parents, and guardians
   A) CANTON CITY PUBLIC HEALTH will respond to reasonable requests for explanation and interpretation of the records.
4) Time for response to request for access
   A) Access shall be granted without unnecessary delay. Requests in all cases shall be honored within 10 business days.
5) Fees for copying
   CANTON CITY PUBLIC HEALTH fee schedule is as indicated in Appendix G – Miscellaneous.

1210 Patient's Right to Request Amendment of Records

POLICY
Subject to the rules set forth in applicable requirements and CANTON CITY PUBLIC HEALTH procedures, a patient has the right to have CANTON CITY PUBLIC HEALTH amend PHI or a record about the patient in a designated record set for as long as the PHI is maintained in the designated record set.

AUDIENCE
Privacy Officer, Supervisors of Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.526(f) patient's right to request amendment

PROCEDURES
REQESTS FOR AMENDMENTS

1) A patient, parent, guardian, or other person acting as a HIPAA personal representative may request amendment of PHI about the patient (and exercise rights for hearing and statements of disagreement), which they believe is inaccurate, misleading, or violates the rights of the patient, and is held by CANTON CITY PUBLIC HEALTH or any Business Associate. Such request shall be in writing and shall be subject to the requirements set forth in these procedures.
2) The Privacy Officer of CANTON CITY PUBLIC HEALTH is responsible for receiving requests for amendment, processing the requests, arranging for any hearings, and completing required documentation.
3) CANTON CITY PUBLIC HEALTH will act on a request for amendment without unnecessary delay and no later than 60 days after the date of the request.
4) If CANTON CITY PUBLIC HEALTH accepts the requested amendment, in whole or in part,
   A) CANTON CITY PUBLIC HEALTH must make the appropriate amendment, and inform the patient and other persons or entities who have had access to the information.

   Otherwise, if CANTON CITY PUBLIC HEALTH believes the existing record is correct as is, it may deny the amendment:
   A) If an amendment is denied, CANTON CITY PUBLIC HEALTH will give written notice in plain language which includes the following:
      i) The basis for the denial;
      ii) The patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;
      iii) A statement that, if the patient does not submit a statement of disagreement, the patient may request that CANTON CITY PUBLIC HEALTH provide the patient's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment
      iv) The patient's right for a hearing to challenge the information
   B) If the patient submits a statement of disagreement, the Privacy Officer will insert this statement into the appropriate portion of the record. Otherwise, the Privacy officer will insert into the record that the patient requested an amendment and CANTON CITY PUBLIC HEALTH's denial.
   C) CANTON CITY PUBLIC HEALTH may prepare a written rebuttal to the patient's statement of disagreement. Whenever such a rebuttal is prepared, CANTON CITY PUBLIC HEALTH must provide a copy to the patient who submitted the statement of disagreement.
   D) The inserted statement of disagreement and any rebuttal become a part of the permanent record and must be included with all future disclosures of the covered records
   E) At the patient's request, CANTON CITY PUBLIC HEALTH will send a copy of the changed record to any party requested by the patient
   F) If the disclosure which was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, CANTON CITY PUBLIC HEALTH may separately transmit the information to the recipient of the transaction in a standard EDI format.

1220 Patient's Right to Receive an Accounting of Disclosures

POLICY
In accordance with HIPAA Regulations, Patients must be told, if they ask, what personal health information has been sent to whom and why.

AUDIENCE
Privacy Officer, Supervisors of Staff providing patient services and with access to PHI

REFERENCES
45 CFR 164.528(d) patient's right to an accounting of disclosures of PHI

PROCEDURES
1) The Privacy Officer shall be responsible for ensuring that proper records are kept to allow for proper and complete responses to any requests for accountings of disclosures. See also procedures listed in Policy 1090 Disclosures that do Not Require an Authorization and Policy 1050 Authorizations which detail the use of the Disclosure Log.
2) Generally, a patient has the right to request an accounting of disclosures of their PHI by CANTON CITY PUBLIC HEALTH and its business associates during a time period of up to six years prior to the date of the patient's request. Most disclosures are **not** required to be included in the accounting. The types of disclosures which are **not** required to be accounted for are:
   A) For the purposes of treatment, payment and health care operations (45 CFR §164.502);
   B) To the patient receiving services, or to a parent, guardian or personal representative, of the patient's own PHI (45 CFR §164.502);
   C) Incidental disclosures, as detailed in (45 CFR §164.502)
   D) Pursuant to an authorization (45 CFR §164.508);
   E) To persons involved in the patient's care or other notification purposes (45 CFR §164.510);
   F) For national security and intelligence purposes, as detailed in (45 CFR §164.512(k)(2);
   G) Disclosures to prisons and other law enforcement agencies regarding a patient who is in custody, as detailed in (45 CFR §164.512(k)(5);
3) Any employee who makes a disclosure other than listed above shall document the disclosure in the Patient File, with all information described in step 6B below. More specifically, the following types of disclosures must be documented:
   A) To public health authorities
   B) Birth and death reporting
   C) To law enforcement regarding crime on premises
   D) To law enforcement in emergencies where crime is suspected
   E) For cadaveric organ, eye, tissue donation purposes
   F) For judicial and administrative proceedings
   G) For research with an IRB waiver
   H) To military command authorities
   I) For Workers Comp purposes
   J) To correctional institutions except as detailed in 2G above
   K) About decedents to medical examiners, funeral directors, coroners
   L) For public health activities
   M) About victims of abuse
   N) Regarding child abuse or neglect
   O) To the FDA
   P) To a person who may have been exposed to a communicable disease
   Q) To health oversight agencies for audits, civil or criminal investigations, inspections, licensure or disciplinary actions
   R) In response to a court order

S) In response to a subpoena or discovery request
T) As required by law for wound or injury reporting
U) For identification & locating suspect or fugitive
V) Unlawful and unauthorized disclosures we have knowledge of

4) Health oversight agencies and law enforcement officials may request a suspension of a patient's rights to disclosure. If such a request is received, follow procedures in 45 CFR § 164.528.

5) The HIPAA Privacy Officer shall comply with a patient's request for an accounting within 45 days of the request. CANTON CITY PUBLIC HEALTH does not charge a fee for accountings.

6) The written accounting must meet the following requirements:
   A) All disclosures of the Patient's PHI during the 6 years prior to the request (or such shorter period as is specified in the request) as stated above.
   B) As to each disclosure, the accounting must include:
      i) The date of the disclosure
      ii) The name of the entity or person who received the PHI, and, if known, the address of such entity or person
      iii) A brief description of the PHI disclosed
      iv) A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis of the disclosure, or as an alternative, a copy of the request for the disclosure
      v) If during the time period for the accounting, multiple disclosure have been made to the same entity or person for a single purpose, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosure made during the accounting period and the date of the last such disclosure during the accounting period.
   C) CANTON CITY PUBLIC HEALTH will retain documentation (in written or electronic format) for a period of 6 years:
      i) All information required to be included in an accounting of disclosures of PHI
      ii) All written accountings provided to patient

1230 Patient's Right to Request Additional Restrictions

POLICY
CANTON CITY PUBLIC HEALTH supports patient's right to request restrictions on the use or disclosure of protected health information which may be above and beyond the restrictions in organizational policy

AUDIENCE
Privacy Officer, Supervisors of Staff providing patient services and with access to PHI

REFERENCES
45 CFR § 164.522(a)

PROCEDURES:

1) **Refer the Request to the Privacy Officer:** All requests will be referred to the HIPAA Privacy Officer, or his/her designee. Upon receiving a request, the Privacy Officer shall consider the following factors, in the decision to grant or deny the request:
   A) Whether the restriction might cause the organization to violate applicable federal or state law;
   B) Whether the restriction might cause the organization to violate professional standards, including medical ethical standards;
   C) Whether the organization's systems and organization make it very difficult or impossible to accommodate the restriction;
   D) Whether the restriction might unreasonably impede the organization's ability to serve the patient;
   E) Whether the restriction appears to be in the best interests of the Patient.
2) **Decision whether department will agree**: CANTON CITY PUBLIC HEALTH is not obligated to agree to any requests for restriction except:
   A) Disclosures to 3rd party payers. If the patient agrees to pay for a service in full, any request to avoid billing a 3rd party payer must be honored.
   B) For any other request, the Privacy Office shall make the determination whether the organization will honor the request.
3) **Notify the Patient:** CANTON CITY PUBLIC HEALTH will notify the Patient of its final decision (whether approving or denying the request) in writing. The notice will be maintained in the Main Patient Record.
   A) Granting the Request: If CANTON CITY PUBLIC HEALTH agrees to the restriction, the notice to the patient will clearly state what restriction CANTON CITY PUBLIC HEALTH is agreeing to in language the Patient will understand. This notice will state that the restriction will not apply if the information is needed for emergency treatment.
   B) Denying the Request: If the request is denied, the notice will clearly state why the request cannot be complied with, in language the Patient will understand.
4) **Take Appropriate Action to Implement Restrictions:** If CANTON CITY PUBLIC HEALTH agrees to the requested restriction, the Privacy Officer/designee will be responsible for taking appropriate action to implement the restriction.
5) **Modifying or Terminating a Restriction:** A Patient may request a restriction to be eliminated at any time. If the organization desires a modification, consult legal counsel regarding appropriate procedures.
6) **Documentation:** The Privacy Officer is responsible for maintaining the following documents, to assure that additional privacy protections are handled properly, and assure they are maintained for six years from the date of their creation:
   A) Copies of patient requests for restrictions
   B) Copies of any notice informing the patient about the organization's decision to grant or deny a restriction
   C) Copies of any written patient request to terminate a restriction, or alternatively, copies of any documentation in the patient's record that the patient made such request orally

1240 Patient's Right to Request Confidential Communications

POLICY:
Patients (or their parents) are entitled to request confidential communications, including for example, to not receive communications at their home address. These requests will be honored to the extent that they can be reasonably accommodated with our administrative systems.

AUDIENCE
Privacy Officer

AUTHORITY
164.522(b) Confidential communications requirements

PROCEDURES
1) **Request**. Patients, or their personal representative, may make a request for confidential communications in writing to the Privacy Officer.
2) **Non-intimidation**. When the Privacy Officer receives a request, the privacy officer may not ask the reason for the request. The Privacy Officer shall contact the patient making the request to obtain an alternate means of contacting them (e.g. cell phone, PO Box, etc.). The patient will be informed at that time of steps the department will take to implement the request.
3) **Implementation**. Reasonable requests must be honored. If existing systems are capable of administering the request, the privacy officer shall take necessary steps to implement the request, such as adjusted phone numbers or addresses in computer files or mailing lists.
4) **Documentation**. The Privacy Officer shall document the request, and disposition, in the Patient's Record.

CONFIDENTIALITY POLICIES FOR SUPERVISORS

1300 Mitigation

POLICY
CANTON CITY PUBLIC HEALTH will mitigate, to the extent reasonable and practical, harm that is done to patients as a result of our violations of these HIPAA policies

AUDIENCE
Privacy Officer, Health Commissioner

AUTHORITY
164.530(f) Mitigation

PROCEDURES
1) **Assessment.** The HIPAA Privacy Officer shall investigate and access the impact of any violations of these policies on the patient. The assessment should evaluate any type of harm, including financial, reputation, inconvenience, embarrassment or any other type of harm.

2) **Mitigation.** The HIPAA Privacy Officer shall determine some action, within the power of the department, which can mitigate that harm. If it is within the scope of their authority, the HIPAA Privacy Officer shall take steps. If it is beyond the scope of the Privacy Officer's authority or budget, the Privacy Officer shall take the proposed action to the Health Commissioner who shall make the final decision about mitigation steps.

1310 Notice of Privacy Practices

POLICY
CANTON CITY PUBLIC HEALTH will provide a written Notice of Privacy Policies, as required by law, to each Patient.

AUDIENCE
All Staff providing patient services and with access to PHI

REFERENCES
45 CFR 164.520

PROCEDURES
1) **Creation and Update of Notice**.
   A) The HIPAA Privacy Officer shall create the Notice of Privacy Practices to conform to requirements of the HIPAA regulations.
   B) Upon change of the Notice of Privacy Policies, a new version must be posted on the website, must be posted in the office, and made available to any patient who asks.
2) **Distribution of Notice.**
   A) All patients and/or their parents will receive a copy of the Notice of Privacy Practices upon intake with the department.
   B) As part of that intake process, the patient and/or parent, guardian or personal representative, shall sign an acknowledgement of their receipt of this Notice as part of the intake paperwork. This acknowledgement will be retained as part of the permanent record.
3) **Other Postings and Requirements**
   A) The Notice of Privacy Practices will be posted in reception areas of all department facilities
   B) The Notice of Privacy Practices will be posted on the website, if a website exists.
   C) Copies of the notice will be maintained for 6 years.

1320 Non-intimidation and Non-retaliation

POLICY
CANTON CITY PUBLIC HEALTH will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against patients who exercise any right, not against staff or other patients who express the opinion that the department's policies are not consistent with the law, or not being implemented properly. CANTON CITY PUBLIC HEALTH will not require any patient receiving services to waive any of his/her rights under HIPAA as a condition of education, treatment, or enrollment.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
164.530(g) refraining from intimidating or retaliatory acts

PROCEDURES
1) No employee of the department will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
   A) **Any patient** for the exercise by the patient of any right under, or for participation by the patient in any process established by the HIPAA compliance rule;
   B) **Any patient** receiving services, or **other person** for:
      i) Filing of a complaint with the Secretary under HIPAA compliant
      ii) Testifying, assisting or participating in an investigation, compliance review, proceedings or hearing under Part C of Title XI; or
      iii) Opposing any act or practice made unlawful by HIPAA compliance rules, provided the patient or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protection health information.
2) Retaliatory action is defined as doing any of the following:
   A) Removing or suspending the employee from employment;
   B) Withholding from the employee salary increases or employee benefits to which the employee is otherwise entitled;
   C) Denying the employee a promotion that would have otherwise been received;
   D) Transferring or reassigning the employee;
   E) Reducing the employee in pay or position.
3) Non-retaliation statement – A person who in good faith brings a complaint will not be subject to retaliation. Retaliation against any person who falls within this definition, either patient served or staff member of CANTON CITY PUBLIC HEALTH, is strictly prohibited.
4) Prohibition against Waiver of Rights -- No employee of CANTON CITY PUBLIC HEALTH shall require patients to waive any of their rights under HIPAA as a condition of treatment.

1340 Privacy Complaints

POLICY
Any patient or employee may complain about the health district's HIPAA policies and procedures and/or the department's compliance with those policies and procedures. The Privacy Officer shall follow up and document all such complaints.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.530(d) HIPAA complaint procedures

PROCEDURES
1) The HIPAA Privacy Officer shall manage this complaint process, and shall be designated in the Notice of Privacy practices as the person to receive complaints.
2) An employee or patient should file their complaint in writing to the privacy officer. Those wishing to complain shall be directed to file the complaint in writing and submit it to the Privacy Officer.
3) Upon receipt of a complaint, the Privacy Officer (or the employee's supervisor or Health Commissioner) shall review and investigate the complaint.
4) If warranted, the Privacy Officer shall take corrective action, which may include
   A) Change of policy and/or procedure.
   B) Intervention with an employee who is not following procedures including additional training and/or sanctions
   C) Other action as appropriate
5) The Privacy Officer shall communicate the results of the investigation and any corrective action taken to the patient filing the complaint.
6) The Privacy Officer shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with Policy 1380 HIPAA Assignments and Documentation.

SHARED PRIVACY/SECURITY POLICIES

1350 Policy Updating and Staff Training

POLICY:
The department is committed to maintaining updated Policies as required by law, and to train staff as necessary on these policies.

AUDIENCE
All Staff

REFERENCES
45 CFR 164.530(b) and (i)

PROCEDURES:
1) The HIPAA Privacy and Security Officer shall conduct a review every three (3) years of all policies, and update policies as necessary based on new circumstances, changes in federal regulations and any changes in state laws and regulations. An audit trail of policy changes will be maintained as detailed in Policy 1380 HIPAA Assignments and Documentation.
2) The Fiscal Officer shall ensure that all new staff receive training on HIPAA Privacy and Security policies promptly after hiring, and will maintain documentation of the individual's training occurred in the personnel file or other permanent record.
3) The HIPAA Privacy and Security Officer shall ensure that staff receive training on HIPAA policies when they are substantially changed.

1360 Sanctions for Staff Violations of Privacy/Security Policies

POLICY
Confidentiality of individual information is taken very seriously at CANTON CITY PUBLIC HEALTH. Employees are prohibited from improperly using or disclosing confidential patient information as detailed in these HIPAA policies. Such improper uses include but are not limited to curiosity, malicious purpose, or financial gain. In addition, employees are expected to comply with all policies involving HIPAA mandated computer security. Employees who violate these policies will be subject to sanctions as detailed in this policy.

AUDIENCE
All Staff providing patient services and with access to PHI

AUTHORITY
45 CFR 164.530(e) Sanctions (Privacy rule)
45 CFR 164.308(a)(1)(ii)(C) Sanctions Policy (Security rule)

PROCEDURES
1) Any staff member observing a Privacy or Security Violation is to report the violation to his/her supervisor. Failure to report a Privacy Violation is in itself a disciplinable offense.
2) The supervisor should refer the incident to the Privacy Officer. The Privacy Officer shall, in conjunction with other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, patients, or others, and/or review of computer or paper audit trails.
3) The Privacy Officer or HIPAA Security Officer, in conjunction with the employee's supervisor, and the Office Manager will evaluate the severity of the violation, the degree of harm caused, the frequency of past violations, and the employee's overall record of performance with CANTON CITY PUBLIC HEALTH. Based on this evaluation, one or more of the following sanctions will be applied:
   A) Coaching on allowed uses and disclosures
   B) Formal warning
   C) Formal reprimand
   D) Requirement to review policies and procedures
   E) Suspension from 1 to 30 days without pay
   F) Termination
4) For grievous violations, such as uses or disclosures for financial gain or made with malicious intent, immediate termination may be appropriate. For other violations, because of the wide variety of types of violation possible and circumstances involved, considerable flexibility in administering sanctions is given to management.
5) The Privacy Officer, in conjunction with other members of the management staff as he/she deems appropriate, shall take action to mitigate the harmful effects of the Privacy Violation, if this is reasonable and possible.
6) A written incident report will be written by the Supervisor/Privacy Officer and filed in the Privacy Officer's Privacy Violations file, in the employee's personnel file, and one will be given to the employee.

1370 Business Associate and other Confidentiality Contracts

POLICY
CANTON CITY PUBLIC HEALTH will obtain satisfactory assurance that Business Associates will appropriately safeguard PHI by maintaining appropriate HIPAA Business Associate agreements that are compliant with HIPAA regulation standards.

AUDIENCE
All Staff with Business Associate Relationships

REFERENCES:
45 CFR 160.103 Definitions (of Business Associate)
45 CFR § 164.502(e) Disclosures to Business Associates
45 CFR § 164.504(e) Business Associate Contracts
45 CFR 164.308(b) (1),(2),(3) Security Rule - Business Associate Contracts

PROCEDURES

1) The department will have a written Business Associate Contract with every Business Associate. The department will use appropriate diligence to define the procedures, responsibilities and financial details in the event that the Business Associate's causes a data breach. See Appendix A Identifying who Is a Business Associate.
2) On an annual basis, the HIPAA Privacy Officer will review all vendor and other contractual relationships to verify that up-to-date Business Associate contracts are in place.
3) The Business Associate Contract will provide satisfactory assurances that the Business Associate will not use or disclose the PHI of CANTON CITY PUBLIC HEALTH individuals receiving services other than as provided in the Business Associate Contract. The Business Associate Contract will conform to both the requirements of the HIPAA regulations. See Appendix B - Sample HIPAA Business Associate Agreement.
4) In the event CANTON CITY PUBLIC HEALTH learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, CANTON CITY PUBLIC HEALTH will take steps to cure the breach or end the violation. If CANTON CITY PUBLIC HEALTH is unable to cure the breach, and if it is feasible to terminate the agreement, then relationship with the vendor or entity shall be terminated.
5) Whenever the Non-Health Care Component of CCPH, as defined in Appendix G, releases Protected Health Information to a third party, the State Law Provider Confidentiality Agreement detailed as Attachment 6 must first be executed with the third party.

1380 HIPAA Assignments and Documentation

POLICY:
CANTON CITY PUBLIC HEALTH will maintain written Policies and Procedures, including a 6-year audit trail. In addition, all documentation required by HIPAA regulations will be maintained for 6 years. The HIPAA Privacy Officer shall be responsible for insuring the proper maintenance of all required documentation.

AUDIENCE
All Staff providing patient services and with access to PHI

REFERENCES:
Federal Law 45 CFR 164.530(j) – Documentation requirement,
164.520(e) – Notices of Privacy Practices;
164.524(e) – Access of patients to protected health information;
164.526(f) – Amendment to protected information;
164.508(b)(6) – Uses and disclosures for which an authorization is required;
164.512(i)(2) – Uses and disclosures for research purposes;
164.522(a)(3) – Rights to request privacy protection for protected health information;
§164.528(d) – Accounting of disclosures of protected health information – Implementation specification

PROCEDURES:
1) The Health Commissioner shall designate an individual to be the Privacy Officer, who is responsible for development, implementation, enforcement, and update of HIPAA Privacy policies and procedures.
2) The records covered by HIPAA shall be detailed and documented following the procedures for the "Designated Record Set" of the HIPAA regulations. In addition, the Health District shall define which of its activities give rise to its HIPAA obligations, and which activities are not regulated by HIPAA. This analysis shall be documented in Appendix G.
3) **HIPAA Mandated records**. HIPAA Mandated records include the following:
   A) HIPAA Required designations, including, hybrid entity designation if applicable, description of records in Designated Record Set, the names of staff responsible for duties of Privacy Officer, Security Officer, receiving HIPAA complaints, providing access to Patient records, receiving requests for amendment of Patient records, answering questions about HIPAA policies and procedures.
   B) Notice of Privacy Practices, as described in Policy 1310 Notice of Privacy Practices.
   C) Restrictions on use or disclosure of PHI agreed to by CANTON CITY PUBLIC HEALTH as described in the Policy1230 Patient's Right to Request Additional Restrictions.
   D) Records of disclosures, as required by the Policy 1220 Patient's Right to Receive an Accounting of Disclosures.
   E) Any signed authorization as described in Policy 1050 Authorizations.
   F) All privacy-related complaints received, and their disposition, if any, as described in Policy 1340 Privacy Complaints.
   G) Staff training records, as detailed in Policy 1350 Policy Updating and Staff Training.
   H) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Policy 1080 Duty to Report Violations and Security Incidents.
   I) Incident Reports and other documentation specified by Policy 2100 Breach Reporting and Policy 3090 Security Incident Response and Reporting.

   The above records will be maintained for 6 years
4) **Policy and Procedure Audit Trail** – When created or updated, all policies will be annotated with the approval date and revision history. Current policies will be maintained in a computer file folder designated "current policies". Any previous versions will be renamed with the creation date in the file name, and placed in a computer file folder designated "archived policies".
5) **Updating Required Designations**. The Privacy Officer, will maintain and update HIPAA Required Designations as necessary.

6) **Compliance Notes**. The Privacy Officer and Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, and internal audit activities.
7) **Internal Audit**. The privacy officer shall conduct a periodic audit, as necessary, to ensure proper maintenance of all documentation itemized in this policy.

HIPAA SECURITY POLICIES

POLICIES FOR HEALTH COMMISSIONER AND THE SECURITY OFFICER

2000 HIPAA Security Officer and Security Management Process

POLICY
CANTON CITY PUBLIC HEALTH will appoint a HIPAA Security Officer. The HIPAA Security Officer will orchestrate the department's risk management process.

AUDIENCE
Health Commissioner
HIPAA Security Officer

AUTHORITY
45 CFR 164.308(a)(1) Security management process and (a)(2) Assigned Security Responsibility

PROCEDURES
1) The Health Commissioner will appoint a HIPAA Security Officer. The job responsibilities for this individual are detailed in Appendix C: Sample Privacy & Security Officer Duties. The name of the person appointed shall be documented in the "Required Designations" as detailed in Policy 1380 HIPAA Assignments and Documentation. Any changes of personnel should be promptly documented.
2) The Canton City IT Department will be responsible for the security management process and keep the HIPAA Security Officer apprised of changes. This will include:
   A) **Security Team**. If the size of the department justifies, the HIPAA Security Officer may request that the Health Commissioner appoint a Security Team consisting of managers representing the different functional areas and facilities maintained by the department. The Information Security Office may also engage an outside consultant to assist with any or all of the functions of the Security Team. The Security Team's charter (whether it be a single individual or a group of individuals) is to assist the HIPAA Security Officer with the duties detailed in this policy.
   B) **Information System Inventory**. The Canton City IT Department shall maintain an inventory of the hardware, software and networking infrastructure. This will include servers, desktop computers, laptops, smartphones, tablets, USB flash drives, external disk drives, and any other computing equipment. A copy of this inventory shall be maintained off-site to ensure availability in the event of a fire or other disaster.
   C) **Computer Security Risk Analysis**. The Canton City IT Department will conduct the computer security risk analysis. The Risk Analysis is an accurate and thorough Analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the department. The Computer Security Risk Analysis will be handled as follows:
      i) The department will use the risk Analysis methodology detailed in NIST SP 800-30 (2001), or other methodology accepted in the industry.
      ii) The results of this Analysis shall be documented and maintained for 6 years
      iii) The Risk Analysis shall be presented to the Health Commissioner to whose responsibility will be to correct deficiencies identified and to make cost – security risk tradeoffs.
      iv) This Risk Analysis cycle shall be reviewed annually and updated as necessary. Updates to the risk analysis should be performed when new technologies are deployed (for example major software updates or new hardware) or when environment changes occur (for example if healthcare organizations are targeted by computer hackers, regulations change, or staff adopt new technologies such as Facebook).

D) **Manage IT Infrastructure, Create and Deploy Security Policies**. On an ongoing basis, implement and maintain the IT infrastructure, create Security Policies and Procedures, and deploy them. More specifically, he/she will
   i) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices
   ii) Prepare recommendations for the Health Commissioner for approval including implementation of new and updated policies, acquisition of technical security measures, or physical security measures. All new policies shall be approved by the Health Commissioner. The Health Commissioner shall have final authority on risk management decisions.
   iii) Update and maintain the HIPAA Security Policies as detailed in Policies 1380 HIPAA Assignments and Documentation and Policy 1350 Policy Updating and Staff Training.
   iv) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
   v) Train CANTON CITY PUBLIC HEALTH staff regarding compliance
   vi) Monitor CANTON CITY PUBLIC HEALTH compliance with the information security policies, and take action as appropriate based on this monitoring

REFERENCES

NIST SP 800-30, Risk Management Guide for Information Technology Systems, Revision 1, 2012
CERT at www.cert.org
SANS at www.sans.org
Center for Internet Security at www.cisecurity.org

2010 Data Backup Policy

POLICY
The Canton City IT Department will ensure that a robust data backup regimen is in place and operational at all times. The Canton City IT Department shall ensure that the procedures below are consistently maintained. This policy works in conjunction with the Information Technology Policy, 800-005-P.

AUDIENCE
Canton City IT Department

AUTHORITY
45 CFR 164.308(a)(7)(ii)(A) Data Backup Plan

PROCEDURES
1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality. Refer to Appendix G - Miscellaneous.
1) **Multiple Backup Generations**. Backups should include as many generations as is practical to store. One backup per day is appropriate.
2) **Backup Software**. Appropriate backup software shall be maintained, with appropriate scripting. These scripts shall be reviewed and adjusted as appropriate whenever hardware or software upgrades are performed to insure that appropriate data backup is maintained.
3) **Off-site storage**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include an off-site backup, that is, in a separate facility from the one containing the physical hardware.
4) **Backup Documentation**.
   A) A written description of the backup regimen must be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
   B) User documentation, for use by a system administrator, shall be maintained to allow for an alternate person to verify the daily operation of the backup.
5) **Responsibility**. The Fiscal Officer shall designate the employee with primary responsibility personally handle the backup if needed in-house. In the event that he/she is absent from work, an alternate individual shall be responsible. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
6) **Backup Log**. A log shall be maintained documenting the date, person, verification that backup was completed successfully, and any comments. Problems should be immediately reported to the Fiscal Officer, or if the Fiscal Officer is away from the office, to the Health Commissioner.
7) **Backup Media Security**. Backup media shall be encrypted and maintained in a secure location.
8) **Testing and Plan Revision.** Review and update of the data backup plan should be conducted with any significant update of the technical environment. Backup must be tested as detailed in POLICY 2020 DISASTER RECOVERY PLAN AND EMERGENCY MODE OPERATION.

2020 Disaster Recovery Plan and Emergency Mode Operation

POLICY
CANTON CITY PUBLIC HEALTH personnel shall develop contingency plans to prepare for system failures, and to prepare procedures for maintaining critical operations in the event of system failure. Refer to Continuity of Operations Plan (COOP).

AUDIENCE
Health Commissioner

AUTHORITY
45 CFR 164.308(a)(7) Contingency Plan

PROCEDURES
1) **Disaster Recovery Team**. If appropriate, the HIPAA Security Officer shall establish a Disaster Recovery Team to assist in the preparation of contingency plans as well as to execute assigned tasks in the event of a disaster. This team may include one or more outside consultants or software support vendors. The Health Commissioner shall direct this team and is responsible for all tasks identified in this policy.
2) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios should include, at a minimum, failure of one or more servers, data corruption of one or more subsystems, and catastrophic loss of the entire facility due to fire or other natural disaster.
3) **Preventative Measures**. The Health Commissioner shall, on an ongoing basis, evaluate the activities that are critical to CANTON CITY PUBLIC HEALTH operations and implement preventative measures to reduce the likelihood of system failure. These would include technical measures such as RAID technology, backup power supplies, fire suppression systems, database transaction logging and the like.
4) **System and Data Recovery Plan**. Refer to Appendix G – Miscellaneous. The Health Commissioner shall maintain a written system and data recovery plan, and take reasonable steps to mitigate losses, for likely failure scenarios. The written plan should include:
   A) Computer applications shall be reviewed and assessed as to their criticality for maintaining CANTON CITY PUBLIC HEALTH operations. The results of this assessment shall be documented.
   B) Development of written documentation of tasks and responsibilities for members of the Disaster Recovery Team in the event of various failure scenarios.
   C) System inventory, as specified in the Policy 2000 HIPAA Security Officer and Security Management Process to facilitate replacement of vital equipment in the event of a catastrophic loss
   D) Identification of, and contact information for, vendors who will be used for replacing equipment following a disaster.

   Reasonable steps to assure rapid recovery and mitigate losses can include, if appropriate:
   A) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by CANTON CITY PUBLIC HEALTH management
   B) Contracts with hot and/or cold system sites if deemed necessary and prudent by CANTON CITY PUBLIC HEALTH management
   C) Steps to manage risk, such as insurance policies, as deemed appropriate, for possible losses to mitigate the financial impact of disasters
5) **Emergency Mode Operations Plan**. Refer to Appendix G – Miscellaneous. The Health Commissioner shall maintain a plan to maintain vital operations in the event of a partial or complete system failure. This should begin with an identification of likely failure scenarios as described above. Elements of this plan may include:
   A) Identification of downtime scenarios, such as loss of electrical power, loss of internet connectivity, hardware failure or software malfunction.
   B) Maintenance of critical patient data in read-only format, updated regularly, on one or more workstations which are powered by battery backup and/or backup generator.
   C) Procedures which allow staff to function, to the extent possible, in the event of system downtime.
6) **Plan Testing**. The Health Commissioner shall be responsible for plan testing of both the data recovery plan and emergency mode operations plan. Results of the test shall design and maintained for one year.

7) **Off Site Storage of Key Documents**. A copy of the key documents described in this policy shall be maintained off site, in either paper or electronic form, so that they are readily and quickly assessable in the event of catastrophic loss of the facility.

REFERENCES

NIST SP 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems

2030 Facility Security and Access Control

POLICY
All employees shall be aware of facility security and access policies to ensure that only authorized personnel have physical access to the facility and its equipment.

AUDIENCE
Health Commissioner

AUTHORITY
45 CFR 164.310(a)(1) Facility Access Controls

PROCEDURES

1) The Health Commissioner shall create and maintain a facility security plan. This plan is kept in Appendix D - Facility Security and Safeguards for Oral and Written PHI.
2) The Health Commissioner shall review and update the plan as needed.

2040 Annual Security Evaluation

POLICY
Annually the HIPAA Security Officer shall assure that a technical and non-technical evaluation of CANTON CITY PUBLIC HEALTH's computer infrastructure for conformance with HIPAA Security Policies and Procedures.

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR 164.308(a)(8) Evaluation

PROCEDURES
1) **Annual Review of Regulations, Statutes, and Technological Issues to Update Security Policies.** On an annual basis, the HIPAA Security Officer will review any updates to federal HIPAA regulations, other applicable federal and/or state statues, and technological issues and update the organization's security policies as appropriate. This review may be conducted internally, or upon the HIPAA Security Officer's recommendation and approval by the Health Commissioner, contracted to an outside firm.
2) **Annual Evaluation.** On at least an annual basis, an evaluation of the technical infrastructure and/or the organizations compliance with computer security regulations will be conducted. From year to year, type of evaluation(s) may vary and will be selected by the Canton City IT Department. Appropriate evaluations may include
   A) Vulnerability scanning and remediation
   B) Firewall audits
   C) Penetration tests
   D) Social Engineering exercises/tests
   E) IT Asset audits to identify missing assets
   F) Audits of policies and procedures for compliance with the HIPAA regulations
   G) Audits of compliance with policies and procedures, including verification that the processes, procedures and documentation specified in the policies exist, and that the responsible personnel understand the policies
3) **Report and Recommendations**. When changes are made, the HIPAA Security Officer shall submit their report to the Health Commissioner with any recommendations. Documentation of results shall be retained for 6 years.

2050 Audit Control and Activity Review Policy

POLICY
System capabilities for maintaining audit trails of system use shall be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews should be conducted to identify inappropriate activity so that appropriate corrective action is possible.

AUDIENCE
Canton City IT Department

AUTHORITY
45 CFR 164.312(b) Audit Controls
45 CFR 164.308(a)(1)(ii)(D) Information System Activity Review
45 CFR 164.308(a)(5)(ii)(C) Log-in Monitoring

PROCEDURES
1) **System Activity Logs**. Activity logs shall be enabled at the following levels
   A) Operating Systems (Windows Server, Windows Workstations): Audit Policy should be set to log logon events, account management events, policy changes, and system events as detailed in vendor recommended best practices.
   B) Firewall Hardware and Software: Logs should be enabled to track inbound and outbound activity, including internet access.
   C) Application Software: All software which stores data on individuals served shall have audit trail capabilities. Logs should be enabled in application software such as clinical record software, billing software, or information systems which store PHI information regarding individuals being served.
2) **Security on Logs**. Appropriate security features and passwords should be used at all levels above to permit log file access only by the Fiscal Officer and/or an individual designated by him/her.
3) **Quarterly Audit of PHI Access**. A review of system activity will be conducted on at least a quarterly basis. The Fiscal Officer shall design an audit strategy to identify probable or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:
   A) Accesses to records of relatives of celebrities, celebrities' children or employees
4) **System Activity Review**. In a manner determined by the Canton City IT Department staff, he or she will monitor system activity to detect suspicious or unusual system activity, including:
   A) High number of log-in attempts
   B) Unauthorized changes to security settings
   C) Access by individuals at unusual hours
   D) Higher access/usage levels than normal
   E) Web sites viewed by employees to verify that they are work related
   F) Outside probe attempts and/or accesses via the internet connection
   G) Other unusual patterns of activity
5) **Corrective Action.** The HIPAA Security Officer in conjunction with the Health Commissioner will initiate corrective action, in conjunction with other members of the management staff, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
6) **Purge of Log files**. System log files which grow large may be purged under the direction of the Fiscal Officer.
7) **Annual Policy Review**. Annual attention should be given this policy regarding audit controls, as the threat level varies and the cost of monitoring tools changes.

2060 Malicious Software Protection Policy

POLICY
All company computer systems will be protected by virus and malicious software protection capabilities.

AUDIENCE
Canton City IT Department

AUTHORITY
45 CFR 164.308(a)(5)(ii)(B) Protection from malicious software

PROCEDURES
1) The Canton City IT Department will ensure that all computers in the facility are protected with reputable software for protection against malicious software.
2) Appropriate configuration options will be established in the software to protect against malicious software contained in:
   A) Incoming e-mail and e-mail attachments
   B) Files saved to any hard disk
   C) While browsing the internet
3) Necessary procedures will be implemented to enable centrally managed and/or automatic updates of the virus protection software. If the anti-virus software is not centrally managed, the Fiscal Officer shall periodically verify for each workstation that it is operable and updated.
4) Additional layers of security. As anti-virus software alone is not sufficient to provide complete protection against malicious software, additional layers of security shall be employed as detailed in Policy 2090 Technical Safeguards.

2070 Security Awareness Program

POLICY
CANTON CITY PUBLIC HEALTH will conduct an ongoing security awareness program to train and refresh staff on CANTON CITY PUBLIC HEALTH's security policies. Priority topics shall include recognizing and avoiding malicious software, avoiding "social engineering" ploys, using passwords effectively, and adhering to workstation use policies.

AUDIENCE
Fiscal Officer

AUTHORITY
45 CFR 164.308(a)(5)(i) Security awareness and training

PROCEDURES
1) The Fiscal Officer shall develop, and maintain, a security training program for new employees. This should include, at a minimum:
   A) Password policies
   B) Recognizing and avoiding malicious software
   C) Understanding e-mail attachments
   D) Safe web browsing practices
   E) Dangers of downloading files from the internet
   F) Understanding of "Social Engineering" and how to recognize such ploys
   G) Knowledge of Workstation Use Policies
   H) Consequences for non-compliance
   I) Security Incident Reporting Procedures

   Other appropriate topics may be included at the discretion of the Fiscal Officer. The program may be conducted one-on-one, via e-learning system, or other media as determined by the Fiscal Officer.
2) Upon initial implementation, the Security Training program will be provided to all staff. Subsequently, all new staff should receive the training.
3) At the discretion of the Fiscal Officer, periodic security awareness training may be offered to all employees. The Fiscal Officer shall develop a plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; evaluation and measurement techniques; and the frequency of training.

2080 Device and Media Disposal and Re-Use

POLICY
Electronic storage media and devices shall be cleaned of protected health information and other confidential information prior to disposal and/or re-use.

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR 164.310(d) Device and Media Controls

PROCEDURES
1) **Device Disposal/Reuse**. When disposing of computer equipment with PHI, or sending it for re-use or recycling, any data on the device should be removed. Computer equipment includes desktop or laptop PCs, tablets, smartphones, photocopy/imaging machines, medical equipment with memory capabilities, cameras, and any other device that stores PHI electronically. See "Technical Guidance" below for technical details for appropriate data removal techniques.
2) **Media Disposal Handled by HIPAA Security Officer**. As specified in Policy 3080 Computer Usage, CANTON CITY PUBLIC HEALTH employees are prohibited from storing Protected Health Information on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee should be instructed to give it to the HIPAA Security Officer for disposal when it is no longer needed.
3) **Technical Guidance**. In accordance with instructions from the Secretary of HHS, technical guidance regarding media disposal should be obtained from NIST SP 800-88 *Guidelines for Media Sanitization*. CANTON CITY PUBLIC HEALTH requires that at a minimum, data from electronic media should be "cleared", that is, protected against a robust keyboard attack but not necessarily against a laboratory attack.
4) **Media Disposal and Re-use**. Procedures vary based on type of storage media:
   A) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
   B) **Hard Drives and floppy disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
   C) **Other Media**. See NIST SP 800-88 for disposal/recycling methods for other media.
5) **Records.** At the discretion of the HIPAA Security Officer, records of data destruction may be maintained. A certificate of destruction shall be obtained from any vendor handling data destruction. If records are maintained, the following guidelines are suggested:
   A) Item Description
   B) Make/Model
   C) Serial number(s) / Property Number(s)
   D) Backup Made of Information (Yes/No)
   E) If Yes, location of backup
   F) Item Disposition (Clear/Purge/Destroy)
      i) Date Conducted:
      ii) Conducted by
      iii) Phone #
      iv) Validated By
      v) Phone #
   G) Sanitization Method used
   H) Final disposition of media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer /Other)

2090 Technical Safeguards

POLICY
Technical Safeguards will be employed as necessary to maintain the integrity of data, and to ensure the security of data during transmission.

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR 164.312(c) , (d) and (e) Integrity, authentication and transmission security

PROCEDURES
1) **Firewalls.** Hardware and/or software firewalls shall be employed to protect against network intrusions. These should be configured to enforce CANTON CITY PUBLIC HEALTH policies, such as blocking of internet e-mail sites, and other safeguards.
2) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   A) The beacon shall be enabled
   B) The SSID should be changed from the default
   C) WPA2 should be enabled
   D) These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
   E) A strong password (8 or more characters including 1 upper case, 1 lower case and 1 digit) shall be used.
   F) If guests are provided access to wireless networks to provide internet access, this access should be configured to prevent access to the internal company network
3) **Software Patching**. Hypervisor, operating system, and application software shall be patched on a timely basis:
   A) Workstations. Workstations should be monitored regularly so that installed software is patched when determined to be appropriate by the Canton City IT Department.
   B) Servers. Software on servers shall be patched after appropriate testing by the department's electronic patient record/billing software vendor.
   C) Hypervisors. If virtualization is used, the hypervisor shall be kept patched.
4) **Secure Configuration.** Operating System, Application Software and other hardware/software shall be securely configured.
   A) Default administrator passwords shall be removed, and new administrator accounts shall be protected with strong passwords.
   B) Unnecessary services should be disabled.
   C) Logging should be enabled per best practices.
   D) For Microsoft software, Microsoft's secure configuration guidelines should be used.
5) **Virtualization Software and environment**. If virtualization is employed, the virtualization-enabling software, aka "hypervisors", shall be secured as follows:
   A) unneeded capabilities shall be disabled to reduce potential attack vectors
   B) A strong password (minimum of 8 characters, 1 upper case, 1 lower case, 1 digit) shall be used for the management console
   C) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's
   D) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations
   E) Use separate logon credentials for each virtual server
6) **E-mail**. For transmission of PHI, secure e-mail should be employed if PHI is to be included in any email. A reputable secure email vendor shall be utilized. The E-mail system should be configured, if possible, to automatically detect and encrypt messages containing PHI. See also Policy 3080 Computer Usage.
7) **Encryption of desktop, mobile devices and portable media**. When encryption of end-user devices is determined appropriate based on risk analysis, CANTON CITY PUBLIC HEALTH shall employ the

framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically,

A) CANTON CITY PUBLIC HEALTH should consider solutions that use existing system features (such as operating system features) and
B) infrastructure should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments
C) should select appropriate user authenticators for storage encryption solutions
D) should implement measures that support and complement storage encryption implementations for end user devices

8) **Transmission Security**. For data in motion, the HIPAA Security Officer implement solutions consistent with the Secretary of HHS's guidance on securing PHI. Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described
   A) NIST 800-77, *Guide to IPsec VPNs*,
   B) NIST 800-113, *Guide to SSL VPNs*
   C) Other FIPS 140-2 Security Requirements for Cryptographic Modules
9) **Appropriate Audit Controls in CANTON CITY PUBLIC HEALTH-Used Software**. Software with PHI used by CANTON CITY PUBLIC HEALTH should be evaluated for the appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements should be made as appropriate. Appropriate audit controls should be a criteria for continued use of and/or procurement of any new operating or application software.
10) **Automatic Log Off**. Appropriate measures shall be taken, based on the technology available, to enable the automatic log-off provisions as determined by the risk assessment. See also Policy 3080 Computer Usage .
11) **Integrity Checks**. The HIPAA Security Officer should run integrity checks on database applications periodically.

2100 Breach Reporting

POLICY
The department will notify patients, the Secretary of HHS and, when appropriate, the news media regarding breaches of protected health information.

AUDIENCE
HIPAA Security Officer

AUTHORITY
45 CFR Part 164, Subpart D HIPAA Breach Notification Rule

PROCEDURES
1) Upon becoming aware of a privacy rule violation or security incident, the HIPAA Security Officer and HIPAA Privacy Officer shall jointly determine if the incident meets the definition of a breach. If a Security Incident Response Team (Team) has not been assembled, they may assemble a Team at this point. Legal counsel and other outside expert advice shall be obtained, if appropriate, for additional guidance on the Team. An investigation should be launched, with attention to preserving evidence. The Team shall follow the following 3 step procedure:
   A) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
   B) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
   C) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
      i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      iii) Whether the protected health information was actually acquired or viewed; and
      iv) The extent to which the risk to the protected health information has been mitigated.

      The results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 1380 HIPAA Assignments and Documentation. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred and this process may stop. Otherwise, a breach has occurred and the Team should proceed with the steps that follow in the remainder of this policy.
2) **Public Relations Strategy**. The Team should develop a public relations strategy to include when and who should speak to the media and what should be said.
3) **Breach Notification**. In the event of a breach, the Team shall:
   A) Notify Individuals affected by the breach without unreasonable delay (and in no case later than 60 calendar days after the discovery of the breach):
      i) In the event of an urgent situation, the board may use telephone, email or other means to immediately notify individuals of the breach.
      ii) Prepare formal written notification for approval by superintendent. The notification shall be written in plain language and include the following:
         1) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
         2) A description of the types of unsecured protected health information that were involved in the breach;
         3) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
         4) A brief description of what the board is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

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

iii) Send the primary breach notification to:
1) Individuals affected by the breach by first-class mail at their last known address, or by e-mail if agreed in advance by the individual for this type of notice, or
2) Parent, guardian, or HIPAA Personal Representative of the Individual in the event the individual is a minor and/or not competent to make decisions, or
3) Next of kin or personal representative of the Individual in the event that the individual is deceased and the next of kin name and address are available.

iv) Track returned mail and provide a substitute notice to Individuals who did not receive the primary notification (no further effort is necessary for unreachable next-of kin):
1) In the event that fewer than 10 individuals, the HIPAA Security Officer shall research updated address and/or phone number and make best efforts to inform those individuals by either phone or mail.
2) In the event that 10 or more individuals are not reachable by first class mail,
a) A toll-free phone number shall be established, and staffed with operators, for at least 90 days
b) a notice shall be conspicuously placed on the board's web site home page with details of the above details on the breach plus the phone number

B) Notify the news media if more 500 Individual records are involved in the breach
i) Under direction of the board superintendent, a press release shall be prepared detailing the information in section 2Ab above, and other relevant information.
ii) Upon approval of the board superintendent, the press release shall be issued without unreasonable delay (and in no case later than 60 days after discovery of the breach) to the major print, broadcast and online media serving the county.

C) Notify the Secretary of the Department of HHS regarding the breach
i) In the event that the breach involves 500 or more individuals, notice to the Secretary should be provided at the same time as the Individual notification in the manner detailed on the HHS Web site.
ii) For breaches involving fewer than 500 individuals, a log including at a minimum the information in 2Ab above, and other relevant information, should be maintained. At the end of the calendar year, the contents of the annual log should be provided to the secretary in the manner detailed on the HHS Web site.

2) **Breaches by Business Associates**. Breaches by business associates are handled in the same manner. Business associates are obligated to cooperate in providing necessary information; the board is responsible for issuing the notice detailed in this policy.

3) **Law Enforcement Delay**. The notices to Individuals and the media may be delayed if a request is received by a law enforcement official:
A) If written notice is received from a law enforcement official which specifies the time period of delay, the board shall comply with that request.
B) If the request is made orally, the notification shall be delayed but not longer than 30 days from the date of the oral request.

4) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that the board should have become aware if it exercised reasonable diligence. Breaches shall also be recorded in the Disclosure Log to facilitate compliance with the Accounting for Disclosures requirements.

SECURITY POLICIES FOR OFFICE MANAGER & SUPERVISORS

3010 Employee System Access and Termination Procedures

POLICY

System access will be granted to employees in a manner consistent with the HIPAA Privacy laws and other state regulations, including specific policies for access control, granting access to new staff and staff with assignment changes, handling staff terminations, password selection, maintenance and use, and access to the system in the event of an emergency. This policy is to be used in conjunction with the IT policy, 800-005-P.

AUDIENCE

Health Commissioner, Office Manager, Supervisors, HIPAA Security Officer

AUTHORITY

164.308(a)(3) & (a)(4) Workforce Security and Information Access Management
164.312(a) Access Control, Unique User identification, Emergency access procedure, and Automatic logoff
164.308(a)(5) Password Management

PROCEDURES

AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS

Audience: HIPAA Privacy and Security Officer

1) The HIPAA Security Officer shall coordinate with the Privacy Officer to maintain and document a current "minimum necessary" analysis, per the Policy 1020 Minimum Necessary Policy which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to. These should be maintained in Appendix E - Workforce Access to PHI and Safeguards.
2) The HIPAA Security Officer shall utilize the security capabilities of the various network and application software systems at the department and develop role-based "Access Profiles" for these different job descriptions. Vendors will be contacted for any enhancements necessary for appropriate implementation of these access profiles.
3) The authority to grant access to information systems rests with Health Commissioner and is delegated to the HIPAA Security Manager. Implicit in a hiring decision is the provision of access to the information systems necessary for the job, as determined above based on the minimum necessary analysis and the Access Profiles.
4) In certain situations, such as when employees are assigned special projects, information access may be required beyond what the job description would dictate. In these cases, the HIPAA Security Officer, after any necessary consultation with the management staff at the CANTON CITY PUBLIC HEALTH, shall have the authority to grant access to information systems which go beyond the standard Access Profiles described above. Access should be terminated when the need for access is completed.
5) The HIPAA Security Officer shall maintain an updated, inventory of employees with access to PHI and the access rights which are granted.
6) At the discretion of the HIPAA Security Officer, he or she may annually audit the access controls to verify that the above policies have been implemented properly and consistently. Such an audit could include verification that recently terminated employees no longer have access, a review of access for employees with job changes in the previous year, and a random sampling of other employee access authorization.

SYSTEM AND FACILITY ACCESS FOR NEW HIRES

Audience: Supervisors, Office Manager

1) Supervisors and/or the Office Manager shall direct requests for access to PHI information systems to the HIPAA Security Officer or his/her designee. The HIPAA Security Officer shall verify with the Office Manager in the event of any question regarding the accuracy of the job assignment.
2) The Fiscal Officer shall issue any necessary office keys to the new hire and maintain records of the keys issued.
3) The Canton City IT Department or appropriate department staff person will assign new hires requiring computer access a unique network User ID and password, and/or User IDs and passwords for other application

systems. Security settings appropriate for the individual will be assigned in accordance with this policy, as described above.

4) The Canton City IT Department or appropriate department staff person shall communicate the User IDs and passwords in a manner which does not compromise security by revealing the passwords to another person.
5) As described above, the Fiscal Officer or appropriate department staff person will maintain documentation of system access rights.
6) The IT Department will configure a User Data Area on the Server to provide data storage space for the employee. All data is to be stored on the server and not on individual workstations.
7) Automatic Logoff. The IT Department shall configure user accounts with access to PHI to automatically logoff after 20 minutes of inactivity, unless a different determination is made in the Risk Analysis.
8) Employees will receive Security Awareness Training, in the manner chosen by the HIPAA Security Officer, in accordance with the Policy 2070 Security Awareness Program. In addition, new employees should receive a written or electronic copy of these HIPAA Privacy and Security Policies, and they will sign written acknowledgement (form #800-016-03-F) that they understand and will adhere to all policies. This will be maintained in the employee personnel file.

PASSWORD MANAGEMENT

Audience: IT Department

1) Passwords shall be set as stated in the IT Policy, 800-005-P.
2) The IT Department shall implement a mechanism to ensure that all employees change their passwords at least every 6 months.
3) The IT Department shall not maintain a list of user passwords but should use the "Administrator" account on the workstation to perform maintenance activities.
   A) In cases where IT personnel might need to be logged in to a user's account for maintenance they should request that user to log them in to the account without providing the password. If this is not possible, the password can be temporarily changed by logging in to the administrator account and using the administrative tools. The IT department would then be responsible for the security of the User ID until the user is provided the opportunity to change the temporary password.

EMPLOYEE JOB CHANGES

Audience: Supervisors, Fiscal Officer

1) The Supervisors shall notify the Fiscal Officer of all job changes so that adjustments to system access can be made if necessary.

EMPLOYEE TERMINATION

Audience: Supervisors, Human Resource Department, HIPAA Security Officer

1) On the last day of employment, employee passwords to the network and Application Software will be changed and/or their User IDs will be disabled. The individual's keys to the facility should be returned.
2) The Fiscal Officer shall document the disabling of system access.
3) For involuntary terminations or certain administrative leave situations, in the event that any manager believes there is the potential for any retaliatory behavior, that manager should notify the HIPAA Security Officer who shall take appropriate precautions to ensure the integrity and security of confidential CANTON CITY PUBLIC HEALTH information. This could include such measures as:
   A) Physically escorting the individual off the premises after notifying him/her of the termination
   B) Disabling system access as specified above on a timely basis
   C) Requiring all staff in the individual's workgroup to change passwords
   D) Other measures as deemed appropriate by the Information Security Manager based on the technical sophistication of the individual and perceived threat.

EMERGENCY SYSTEM ACCESS

Audience: Supervisors, HIPAA Security Officer

In the event of an emergency, such as a life-threatening situation in which immediate access to PHI is required, a staff member who does not have appropriate system permission but requires access shall contact the HIPAA Security Officer (or another staff person in that department) who will provide the necessary access on an expedited basis.

HIPAA ADMINISTRATIVE REQUIREMENTS SECURITY POLICIES FOR ALL STAFF

3080 Computer Usage

POLICY
Each staff member is responsible for understanding and following the policies regarding workstation use and security.

AUDIENCE
All Staff

AUTHORITY
164.310(b) Workstation Use and (c) Workstation Security
164.308(a)(5) Log in Monitoring

PROCEDURES

WORKSTATION USE

1) **System is for Job Duties**. Computer workstations, including use of internal systems, e-mail and the internet, are for use by employees to conduct their job responsibilities.

2) **Internet Use**. Employees should exercise good judgement when using the internet in order to maintain a secure system and network.

   A) Employees are prohibited from both downloading and installing executable programs without the express permission of the Fiscal Officer or designee (see pre-approved list of programs in the IT Policy, 800-005-01-A). Employees must not download, view text or images, or otherwise engage in communications which involve pornographic or racist materials; obscene material, derogatory, inflammatory or profane material; any other objectionable material. Copyrighted materials such as software or music files must not be downloaded in violation of copyright law.

      a) The Fiscal Office and HIPAA Security Officer shall establish guidelines to assist Directors/Administrators in recognizing executable programs that might jeopardize the system or network security

3) **E-Mail Use**. Employees with CANTON CITY PUBLIC HEALTH e-mail accounts should check e-mail daily. E-mail is to be used for CANTON CITY PUBLIC HEALTH purposes only. E-mail should be written in professional manner and should be courteous and respectful. Other policies when using e-mail:

   A) Standard e-mail is not a secure method of delivery. Use of email to transmit any PHI is prohibited except in the limited case specified in the HIPAA regulations and outlined in Policy 1200 Patient's Right of Access to Records, when a patient requests that an electronic copy of their record be sent via email.

   B) Use only CANTON CITY PUBLIC HEALTH-supplied e-mail account. The use of internet-based e-mail accounts such as Yahoo mail is prohibited.

4) **Social Media and Instant Messaging**. Social Media use shall be compliant with Policy 3082 Use of Social Media. Instant Messaging software shall not be used on CANTON CITY PUBLIC HEALTH workstations.

5) **Personal Use of System Must be Limited**. Use of Health District computers for any personal use that interferes with the public mission of the District is prohibited. In particular, any video and/or audio streaming for personal use is expressly prohibited.

6) **Storage of PHI or Confidential material to Removable Media Prohibited**. Personnel may not copy to removable media, or transmit via e-mail or fax or other method, any CANTON CITY PUBLIC HEALTH confidential information or Protected Health Information on CANTON CITY PUBLIC HEALTH computer

system, except when specifically authorized by the HIPAA Security Officer for CANTON CITY PUBLIC HEALTH purposes.

7) **All Usage is Logged**. CANTON CITY PUBLIC HEALTH RESERVES THE RIGHT TO MONITOR ALL USAGE OF CANTON CITY PUBLIC HEALTH WORKSTATIONS, THROUGH THE LOGGING AND STORAGE OF ALL ACTIVITY, INCLUDING ALL E-MAILS SENT OR RECEIVED, WEB SITES BROWSED, AND OTHER ACTIVITY. All logs of employee activity are property of CANTON CITY PUBLIC HEALTH. Employees will be held accountable for all computer usage performed using their User ID.

8) **Data Storage on Server Only**. Except with permission from the Fiscal Officer, all data must be stored on the server. Employees must use proper procedures to store word processing files, spreadsheets, financial programs, and other data files in the appropriate location on the server. Any staff unfamiliar with the proper procedure should contact the HIPAA Security Officer for instructions on how to access their User Directory on the server. NO DATA ON WORKSTATIONS IS BACKED UP!

WORKSTATION SECURITY

1) Except with specific approval of the HIPAA Security Officer, workstations must not be setup in a public access area.
2) All employees should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.
3) Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.
4) Workstations should be configured with automatic logoff capability so that they will become inaccessible after 20 minutes of system inactivity, or as determined by the HIPAA Security Officer.
5) Employees must not install any software on their computer except in accordance with the policy outlined under "3080, Workstation Use, 2) Internet Use".
6) All CANTON CITY PUBLIC HEALTH servers must be secured with a strong password (see "User IDs and Passwords" below) and setup to automatically lock out user access after a maximum of fifteen minutes of inactivity or at a shorter time interval as determined by the individual departments.

USER IDs and PASSWORDS

1) Each employee is assigned a unique User ID and Password. Employees will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential.
2) Passwords (see "3010, PASSWORD MANAGEMENT 1"). The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed.
3) In general, passwords should be memorized and not written, especially not in the vicinity of a workstation.
4) Users are required to change all passwords at least every 6 months.
5) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

EMERGENCY SYSTEM ACCESS

1) In the event of an emergency where immediate access to system information is required but not immediately possible, employees should contact the HIPAA Security Officer, who has contingency plans to allow access to vital data in a wide variety of scenarios (system down, patient emergencies which mandate system access by personnel who otherwise are not permitted access.)

3082 Use of Social Media

POLICY

When using department computers, Social Media sites, including Facebook, LinkedIn and others, are to be used only in conformance with this policy. This policy also addresses requirements for use of social media from outside the department.

AUDIENCE

All Staff

PROCEDURES

1) **CANTON CITY PUBLIC HEALTH Sponsored Use**. The HIPAA Privacy officer or Health Commissioner may approve the establishment of a CANTON CITY PUBLIC HEALTH sponsored Company Page or Social Media Site.
2) **Personal use of Facebook and other social network sites by employees**.
   A) Employee Personal use of Facebook.
      i) **Employee Use during Work Hours**. During work hours, employees are expected to focus on work-related activities. Consequently, in general, they are expected to keep Facebook and other social network sites closed so they do not lose productivity unless related to his/her work (i.e., Public Information Office, Disease Intervention Specialist)
      ii) **Employee Use at any time**. Facebook and other social network sites is a new communication medium. The medium is semi-public; while it includes many options for specifying levels of privacy, Facebook users often share private information in unintended ways. Consequently, any use of Facebook has the potential to become a public communication, so, employees of CANTON CITY PUBLIC HEALTH must follow the following guidelines:
         1) **Sharing of work-related activities**. Employees should limit the sharing of any CANTON CITY PUBLIC HEALTH related information to information that they would be acceptable to be made public, for example, on the front page of a major newspaper.
            a) Examples of information that would be appropriate to share on one's wall include:
               i) The employee's excitement and satisfaction with the work and mission of CANTON CITY PUBLIC HEALTH,
               ii) Details of an upcoming public event sponsored by CANTON CITY PUBLIC HEALTH, such as a local "Health Fair" day,
               iii) The name of a friend who is a co-worker at CANTON CITY PUBLIC HEALTH
            b) Examples of information that would be inappropriate to share on one's wall include:
               i) The name of a patient of CANTON CITY PUBLIC HEALTH
               ii) A complaint about CANTON CITY PUBLIC HEALTH such as displeasure with a supervisor or co-worker
               iii) Any Protected Health Information, or PHI, (which includes facial images of Patients)
            c) Employees shall not be prohibited from any communication that is protected and regulated by the National Labor Relations Board.

            Employees are further encouraged but not required to limit communications on Facebook to those that would portray them in a professional manner.
         2) **Friending**. It is management's judgment that employees must not "friend" any patient being served by CANTON CITY PUBLIC HEALTH, or the parent/guardian of a Patient being served. CANTON CITY PUBLIC HEALTH expects employees to maintain an acceptable professional boundary with patients.
            a) In cases where a relationship existed prior to the patient relationship, this recommendation may not apply. For example, if a Nursing Division employee were to administer a flu vaccine to a coworker's minor child that Nursing Division employee would not be expected to "unfriend" their coworker.
            b) In cases where the employee does not work in the division providing the services, this recommendation may not apply. For example, if an Air Pollution Control (APC) Division employee becomes "friends" with a person they have a relationship with outside of

work, whom happens to also receive services by the Nursing Division employees, unbeknownst to the APC Division employee.

3) **Messaging**. Employees must not use Facebook messaging for CANTON CITY PUBLIC HEALTH communications, especially if they involve PHI. This is prohibited since the department does not have a Business Associate agreement with Facebook.

3085 Portable Computing Devices and Home Computer Use

POLICY
Special procedures must be followed for employees who use portable computing devices, including laptop computers, smartphones and tablets for CANTON CITY PUBLIC HEALTH purposes, including devices that are owned by the employee. In addition, special measures must be utilized for any work at home arrangements involving the employee's home computer.

AUDIENCE
All Staff

AUTHORITY
164.312(a)(2)(iv) Encryption and decryption

PROCEDURES
1) **Remote Access to CANTON CITY PUBLIC HEALTH Systems via mobile devices**. When using a mobile device (laptop computer, smartphone, or tablet) to access CANTON CITY PUBLIC HEALTH systems, a VPN connection must be used. Any employee who is unfamiliar with this technology must contact the designated IT contact for instructions.
2) **Encryption on Laptops and other mobile devices**. Employees who use CANTON CITY PUBLIC HEALTH provided laptop computers, smartphones, or other portable computing devices containing PHI must use the encryption features to reduce the impact of disclosure in the event that the device is lost or stolen.
3) **Text Messaging Prohibitions**. SMS Text messaging may not be used for any communications involving PHI. See the HIPAA Security Officer for a secure messaging capability if this is required.
4) **Lost devices**. Employees must immediately report lost or stolen devices to their supervisor and the HIPAA Security Officer in accordance with the Security Incident procedure.
5) **Employee-owned portable computing devices, (BYOD)**. Employees may use their personal smartphones or other portable devices for the purposes of CANTON CITY PUBLIC HEALTH activities including email access. Employees are expressly prohibited from storing any PHI on a personally-owned device. Loss of a smartphone containing PHI is a security incident and should be reported per Policy 3090 Security Incident Response and Reporting.
6) **Work at home and use of employee's home computer.** Employees working at home and using their home computers for work purposes are prohibited from storing PHI on their home computers. Employees must obtain permission from the HIPAA Security Officer prior to accessing EHR software from any device not owned by the Health District.
7) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required while using these devices.

3090 Security Incident Response and Reporting

POLICY
CANTON CITY PUBLIC HEALTH will monitor all electronic information systems with PHI access for breaches of security, mitigate harmful effects of security incidents to the extent practicable, investigate any deficiencies identified and correct them, and document any such security incidents and their outcomes.

AUDIENCE
All Staff

AUTHORITY
45 CFR 164.308(a)(6) Security incident procedures

PROCEDURES
Creation of Response Team and Contingency Planning

1) The HIPAA Security Officer is responsible for managing security incident response and reporting. As part of a pro-active management process, he or she may recommend to the Health Commissioner assignment of individuals for an incident response team. The mandate to this group would be to coordinate CANTON CITY PUBLIC HEALTH's response to security incidents. This would include mitigation strategy, communications with law enforcement, CANTON CITY PUBLIC HEALTH's patients and the media. The incident response team may meet on a periodic basis to develop contingency plans, such as identification of security consultants who can be contacted in the event of a problem.

Security Incident Reporting and Response Procedure

1) Any employee who becomes aware of a security incident must immediately contact the HIPAA Security Officer to report the incident.
2) The HIPAA Security Officer and/or Incident Response Team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. See Policy 1300 Mitigation.
3) In conjunction with the HIPAA Security Officer, a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include
   A) Date and time of report
   B) Date and time of incident
   C) Description of circumstances
   D) Corrective action taken
   E) Mitigating action taken

   Documentation will be kept for 6 years.
4) The HIPAA Security Officer and/or Incident Response Team will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response, and recommend to management any changes they believe appropriate.

APPENDICES

Appendix A - Identifying Business Associates

Identifying your Business Associates

HIPAA-Covered Entities are obligated to identify and place any "Business Associate" under a contract that meets the specifications of the HIPAA regulations. Further, these Business Associates, as of January 25, 2013, are directly regulated by the HIPAA regulations and for the first time are subject to the same civil and criminal penalties for any failures to comply with the portions of the HIPAA regulations that apply to them.

An abbreviated definition of "Business Associate" is a person or entity, other than a member of the workforce that performs certain functions, activities or provides services that involve the use or disclosure of PHI on behalf of the department.

More specifically, the functions and activities that create a Business Associate relationship are:

- claims processing or administration,
- data analysis, processing or administration,
- utilization review,
- quality assurance,
- patient safety activities listed at 42 CFR 3.20,
- billing,
- benefit management,
- practice management,
- repricing,
- legal,
- actuarial,
- accounting,
- consulting,
- data aggregation,
- management,
- administrative,
- accreditation or
- financial services.

Subcontractors of Business Associates are Business Associates. A significant change in the January 25, 2013 HIPAA Rule changes is that subcontractors of your business associates, who have access to PHI, are now Business Associates. For example, suppose you contract with a billing service. The billing service subcontracts with computer support vendor to provide its billing system and software support. The computer support vendor is a Business Associate. However, it is billing service's responsibility, not yours, to place the computer support vendor under the Business Associate contract.

1) Examples of Business Associate Relationships.
   A) A health care clearinghouse
   B) A computer contractor that provides support for the department software and/or its computer network and has access to PHI as part of its support and service capacity
   C) An answering service
   D) A collection agency
   E) A billing service
   F) A CPA firm whose accounting services to CANTON CITY PUBLIC HEALTH involves access to protected health information, such as a review of your accounts payable ledger which includes patient names on the patient refund checks.

G) An attorney whose legal services to CANTON CITY PUBLIC HEALTH involve access to protected health information, such as malpractice defense
H) A consultant that performs utilization reviews, compliance audits or billing support for CANTON CITY PUBLIC HEALTH.

2) Examples of relationships which are not Business Associates
A) Other healthcare providers including hospitals, other physicians, home health agencies, labs, etc.
B) A physician or a nurse who is an independent contractor working at the department
C) Cleaning services
D) Contractors who provide services not relating to any of the above, such as electricians, plumbers, telephone installation personnel and carpenters

Note that while these entities are not Business Associates, it may be appropriate to include a confidentiality clause in any contract, such as in a contract with another physician who treats patients at your facility.

Full Definition of Business Associate from the HIPAA Rules (1/25/2013 Revision):

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:
(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and re-pricing; or
(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
(2) A covered entity may be a business associate of another covered entity.
(3) Business associate includes:
(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.
(4) Business associate does not include:
(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.
(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Appendix B: Sample HIPAA Business Associate Agreement

Health Districts are obligated to place Business Associates under a contract that meets detailed specifications that were updated on 1/25/2013. Below is a contract that meets these specifications. Note that it must be customized in Appendix A with a brief clause which defines the "allowed uses and disclosures". Several example clauses are included.

Any new contracts must comply with the new specifications.

Limited Grandfathering of Existing Contracts. BA Contracts compliant with earlier specifications that existed prior to 1/25/2013 and were renewed no later than 3/26/2013 will be deemed compliant until 9/22/2014. However, if the agreement is renewed on or after 9/23/2013, it must be updated to the new specifications.

HIPAA BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE Agreement ("Agreement") is entered into by and between _____ ("BUSINESS ASSOCIATE") and _____ (the "COVERED ENTITY").

RECITALS

1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 164. This agreement is written to comply with the revisions enacted in the HITECH statute in February 2009, the regulation changes published in August 2009 and further updates published January 25, 2013.
2) Terms used in this agreement, including but not limited to "covered entity", "business associate", "Protected Health Information (PHI)", "unsecured protected health information", "use", "disclose", "breach", and "security incident", shall have the same meaning as defined in most current versions of the above referenced regulations.
3) COVERED ENTITY is a covered entity and regulated by the HIPAA regulations.
4) Per the January 25, 2013 HIPAA Regulation changes, BUSINESS ASSOCIATE is also regulated by the HIPAA regulations, and further agrees to comply with the unique requirements of this agreement.

NOW, THEREFORE, in consideration of the foregoing, the parties agree as follows:

1) **Allowed Uses and Disclosures of Protected Health Information**. The BUSINESS ASSOCIATE provides services for the COVERED ENTITY. The BUSINESS ASSOCIATE may use and disclose protected health information only as follows:
   A) BUSINESS ASSOCIATE may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, BUSINESS ASSOCIATE may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.
   B) BUSINESS ASSOCIATE may further use and disclose PHI, if necessary:
      i) for the proper management and administration of the BUSINESS ASSOCIATE's business, and/or
      ii) to carry out the legal responsibilities of the BUSINESS ASSOCIATE if the disclosure is either
         a) required by law, or

b) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.

2) **Responsibilities of BUSINESS ASSOCIATE**. With regard to its use and disclosure of protected health information, BUSINESS ASSOCIATE agrees to do the following:

A) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.

B) Use appropriate physical, technical and administrative safeguards to protect electronic PHI, and comply with the requirements of the HIPAA Security Regulations (45 CFR Part 164 Subpart C) which are applicable to business associates.

C) Report to the COVERED ENTITY any security incident, and any use or disclosure not provided by this contract, including breaches of unsecured protected health information as required by 45 CFR 164.410.

D) Require that subcontractors who create, receive, maintain or transmit ePHI on behalf of Business Associate comply with applicable HIPAA Security regulations by entering into a Business Associate contract with these subcontractors. The Business Associate contract shall meet the specifications of 45 CFR 164.314.

E) Make available to the individual any requested protected health information, in accordance with procedures specified by COVERED ENTITY and in compliance with 45 CFR 164.524, "Access of individuals to protected health information".

F) Make available for amendment, and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR 164.526, "Amendment of protected health information".

G) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528.

H) To the extent that BUSINESS ASSOCIATE is to carry out COVERED ENTITY's obligations under the HIPAA Privacy Regulations, 45 CFR 164 Part E, comply with the requirements of the Privacy Regulations in the performance of those obligations.

I) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the COVERED ENTITY's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

J) Return to the COVERED ENTITY or destroy, as requested by the COVERED ENTITY, within 30 days of the termination of this Agreement, the protected health information in BUSINESS ASSOCIATE's possession and retain no copies or electronic back-up copies. If this is not feasible, BUSINESS ASSOCIATE will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.

3) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

4) **Term and Termination**.

A) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

B) Termination. As provided for under 45 C.F.R. §164.504, the COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that the BUSINESS ASSOCIATE has breached a material provision of this Agreement. Alternatively, the COVERED ENTITY may choose to: (i) provide the BUSINESS ASSOCIATE with 30 days written notice of the existence of an alleged material breach; and (ii) afford the BUSINESS ASSOCIATE an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

5) **Survival**. The respective rights and obligations of BUSINESS ASSOCIATE and COVERED ENTITY under the provisions of Sections 2(j), detailing BUSINESS ASSOCIATE's return and/or ongoing protections of protected health information, shall survive the termination of this Agreement.

6) **Amendment**. This Agreement supersedes any previously negotiated HIPAA Business Associate agreements. Further, it may be modified or amended only in writing as agreed to by each party.

7) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to BUSINESS ASSOCIATE _____
_____
_____
_____

If to COVERED ENTITY: _____
_____
_____
_____

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of _____.

BUSINESS ASSOCIATE

By:_____
Name: _____
Title: _____
Date:_____

COVERED ENTITY

By:_____
Name:_____
Title:_____
Date:_____

Attachment A – Permitted Uses and Disclosures

BUSINESS ASSOCIATE is authorized to use protected health information for the purposes of

[INSERT A CLAUSE THAT DESCRIBES BUSINESS ASSOCIATE's ALLOWED USES AND DISCLOSURES. THIS WILL VARY DEPENDING ON THE NATURE OF THE RELATIONSHIP. THE FOLLOWING IS AN EXAMPLE OF A CLAUSE FOR A BILLING SERVICE.]

Example Clauses:
Billing Service: Business Associate is authorized to use and disclose protected health information for the purposes of providing billing services and other activities detailed in the contract dated mm/dd/yy.

Computer Software Vendor: Business Associate is authorized to use and disclose protected health information for the purposes of providing software training, support and troubleshooting.

Computer Network Support Consultant: Business Associate is authorized to use and disclose protected health information for the purposes of providing computer network support services.

Appendix C: Sample Privacy & Security Officer Duties

HIPAA Privacy Officer Job Description

REPORTS TO: Health Commissioner

General Purpose:
The privacy officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to CANTON CITY PUBLIC HEALTH's policies and procedures covering the privacy of, and access to, patient health information in compliance with federal and state laws and CANTON CITY PUBLIC HEALTH's information privacy practices.

Responsibilities:

- Provides development guidance and assists in the identification, implementation, and maintenance of CANTON CITY PUBLIC HEALTH information privacy policies and procedures in coordination with CANTON CITY PUBLIC HEALTH management and administration, the HIPAA Committee, and legal counsel.
- Serves in a leadership role for all HIPAA activities.
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Works with legal counsel and the HIPAA committee to ensure CANTON CITY PUBLIC HEALTH has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current CANTON CITY PUBLIC HEALTH and legal practices and requirements.
- Oversees, directs, delivers, or ensures delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
- Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Assists HIPAA Security Officer with handling of any security incidents and/or security rule violations.
- Works cooperatively with the applicable CANTON CITY PUBLIC HEALTH units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate.
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning CANTON CITY PUBLIC HEALTH's privacy policies and procedures and, when necessary, legal counsel.
- Assists HIPAA Security officer by reviewing all system-related information security plans throughout CANTON CITY PUBLIC HEALTH's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Maintains current knowledge of federal privacy laws, specifically HIPAA, as well as state privacy laws, accreditation standards, and monitors advancements in information privacy technologies to ensure CANTON CITY PUBLIC HEALTH adaptation and compliance.
- Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.
- Works with CANTON CITY PUBLIC HEALTH administration, legal counsel, and other related parties to represent CANTON CITY PUBLIC HEALTH's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.
- Seeks outside help as necessary when not qualified to perform any of the duties above

Qualifications of Privacy Officer:

- Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
- Knowledge in and the ability to apply the principles of health information management, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

HIPAA Security Officer Job Description

REPORTS TO: Health Commissioner

GENERAL PURPOSE:
The information security manager creates HIPAA Security Policies and orchestrates CANTON CITY PUBLIC HEALTH's Security Management Process so as to protect the confidentiality and integrity of patient, provider, employee, and business information in compliance with organization policies and standards.

DUTIES:
1) Document security policies and procedures created by the information security committee/council
2) Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures
3) Initiate activities to create information security awareness within the organization
4) Perform information security risk assessments and act as an internal auditor
5) Serve as the security liaison to clinical administrative and behavioral systems as they integrate with their data users
6) Implement information security policies and procedures
7) Review all system-related security planning throughout the network and act as a liaison to information systems
8) Monitor compliance with information security policies and procedures, referring problems to the appropriate department manager
9) Coordinate the activities of the information security committee
10) Advise the organization with current information about information security technologies and issues
11) Monitor the access control systems to assure appropriate access levels are maintained
12) Prepare the disaster prevention and recovery plan
13) Secure professional help for assistance with any of the above if the individual is not qualified to perform the task

Appendix D -Facility Security and Safeguards for Oral and Written PHI

FACILITY SECURITY PLAN

1) **Key and Card Access System**. The Fiscal Officer, in conjunction with the Health Commissioner, shall authorize and distribute keys and access cards (fobs) to staff based on their best judgment. When an employee is terminated, their keys shall be recovered and access terminated.
2) **Last Person Out Locks Doors**. When leaving at the end of the day, the last person out must ensure that all outside doors are locked (this is routinely done by Vital Statistics staff).
3) **Verify Credentials of Service Personnel**. All employees should verify the credentials of any service personnel, such as telephone company representatives, computer support vendors, etc., before providing granting access to the facilities. In addition, employees should verify that the service person is performing an authorized service.
4) **Visitors**. Visitors such as vendors or other third parties will be escorted or otherwise supervised while in the office. Any employee who sees an unfamiliar person in a private area of the office suite shall politely verify the person's identity and authority to be on the premises, and take appropriate action with any unauthorized person.
5) **Computer Equipment Access**. The computer servers and networking equipment shall be kept in a locked room with limited access controlled by the Fiscal Officer and/or the Nursing Office Manager.

SAFEGUARDS TO PROTECT ORAL AND WRITTEN PHI

1) Oral Privacy
   A) Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings, and using appropriate volume when speaking to prevent others from overhearing conversations.
   B) Employees should refrain from holding conversations in common areas where patients, their family members, or visitors can overhear PHI.
   C) Discussions concerning patients should be done in a private area and discussions must be limited to "need to know" information for purposes of providing the best services. Joking or complaining about patients is not permitted. Issues with patient behavior that require discussion among staff shall be done in a professional and respectful manner.
   D) Overheard conversations are not to be shared or repeated.
   E) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.
2) Safeguards for Written PHI
   A) Paper Charts and other Written Documentation
      i) All employees using records for patients and other paperwork with PHI shall arrange these items so that PHI is not readily visible to other patients/visitors, especially in high traffic areas such as reception area.
      ii) Charts and other written documentation shall be put away promptly after use, and always at the end of the day to reduce incidental exposures to cleaning personnel and others who may use the facilities at night. Charts shall be kept in designated locked cabinets. Access to the locked storage areas shall be controlled by the Nursing Director.
      iii) Charts shall be available and accessible for patient care during regular business hours.
      iv) Charts in use shall be stored away from patient view. When placing a chart outside a treatment room door, it shall be placed to minimize information that can be seen by a visitor or patient in the corridor.
      v) Charts shall not be left unattended in areas accessible to unauthorized individuals.
      vi) Whenever possible, the original chart will be used rather than a copy.
      vii) Unneeded paper documents containing PHI shall be destroyed by shredding them in an office shredder or with a secure shredding service.
      viii) Charts shall not be removed from the building without the authorization of the HIPAA Privacy and Security Officer.

B) Transportation/outside use of documents with PHI
   i) Health district employees will remove patient records or copies of records only with permission and only for performance of his/her duties.
   ii) Caseworkers and other employees who remove documents from the facility, to conduct field work, for example, are responsible for safeguarding these documents.
   iii) While transporting paper documents, the documents shall be kept in a locked container.
   iv) When leaving documents unattended in a personal vehicle, the vehicle shall be locked and the locked container shall be kept in the trunk and not visible.
   v) If any documents with PHI are lost or stolen, the incident should be immediately reported to a supervisor.

C) Faxing Procedure
   i) When faxing a document with PHI, use a cover sheet which indicates that information is confidential, protected under state and federal laws, and not to be re-disclosed
   ii) Care should be taken to transmit fax to the proper recipient
   iii) Faxed documents should not be left at a common fax machine.
   iv) Faxed documents containing PHI shall only be sent from a designated, secure fax machine.

D) Printing and Copying PHI
   i) Printers and copiers used for printing of PHI shall be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
   ii) PHI printed to a shared printer shall be promptly removed.

E) Any written PHI in non-paper formats, such as medication bottles with patient Rx information, imprints on carbon films used in fax machines, should be destroyed appropriately.

F) Cleaning personnel with access to the facility shall be placed under a confidentiality agreement.

Appendix E - Workforce Access to PHI and Safeguards

Major systems legend:
EHR, Electronic Record Software - Charts
PMS, Electronic Record Software - Billing and Scheduling
HDIS, Case Management / Immunizations / Time and Effort / Limited Billing

Person, Classes of Persons, or Business Associates	***Categories of PHI Needed***	***Comments / Additional Safeguards(*)***
Medical Director	All EHR, except administration and clinical customization, All PMS on an oversight basis	PMS access credentials will be enabled on an as-needed basis when necessary for management oversight
Nurse Practitioner	All EHR, except administration and clinical customization, All PMS on an oversight basis HDIS for time and activity	
Clinical Staff (RNs)	All EHR except administration and clinical customization, PMS – scheduling, demographics, insurance cards and inquiry HDIS for immunization and time & activity	
Nursing Clerical Staff	All PMS HER – scheduling, demographics, insurance cards, notes, reports and inquiry. HDIS for immunization and time & activity	
Payment Posting Staff and Fiscal Manager	All PMS HDIS for time and activity EHR – scheduling, demographics, insurance cards, notes, reports and inquiry	
Nursing Office Manager	All electronic systems - all functions	
Laboratory Personnel	EHR - laboratory sections HDIS - time and activity PMS – scheduling, demographics, and inquiry	
Disease Intervention Specialist	HDIS – time and activity All PMS – Scheduling, demographics, and inquiry	
Director of Nursing and Nursing Supervisor	All EHR All PMS All HDIS	
InSync	All EHR and PMS	
HDIS	HDIS	Remote access to a specified workstation
City Auditor or designee	Processes Refunds in Accounts Payable	Minimal patient information is provided to the City Auditor only if

		a refund is necessary.
City Treasurer or designee	Patient check payments, explanation of benefits for fire/health combined payments	
Accumed	Explanation of Benefits for fire/health combined payments and misdirected payments.	
Fire/Police Financial Manager and Fire Clerical	Explanation of Benefits for fire/health combined payments and misdirected payments.	
State Auditor	Paper financial records including billing journals, cash receipts journals and accounts payable journals	
City of Canton IT Department	HDIS; May be exposed to EHR data for configuration and troubleshooting issues	Access to information necessary for system support, including data backup and troubleshooting
City of Canton Law Department	For collection purposes, Patient Demographics including guarantor information, Charges by line item (date of service, net charges, payments, balance due); Any information needed for their legal advice	Any unnecessary information will be redacted from the record

Access control capabilities will be configured in the EHR and PMS systems based on this analysis

Appendix F – Minimum Necessary – Procedures for Routine Disclosures and Requests

ROUTINE DISCLOSURES

1) **Software & Network Providers** – Information in the computer system is incidentally available during system support activities. Computer support providers who have signed Business Associate Agreements may be granted system access, including remote access, so that they are able to perform support activities per the written support agreement.
2) **Insurance Companies and Government payers** – For services rendered, which are reimbursed by an insurance company or government payer, department personnel shall submit eligibility, billing and claim status inquiry information using ANSI standard electronic transactions (including via Payer websites), and respond to payer requests (per agreement with payers) for additional information as necessary for payment adjudication.
3) **Outside Accountant –** Check registers, deposit slips and other accounting records which may contain some patient names may be sent to the outside accountant who is covered by a Business Associate agreement.
4) **Surveyors and Auditors –** Upon confirmation of surveyors (for example, from a 3rd party payer) credentials, the office manager may provide access to patient charts for patients who are within the jurisdiction of the surveyor or auditor.
5) **Bureau of Disability Determination –** Using the Bureau's forms, assessment information will be shared in order to determine patient's eligibility for benefits.
6) **Courts, Law Enforcement and/or Attorneys –** When information requests are presented, the protocol in Policy 1090 Disclosures that do Not Require an Authorization will be carefully followed (with legal counsel's assistance if necessary) to determine what information may be released.
7) **Other Provider Requests for Reimbursement Support –**and other providers who serve patients of the department and require assistance for their proper reimbursement will be provided the information required by their 3rd party payer. **Immunization Records to Schools**. New patient registration paperwork will include parent's permission to disclose immunization records to schools upon a school's request. If paperwork is not in place, staff shall obtain verbal permission from parent prior to disclosure.
8) **Reportable Conditions**. Reportable conditions, as required by law to a public health authority, will be reported pursuant to the specific legal requirements for that condition.

ROUTINE REQUESTS

1. **Eligibility Inquiry** – Patient insurance eligibility will be verified by calling payers or electronically requesting eligibility via their websites or other electronic interface.

Appendix G - Miscellaneous

POLICY 1200 Patient Right to Access Records
There is no fee to provide a written record to patients.

POLICY 1050 Authorizations
Designated Health Records Release Officers
Division of Nursing:
1. Diane Thompson, RN, MSN Supervisor Clinic, Support Services
2. Sarah Thomas, BSN, RN Nursing Supervisor
3. Laura Roach, RD, LD Women, Infant and Children (WIC) Program

POLICY 1380 HIPAA Documentation
HIPAA Mandated Designations:
HIPAA Privacy and Security Officer: Diane Thompson
Person Responsible for Receiving Complaints: Diane Thompson
Person Responsible for Access to Records: Diane Thompson
Person Responsible for handling requests for Amendment of Records: Diane Thompson
Person Responsible for answering HIPAA questions: Diane Thompson
Designated Record Set: All information in the InSync Electronic Record Software
Information in Paper charts for patients who receive medical services as a patient in the clinic
Information in HDIS regarding immunization and case management

Note: CCPH is HIPAA Hybrid Entity. Its Health Care Component includes the following health provider activities: The following covered functions, and information are created as a result of CCPH's health provider role:

Health Care Component
1) Covered Functions
   A) Health clinic providing direct patient care including immunizations, travel medicine, Early Head Start (EHS) Outreach Services and other direct patient care activities
2) Information that is PHI
   A) Paper charts, other written information, oral information, and/or electronic data in the HDIS or InSync systems documenting provision of health care or payment for health care of patients who are seen in the CCPH health clinic,
   B) Paper charts, other written information, oral information, and/or electronic data in the HDIS or InSync systems documenting case management for individuals not seen in the clinic but who have been identified as having or potentially having a communicable disease

Non Health Care Component
1) Non-Covered Functions
   A) Care Coordination activities including case management for individuals with communicable diseases
   B) Disease Surveillance
   C) PREP for Foster Care and Adjudicated Youth
   D) Quality Assurance Assistance for Health Providers regarding immunizations
   E) Environmental Health Activities
   F) Air Pollution Control
   G) Food Protection
   H) Vital Statistics
2) Information that may contain PHI regulated by the State of Ohio Law but not HIPAA
   A) Case management files for individuals (not seen in the clinic) with communicable diseases
   B) HHLPSS - Healthy Housing and Lead Poisoning Surveillance System
   C) COCASA

D) Ohio Disease Reporting System
E) EPI Center

POLICY 2010 Data Backup

1) **Data Criticality Analysis**. Detailed in the Continuity of Operations Plan (COOP)
2) Backup Documentation
   A) Detailed in the COOP

POLICY 2020 Data Recovery and Emergency Mode Operation Plan

Data Recovery Plan:
Detailed in the Continuity of Operations Plan (COOP)

Emergency Mode Operations Plan:
Detailed in the Continuity of Operations Plan (COOP)

CANTON CITY PUBLIC HEALTH Disclosure Log

Date	Person or Entity receiving Records	Description of records disclosed	Purpose of disclosure	Description of threat to health or safety (if reason is in response to health or safety threat or emergency)

CANTON CITY PUBLIC HEALTH

Attachment 1 - Employee Acknowledgement

Acknowledgement of HIPAA Policies and Procedures

Name_____ Date_____

I have reviewed and understand the HIPAA policies and procedures that are relevant to my job duties. These include:

Policy number	Description
1010	HIPAA – General Rules
1015	Clinical Data Collection
1020	Minimum Necessary
1030	Confidentiality Safeguards (Oral and Written)
1040	Speaking with the Family or Friends of a Patient Receiving Services
1050	Authorizations
1070	Minors, Personal Representatives and Deceased Patients
1080	Duty to Report Violations and Security Incidents
1090	Disclosures that do not Require an Authorization
3080	Computer Usage
3082	Social Media
3085	Portable Computing Devices and Home Computer Use

Further, I understand all other HIPAA policies that are relevant to my job duties.

I have been assigned my own User ID, will access the computer only with my User ID, and I will keep my password confidential. I further understand that the software used in the department tracks all records viewed, changed, deleted or printed based on User ID. I understand that I may be held accountable for all computer usage performed with my User ID, and that failure to follow these procedures could result in discipline, termination of employment, civil fines and/or criminal prosecution.

Signature:_____ Date:_____

Attachment 2 - Confidentiality Agreement for Outside Agency or Individual

Confidentiality Agreement for Outside Agency or Individual

Patient information in any form, written, spoken or in electronic systems, is protected by federal HIPAA regulations. AGENCY/INDIVIDUAL has access to the Health District facilities exclusively for the purposes of performing duties in the service agreement and is expressly prohibited from accessing any electronic equipment or reading any information regarding patient care. In the event that any personnel employed by AGENCY/INDIVIDUAL overhear any information regarding patients while on premises or see any information, that information will be kept confidential and not disclosed.

Failure to abide by the terms of this agreement may result in termination of contract and/or legal action against AGENCY/INDIVIDUAL and/or its personnel.

AGENCY/INDIVIDUAL

By:_____
Name: _____
Title: _____
Date:_____

PUBLIC HEALTH

By:_____
Name:_____
Title:_____
Date:_____

Attachment 3 – Employee Confidentiality Agreement

Employee Confidentiality Agreement

As a Canton City Public Health (CCHD) full-time, part-time, seasonal or intermittent employee, subcontracted CCHD employee, visiting professional, work study student, intern, Board of Health member, any City of Canton employee who performs work at the CCHD and/or other CCHD employees as approved by the Health Commissioner:

I understand that I may have access to confidential and privileged information about CCHD clients or customers. This information includes surveillance information such as paper and/or electronic laboratory and/or medical records, study-related forms and/or records, information obtained through oral and/or written interviews and/or other related contact information. This information may also originate from the records of health care providers, health care facilities, medical and health clinics, drug treatment centers, correctional institutions and jails and/or other institutions and facilities. Examples of confidential information include but are not limited to patient names, addresses, telephone numbers, medical, psychological and/or health related conditions and treatment, personal finances, living arrangements and social history.

Terms of Agreement

1. Personally identifiable information will not be discussed except in the performance of job-related duties. These discussions must not take place in hallways, elevators, lavatories, lunchrooms, break rooms, lobbies or other public areas and/or at any time outside of business needs.
2. Reports, records and/or information may only be released in accordance with the Ohio Revised Code. Information cannot be released through e-mail, text message or social media.
3. Any document to be disposed of that contains patient identifiers shall be shredded per the CCHD Records Retention Policy.
4. All confidential files, including compact discs, flash drives and diskettes must be kept in a physically secure location such as a secure file cabinet or locked desk drawer when not in use, when the work area is left unattended and/or when individuals who have not signed this agreement enter the work area.
5. Information on back-up or portable devises (i.e. laptops, compact disks, flash drives, diskettes, etc.) must be encrypted, password protected and the device must be sanitized when the information is no longer needed or upon completion of the activity/project.
6. Visitors are not permitted any CCHD workstation where confidential information is visible.
7. Telephone conversations and/or conference calls requiring the discussion of identifiers will only be conducted in select CCHD work areas.
8. To prevent unauthorized access to confidential data and databases, users must log out of the application and database before work breaks, work lunches, when leaving for an excess amount of time and when leaving work until the next business day.

9. The computer(s) where confidential data is accessed by the employee will be protected by screen saver passwords. The passwords will not be disclosed nor access allowed to unauthorized persons.
10. The data generated and used while employed by the Canton City Health District is property of the CCHD.

I understand that intentional or involuntary violation of these standards is subject to appropriate disciplinary actions(s) per the CCHD 800-006-P_Employee Discipline Policy and such discipline could include being discharged from my position and/or being subject to other penalties.

By signing this statement, I am indicating my understanding of my responsibilities and agree to abide by the CCHD 800-016-P_HIPAA Policy. I also agree to hold the CCHD and its agents harmless from any damages and legal fees arising in any way from the wrongful disclosure of confidential or privileged information resulting from my negligence or willful misconduct.

Employee Signature	Supervisor Signature (if applicable)
Printed Name	Printed Name
Date	Date

Attachment 4 - Standard Authorization Form

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Name of Client: _____ DOB: _____

Address: _____ Telephone: _____

The following programs are authorized to exchange health information as noted below:

_____

CCPH Program Authorized to Disclose/Exchange Information

_____

Authorized Individual/Organization to/from Whom Information is Disclosed/Exchanged

Purpose of Disclosure:

☐ To coordinate treatment
☐ Assessment information for treatment planning
☐ Information for ongoing treatment
☐ Other purpose: _____

Information to be Disclosed:

☐ Lab Results
☐ Progress Notes
☐ Prenatal Care
☐ Diagnosis
☐ Response to Treatment
☐ Treatment Plans
☐ Other Information (specify): _____

Information which will NOT be Disclosed:

☒ HIV/AIDs Testing or status
☐ Other Information (specify): _____

Time Period to be Disclosed: [ ] information from the current/most recent admission/treatment episode, [ ] information for the period of: _____ to:_____

This authorization expires in 60 days, unless an earlier date is specified here: _____

1. I understand that CCPH may not condition treatment on my providing authorization for the requested use or disclosure and that I MAY REFUSE TO SIGN THIS AUTHORIZATION.
2. I understand that I may revoke this authorization by written request at any time, except to the extent that CCPH has already acted on it.
3. I understand that the recipients of this information may not be obligated to follow the federal privacy regulations, and potentially could re-disclose this information.

This facility, its employees, officers, and physicians are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

_____ _____ _____ _____

Signature of Client or Legal Representative Date Signature of Witness Date

Printed Name: _____ Relationship to Patient/Authority: _____

I hereby revoke my consent _____ _____

Signature Date

Attachment 5 - Letter for Non-Conforming Requests for PHI

After April 14, 2004, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that the Canton City Public Health receive HIPAA compliant authorization from all *covered entities* in order to release a patient's medical record. However, your recent request does not meet the HIPAA standards for an authorization and therefore we cannot provide the requested records.

A request for release of information is not valid and will not be accepted unless it contains the following information:

- Name of institution/medical facility that is to release the information;
- Name of individual/institution/medical facility to whom information is to be released;
- Patient's full name and some type of identifying information (i.e., birth date, social security number, address, etc.);
- Purpose or need of information to be disclosed;
- Extent or nature of specific information to be released, including date(s) of treatment;
- NOTE: An authorization specifying "any and/or all information" without further information, will not be accepted;
- Date the request was issued;
- Signature of client, or client's parent(s) or legal guardian if client is a minor or legally incompetent, or signature of next of kin if client has expired or is incapable of signing;
- Date the consent was signed by the client;
- Statement that the authorization is subject to revocation by the patient or the patient's legal representative (see Agency Privacy Notice);
- Statement that information may be re-disclosed and no longer protected by Federal Privacy Regulations.

For your convenience, I have attached a copy of our HIPAA compliant authorization that you may use in any future requests for records from CCPH. If you have any questions, please feel free to give me a call at (330) 489-3322.

Respectfully,

Director of Nursing/Health Records Release Officer

Attachment 6 - Authorization for Confidential HIV Test Results

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Name of Client: _____ DOB: _____

Address: _____ Telephone: _____

The following programs are authorized to exchange health information as noted below:

_____

CCPH Program Authorized to Disclose/Exchange Information

_____

Authorized Individual/Organization to/from Whom Information is Disclosed/Exchanged

Purpose of Disclosure:

☐ To coordinate treatment
☐ Assessment information for treatment planning
☐ Information for ongoing treatment
☐ Other purpose:
_____

Information to be Disclosed:

☐ Lab Results - HIV
☐ Progress Notes
☐ Prenatal Care
☐ Diagnosis
☐ Response to Treatment
☐ Treatment Plans
☐ Other Information (specify):
_____

Information which will NOT be Disclosed:

☐ Other Information (specify):
_____

Time Period to be Disclosed: [ ] information from the current/most recent admission/treatment episode, [ ] information for the period of: _____ to:_____

This authorization expires in 60 days, unless an earlier date is specified here: _____

1. I understand that CCPH may not condition treatment on my providing authorization for the requested use or disclosure and that I MAY REFUSE TO SIGN THIS AUTHORIZATION.
2. I understand that I may revoke this authorization by written request at any time, except to the extent that CCPH has already acted on it.
3. I understand that the recipients of this information may not be obligated to follow the federal privacy regulations, and potentially could re-disclose this information.

This facility, its employees, officers, and physicians are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

_____ _____ _____ _____

Signature of Client or Legal Representative Date Signature of Witness Date

Printed Name: _____ Relationship to Patient/Authority: _____

Legal Notice to the Recipient: This information has been disclosed to you from confidential records protected from disclosure by state law. You shall make no further disclosure of this information without the specific, written, and informed release of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is not sufficient for the purpose of the release of HIV test results or diagnoses.

I hereby revoke my consent _____ _____
Signature Date

Attachment 7 - State Law Provider Confidentiality Agreement

Confidentiality Agreement

This agreement is between the Canton City Public Health, with offices at 420 Market Ave., North, Canton, OH 44702, hereafter "Health Department" and _____, with offices at _____, hereafter, "Provider".

Whereas, the Canton City Public Health, in its role as a public health agency, receives certain Protected Health Information through mandatory reporting and other State of Ohio data sets, and

whereas, the confidentiality of this Protected Health Information is governed by laws of the State of Ohio, and

whereas, the State of Ohio confidentiality laws are different than the federal HIPAA regulations, and

whereas, the State of Ohio laws require the Canton City Public Health to obtain a confidentiality agreement when releasing records for treatment or to ensure their accuracy,

the two parties hereby agree to the following Confidentiality Agreement:

Protected Health Information shall have the same meaning as in Ohio Revised Code 3701.17.
If Provider is a HIPAA Covered Entity, then Provider shall comply with the requirements of the HIPAA Privacy, Security and Breach Notification requirements at 45 CFR 164 Subparts C, D and E.
Provider shall further comply with the requirements of Ohio Revised Code 3701.17.

Agreed by:

Canton City Public Health

_____ _____
James M. Adams, RS, MPH Date
Health Commissioner

Provider

_____ _____
(Signature) Date

_____
(Printed Name)

_____
(Title)

Reference: ORC 3701.17 Protected health information

(A) As used in this section:

(1) "Prosecutor" has the same meaning as in section 2935.01 of the Revised Code.
(2) "Protected health information" means information, in any form, including oral, written, electronic, visual, pictorial, or physical that describes an individual's past, present, or future physical or mental health status or condition, receipt of treatment or care, or purchase of health products, if either of the following applies:

(a) The information reveals the identity of the individual who is the subject of the information.
(b) The information could be used to reveal the identity of the individual who is the subject of the information, either by using the information alone or with other information that is available to predictable recipients of the information.

(B) Protected health information reported to or obtained by the director of health, the department of health, or a board of health of a city or general health district is confidential and shall not be released without the written consent of the individual who is the subject of the information unless the information is released pursuant to division (C) of this section or one of the following applies:

(1) The release of the information is necessary to provide treatment to the individual and the information is released pursuant to a written agreement that requires the recipient of the information to comply with the confidentiality requirements established under this section.
(2) The release of the information is necessary to ensure the accuracy of the information and the information is released pursuant to a written agreement that requires the recipient of the information to comply with the confidentiality requirements established under this section.
(3) The information is released pursuant to a search warrant or subpoena issued by or at the request of a grand jury or prosecutor in connection with a criminal investigation or prosecution.
(4) The director determines the release of the information is necessary, based on an evaluation of relevant information, to avert or mitigate a clear threat to an individual or to the public health. Information may be released pursuant to this division only to those persons or entities necessary to control, prevent, or mitigate disease.

(C) Information that does not identify an individual is not protected health information and may be released in summary, statistical, or aggregate form. Information that is in a summary, statistical, or aggregate form and that does not identify an individual is a public record under section 149.43 of the Revised Code and, upon request, shall be released by the director.

(D) Except for information released pursuant to division (B)(4) of this section, any disclosure pursuant to this section shall be in writing and accompanied by a written statement that includes the following or substantially similar language: "This information has been disclosed to you from confidential records protected from disclosure by state law. If this information has been released to you in other than a summary, statistical, or aggregate form, you shall make no further disclosure of this information without the specific, written, and informed release of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is not sufficient for the release of information pursuant to this section."

Effective Date: 02-12-2004

Attachment 8- Ohio Legal References

The following ORC Statues were reviewed for creation of this policy manual. Note that this is not a comprehensive list of all relevant ORC statutes.

Key Confidentiality Law
ORC 3701.17 Protected Health Information

Patient Rights
ORC 3701.74 Patient or patient's representative to submit request to examine or obtain copy of medical record
ORC 3709.241 Minor may give consent for diagnosis or treatment of venereal disease

Disclosure for Specific Conditions
ORC 3701.243 Disclosing of HIV test results or diagnosis
ORC 3701.248 Emergency medical or funeral services worker exposed to contagious or infectious disease may request notice of test results.
ORC 3701.244 Civil Actions

Public Record Laws
ORC 149.l43 Availability of public records for inspection and copying
ORC 149.433 Exempting security and infrastructure records

Confidentiality of Public Health Records
ORC 307.629 Confidentiality of Child Fatality Review Board Records
ORC 3701.028 Confidentiality of BCMH Program Records
ORC 3701.241 Responsibilities related to AIDS and HIV programs
ORC 3701.62 Help Me Grow Verification Code