KITSAP PUBLIC HEALTH DISTRICT

POLICIES & PROCEDURES

Title:	**Protecting Confidentiality of Health Information**	Page 1 of 12
Number:	Legal Policy L-2	Effective Date: 5/9/14
Applies To:	All Employees, Interns, Contractors and Volunteers	Supersedes: 12/1/08
Approved:	Scott Daniels, MS, RS, Administrator	Next Review: 5/9/17

A. Purpose

The purpose of this policy is to establish rules concerning the use and disclosure of Protected Health Information (PHI) and other confidential health information. This policy provides procedures in order to protect the confidentiality of health information for clients and employees, and establishes processes for both clients and District staff to best assist clients in obtaining such access to comply with the Public Records Act chapter RCW 42.56. The public is encouraged to access public records available on our website, www.kitsappublichealth.org, before submitting a public records request.

B. Policy Statement

The Kitsap Public Health District (District) is committed to protecting the privacy of the Personal Health Information (PHI) of its clients as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the implementing regulations which include the Standards for the Privacy of Individually Identifiable Health Information (the "Privacy" Rule 45 C.F.R. Parts 160 and 164) and the Security Standards for the Protection of Electronic Protected Health Information (the "Security" rule 45 C.F.R. Parts 160 and 164) as amended by applicable provisions of the Health Information Technology for Economic and Clinical Health Act (Title XIII Subtitle D) and its implementing regulations (the "HITECH" act), including the final rule issued on January 25, 2013, that modified HIPAA Privacy, Security, Enforcement, and Breach Notification rules under HITECH.

This policy is not intended to interfere with client or employee access to his or her medical records. It is intended, however, to restrict disclosure of protected health information as required for treatment, payment, or healthcare operations; to other disclosures specifically authorized by the client; or as required by law. Additionally, for the Environmental Health Division, many records are considered public documents as set forth in Washington State's Public Records Act, Chapter 42.56 RCW. The identity of persons filing complaints can be held confidential when certain conditions are met as described in this policy/procedure.

C. Definitions

1. **Breach:** The same meaning given such term in 45 CFR § 164.402; a breach means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

2. **Business Associate:** The same meaning given such term in 45 CFR § 160.103; a business associate is an individual or entity other than a member of the District's workforce that creates, receives, maintains, or transmits PHI in either paper or electronic form to perform or assist an activity on behalf of the District. Examples include legal, actuarial, accounting, consulting, data

aggregation, administrative, financial services or vendors providing "patient safety activities" such as health information organizations, health record vendors, and vendors that facilitate data transmission.

3. **Electronic Protected Health Information (EPHI):** Protected health information specifically in electronic or digital form.

4. **Privacy Rule:** The implementing rules in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), at 45 CFR parts 160 and 164, requiring covered entities to have in place appropriate administrative, physical, and technical safeguards for protected health information and to implement those safeguards.

5. **Protected Health Information (PHI):** Information in any form --- oral, aural, electronic, or printed --- that identifies an individual and relates to his or her physical or mental health. PHI, for the purpose of this policy, includes not only clients, but also employees when protected health information is involved. Health information that has been edited to remove identifiers or potentially identifying data or information is not PHI under this policy. PHI for a person who has been dead more than 50 years is not protected.

6. **Records:** Documents either in paper or electronic form. Under Chapter 42.17 RCW, public records refer to any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

7. **Security Rule:** The implementing rules in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR parts 160 and 164 developed to implement security safeguards to protect electronic protected health information (EPHI) while permitting the appropriate access and use of that information. Sets standards for ensuring that only those who should have access to EPHI will have access by implementing appropriate administrative, technical, and physical safeguards to protect the security of EPHI.

8. **Unsecured PHI:** PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology to unauthorized individuals.

D. Implementing Procedures: In General

1. **Hybrid Entity**

   a. The District declares itself a "hybrid entity" whose business activities include both covered and non-covered functions. The District designates most Community Health Programs and Administrative Services Programs such as Accounting and Information Technology as healthcare components according to CFR §164.504(c)(3)(iii). The District excludes the Environmental Health Division as non-covered functions.

   b. CFR §164.512(b)(1)(i) authorizes public health agencies to collect and receive information for the purpose of preventing or controlling disease, disability, or injury including public health surveillance, public health interventions, and public health investigations. In these circumstances, the District may use or disclose PHI without the written authorization of the individual.

c. Disclosure of PHI between the covered components and the non-covered components must follow the guidelines outlined in this policy.

2. **Training.** The District will provide training on the requirements in this policy to all new employees, contractors, interns, and volunteers and will provide annual training updates to staff who work with records containing PHI. Training will provide an overview of key provisions of the HIPAA act and terminology contained in the act as well as more detailed information about handling PHI, PHI disclosures, and authorization requirements in a medical setting. Training will be provided to all staff as necessary whenever there is a material change in the District's policies and procedures. All initial and ongoing training will be documented.

3. **Formal Acknowledgment of Confidentiality.** All employees, contractors, interns, and volunteers will review and sign a Statement of Confidentiality (Attachment B) that is retained in his/her personnel file. Violations of this confidentiality policy may result in disciplinary action. Willful violations may result in disciplinary action up to and including immediate dismissal.

4. **Business Associates**

a. Business Associates such as auditors, accounting vendors, quality assurance assessors, lawyers, transcriptionists, interpreters, consultants, janitorial workers, building maintenance staff, building security staff, and vendors providing "patient security services" must sign a District Business Associate agreement or such terms will be incorporated into the body of the primary agreement. Entities that store PHI, in either paper or electronic form, are considered to be Business Associates even if they do not access, use, or disclose that information.

b. If the Business Associate is a government entity, the provisions of this policy may be met by entering into a memorandum of understanding. Other Business Associates may comply with the requirements of this policy by executing an amendment to an existing contract or by signing a contract that demonstrates compliance with HIPAA and the requirements in this policy.

c. A Business Associate arrangement does not exist between:

i. The District as a provider and other providers.
ii. The District and financial institutions.
iii. Entities that provide courier or transmission services such as the United States Post Office or internet service providers.

d. Business Associates are directly liable for impermissible uses and disclosures of PHI to include failure to provide breach notifications to the District; failing to disclose PHI to HHS when required; failing to disclose PHI to the District or an individual whose PHI information is at issue, if the individual has requested such information; failing to comply with the minimum necessary standards, and failing to enter into Business Associate agreements with subcontractors that create or receive the District's PHI.

e. The contract may permit the Business Associate to use and disclose PHI and/or EPHI in its capacity as a Business Associate to the District to the extent permitted by law. Business Associates will limit the use, transmission, or disclosure of PHI to the minimum necessary consistent with the District's policies and procedures to perform its duties and obligations under Agreement. The contract will require the Business Associate not to further disclose PHI and/or EPHI other than as allowed by the contract or required by

law, use appropriate safeguards to prevent unauthorized use or disclosure of PHI and/or EPHI, report to the District any unauthorized use or disclosure of PHI once it becomes aware, and ensure that any agents including sub-contractors agree to the same restrictions that apply to the Business Associate. The contract shall also require the Business Associate, at the time the contract is terminated, to return or destroy any PHI and/or EPHI in its possession or, if impractical, to extend or maintain the provisions of the contract as long as the PHI and/or EPHI is retained.

f. Subcontractors of Business Associates to whom the Business Associate delegates such functions to a subcontractor that creates, receives, maintains, or transmits PHI are themselves considered to be Business Associates of the District. The District is not required to enter into a Business Associate agreement with a subcontractor of a Business Associate; however, the Business Associate is required to have a Business Associate agreement with its subcontractors.

g. Business Associates must cooperate with the District to provide access to PHI and/or EPHI to allow for amendment or correction of the PHI and/or EPHI, and for accounting PHI and/or EPHI disclosures.

h. Business Associates must make available to the District their internal practices, books, and records at no charge relating to the use and disclosure of PHI and or EPHI available to the District for purposes of determining that Business Associate is in compliance with the requirements of its agreement with the District and the HIPAA rule.

i. If the District becomes aware of a pattern of activity or practice by a Business Associate that constitutes a material breach, the District shall take reasonable steps to cure the breach or end the violation. If such steps are not successful, the District may elect to terminate the contract or agreement.

5. **Confidentiality.** To the extent possible, District services and operations will be conducted in such a way that only those who need to know can hear or see clients and providers when they are directly sharing PHI.

6. **Maintenance of Information.** To safeguard against unauthorized access to records and data:

a. Documents containing PHI will be attended by a staff person or contained in a locked area. These documents include medical records, billing forms, x-rays, lab reports, client logs and mailed or faxed documents containing protected health information. Fax machines used to transmit and receive PHI will be kept in a room that is in a restricted area and locked at night.

b. Medical records and personnel files with PHI will be kept in locked files when not in use and checked in and out for use using proper accountability procedures.

c. All medical clinic logs and quality assurance records will be retained in locked files or restricted areas.

d. All telephone notes or other client logs not included in medical records or quality assurance files will be disposed of in confidential refuse bins.

e. EPHI will be protected from unauthorized disclosure through staff adherence to District policies on password protection, automatic locking of computers, and leaving

computers unattended. Staff will be prohibited from duplicating data files or removing or transmitting data unless specifically authorized to do so. Additional information technology security policies and procedures are contained in District Administrative Policy A-1, "Information Technology Resources".

f. Records containing client information shall be stored and destroyed in a fashion consistent with District records retention and information technology security policies.

g. The Health District mailroom is located at the Norm Dicks Government Center on a locked secured floor to protect confidential mail and faxes stored there.

h. For incoming mail containing PHI, e.g., medical records, clerical staff will open and date stamp the mail. Medical lab data reports will not be opened and date stamped by clerical staff. Medical lab data reports will only be opened and date stamped by a clinic manager or supervisor who will then be responsible for forwarding the data, as appropriate.

7. **Use of Text Messaging and Social Media.** District staff may use text messaging and social media, such as Facebook, to contact clients with appointment reminders under limited circumstances when it is not possible to contact a client through more conventional means, such as voicemail. It is necessary to obtain a client's consent for text messaging and for leaving messages on voicemail. Since text messages and social media are not confidential, staff must follow minimum necessary HIPAA standards for leaving information: appointment time and clinic phone number without stating the reason for the appointment or the name of the clinic, clinician, or information that would identify the client such as the client's name or date of birth.

8. **Disclosure of Protected Health Information Without Authorization**

a. The District may use or disclose PHI to provide treatment, for payment, or for healthcare operations in compliance with the District's Notice of Privacy Practices, Disclosure of PHI is on a "need to know" basis: only the minimum necessary information to accomplish treatment, payment, or healthcare operations on behalf of the client or District shall be disclosed.

b. Disclosure of PHI for treatment, for payment, or for healthcare operations does not need to be documented in the medical record for disclosure accounting purposes.

c. PHI may also be disclosed without authorization for specific legal, administrative, or emergency reasons as listed in Attachment A at the end of this policy.

9. **Disclosures of PHI that Require Authorizatio**n

a. Specific authorization from the client shall be required for disclosure other than for purposes of treatment, payment, or healthcare operations. Staff must verify the identity of the requestor and confirm the authorization of the entity requesting release of the PHI to receive it before releasing it.

b. After verifying the identity of the requestor and confirming the authorization of the entity requesting release of the PHI to receive it, disclose only the minimum necessary information.

c. The identity of the person requesting the disclosure of PHI must be verified. For example, clients who call for PHI over the telephone (such as when requesting a test result) must identify themselves by providing their date of birth or confirming their address. Compare the signature on a records transfer request with a known sample of the client's signature from the chart. When external providers, such as another medical provider, request PHI without written authorization from the client, such as when confirming date of last visit or confirming medication prescribed, the client's verbal or written permission to release the PHI must be received prior to releasing the PHI to the provider. Confirm the provider's telephone number independently using a directory and call the provider back before releasing PHI.

d. The District will follow records release guidelines contained in RCW 70.02 and WAC 246-100-016(2) where such guidelines are more restrictive than HIPAA guidelines. Staff will be trained on how to comply with these regulations for release of PHI.

e. **Marketing and Fundraising.** The District does not engage in activities where it receives financial remuneration in exchange for the use or disclosure of PHI for marketing or fundraising purposes.

f. **Sale of PHI.** The District does not disclose PHI where the District would directly or indirectly receive financial or non-financial payment from or on behalf of the recipient of the PHI in exchange for the PHI.

g. **Research.** Before individually identifiable PHI may be used for research, the individual whose PHI will be used must provide signed written permission to the District for such use.

h. **Psychotherapy Notes.** Written authorization is required for the release of psychotherapy notes.

i. **Deceased Persons.** PHI of deceased persons is protected for fifty (50) years after death. During that period, the decedent's personal representative will be required to sign the authorization for disclosure of the decedent's health records. (See District policy A-30 Records Management for information about the District's records retention policy.)

j. **Genetic Information.** Genetic information may not be disclosed for underwriting purposes pursuant to the Genetic Information Nondiscrimination Act (GINA).

10. **Disclosure of Records of Minors**

a. Minors 13 years of age or over may consent to care regarding their sexuality without parental consent. A minor patient's signature is required for the release of PHI (refer to RCW chapter 70.24.110 and Washington Supreme Court decision State v. Koome, 84 Wn.2d 901 (1975).

b. Parents of children age 13 and under may request release of their child's record by signing the appropriate release.

c. PHI for legally emancipated minors may not be released without the minor's signature.

11. **Correctional Facilities**

    a. The medical units of correctional facilities are covered entities.

    b. Inmates do not have the right to receive the Notice of Privacy Practices while the inmate is in the custody of the correctional facility.

    c. Staff providing care for inmates may disclose PHI if necessary to:

        i. Provide health care to the inmate;
        ii. Protect the health and safety of the inmate or other inmates;
        iii. Protect the health and safety of officers or other employees of the correctional facility;
        iv. Protect the health and safety of officers or employees of this or other correctional facilities during transport of the inmate;
        v. Provide law enforcement in the correctional facility; and
        vi. Provide for the administration, safety, and good order of the correctional facility.

    d. Once the inmate is no longer in custody or is released on probation, parole, or supervised release, these provisions no longer apply.

12. **Accounting of Authorized PHI Disclosures.** PHI disclosures other than for treatment, payment, or healthcare operations will be recorded in the medical record including the date of disclosure, what protected healthcare information was disclosed, to whom it was disclosed, how it was disclosed, and the name of staff processing the disclosure.

13. **Client Rights**

    a. **Right to inspect and receive copies.** Clients have the right to request to inspect or receive a copy of their PHI. We have 30 days from the date of the request to comply. If necessary, we may request a 30-day extension for a maximum of 60 days. The request must be made in writing and shall be retained in the client's file. We may charge a reasonable fee to cover the cost of copying, labor, and postage. Clients that wish to inspect their record will be taken to a private area during the review and will be accompanied at all times by a staff member. The inspection will be noted in the record including date and signature of accompanying staff.

    b. We may deny the request for covered reasons. If we deny the request, the client has the right to have the denial reviewed.

    c. Right to request nondisclosure to health plans for items or services that are self-paid: You have the right to request in writing that healthcare items or services that you have paid for in full in advance of your visit not be disclosed to your health plan.

    d. **Electronic Copy of PHI.** Clients have the right to request to request access to their own PHI maintained in a designated record set in electronic form. In the event that the PHI cannot be provided in the requested format or the client declines electronic format, the District can comply with the request for an electronic copy by providing a paper copy of the PHI.

e. **Right to Request Restricted Access.** Clients have the right to request a restriction on the use of their PHI; however, the District may deny the request.

f. **Amendment of PHI.** Clients may request to amend their PHI if they believe information in the record is erroneous or incomplete. This request must be made in writing and provide a reason for the request. We have 60 days from the date of the request to comply.

   i. If we deny the request, we must inform the client in writing and explain why we are denied the request. The client may submit a written statement disagreeing with our denial. The written statement of disagreement is filed in the client's medical record.
   ii. The PHI amendment must identify the records that are affected by the amendment.
   iii. Requests for name changes must be made in writing and include a signature with both the old and new names. The date, details of the name change, and staff who processed the request will document the change in the chart.

g. **Right to know about PHI disclosures.** Clients have the right to request an accounting of the times we have disclosed their PHI. A client has the right to receive a list once per year without charge, as required by the Act. A reasonable fee for copying and mailing may be charged for more frequent requests. A client request for PHI accounting must be in writing and should be referred to the District's HIPAA contact person for processing. We must respond to a request for a PHI accounting within 60 days from the date of the request.

h. **Right to receive confidential communications.** Clients have the right to request that the District communicates with them in a particular way or location. For example, a client may request that they be contacted only by mail or only at work.

14. **Records Needed for Fieldwork**

   a. Charts or other medical information that need to be transported will be placed in a secure container and transported directly from one site to another.
   b. Records or devices containing records such as computers taken to the field will be checked in and out on a log using proper accountability procedures.
   c. Field records not returned to District premises overnight will be retained in a secure locked transport bag or box in a locked vehicle or residence.

15. **Notice of Privacy Practices.** Clients must be offered a copy of the District's Notice of Privacy Practices at the time of the first visit. Clients acknowledge receipt of the Notice of Privacy Practices by signing and dating the signature page. The signature page is kept in the client's medical record. If a client refuses to sign the Notice, a staff person will note the client's name, note that the client refused to sign the Notice, date the form, and sign the form. Refusing to sign the Notice of Privacy Practices does not prevent the District from using or disclosing PHI as provided by the HIPAA Privacy Rule or Washington State law.

    The Notice of Privacy Practice is made available to anyone who requests a copy and is posted on the District's website.

16. **Breach**

    a. A breach is the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

    b. **Exceptions.** The term 'breach' does not include:

        i. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the District or Business Associate if (1) such acquisition, access, or use was made in good faith and within the course and scope of employment or other professional relationship of such employee or individual acting under the authority of a covered entity or business associate; and (2) such information is not further acquired, accessed, used, or disclosed by any person;
        ii. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by District or Business Associate to another similarly situated individual at same facility; and
        iii. Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

17. **Breach Notification**

    a. Staff who become aware of a deliberate or inadvertent wrongful disclosure of PHI committed by themselves or another employee must report such violations promptly to their immediate supervisor and the District's Privacy Officer.

    b. Staff that report violations in good faith are protected by the District's Whistleblower Protection Policy (Legal Policy L-1).

    c. **Risk Assessment.** Upon receiving a breach notification, the District's Privacy Officer will conduct a risk assessment to determine the extent of the breach and probability that the PHI was compromised. At the conclusion of the internal investigation, the Privacy Officer will prepare a formal report of the findings. The Privacy Officer will take steps to ensure compliance with HIPAA regulations in the future including, if necessary, implementing changes to policies and procedures to mitigate the effects of improper disclosure.

    d. The Privacy Officer is required to provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media.

    e. **Individual Notice.** Notification to individuals must be in written form delivered by first-class mail. If the District has insufficient or out-of-date contact information for 10 or more individuals, the District must provide substitute notice by either posting the notice on the home page of its website or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the District has insufficient or out-of-date contact information for fewer than 10 individuals, the District may provide substitute notice by an alternative form of written, telephone, or other means. Substitute notices must include a toll-free number for individuals to use to determine if their PHI was involved in the breach.

Individual notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of the breach. The notification must include, to the extent possible, a description of the breach; a description of the types of information that were involved in the breach; the steps affected individuals should take to protect themselves from potential harm; and a brief description of what the District is doing to investigate the breach, mitigate the harm, prevent further breaches, including contact information for the District.

f. **Media Notice**. In breaches affecting more than 500 residents, in addition to notifying the affected individuals, the District is required to provide notice to prominent media outlets serving Kitsap County. Media notification must be provided without unreasonable delay and no later than 60 days after discovery of the breach.

g. **Notice to the Secretary.** The District will notify the Secretary of breaches of unsecured PHI by completing the breach report form on the HHS website. For a breach affecting 500 or more people, the breach must be reported no later than 60 days after discovery of the breach. Otherwise the District may notify the Secretary of any breaches on an annual basis no later than 60 days after the close of the calendar year in which the breach occurred.

h. **Business Associates.** Business Associates are required to notify the District of a breach no later than 60 days following discovery of the breach. To the extent possible, the Business Associate should provide the District with the identity(ies) of the individual(s) affected as well as any information required to be provided by the District in its notification.

18. **Questions and Complaints**

a. Clients with questions and complaints may contact the District's Privacy Officer.

b. Clients who feel the District has violated their privacy rights may file a verbal or written complaint with the District's Privacy Officer.

c. Upon receiving a complaint, the contact person and the program manager will begin an internal investigation to determine the facts of the complaint by reviewing documents and interviewing witnesses. Upon conclusion of the investigation, the contact person and program manager will prepare a formal report of the findings. The Privacy Officer shall review the report prior to filing. The Privacy Officer shall retain such reports in a confidential HIPAA complaint file.

d. Upon completion of the investigation and the filing of the report, the contact person will contact the client to report the findings. Any response from the client will be retained in the HIPAA complaint file with the investigation report.

e. Clients may also file a complaint with the Secretary of the U.S. Department of Health and Human Services.

f. The District will not retaliate against a patient when a complaint is filed.

19. **Changes to Policies and Procedures.** The District reserves the right to change its policies and procedures at any time consistent with HIPAA and other applicable laws and regulations.

E. Implementing Procedures: HIPAA Security Rule

1. **Requirements**

    a. **Development of Security Procedures.** The Privacy Officer is responsible for the development and implementation of policies and procedures for appropriate security safeguards necessary to protect EPHI that the District creates, receives, maintains, or transmits.

    b. **Emergencies and Other Occurrences.** The Privacy Officer is responsible for the development and implementation of policies and procedures to protect EPHI against any reasonably anticipated threats or hazards, such as natural disasters, vandalism, or fire.

    c. **Compliance.** The Privacy Officer is responsible for ensuring compliance by the District's workforce with the requirements of this policy, including establishing training and auditing procedures.

2. **Building Access and Security Controls.** Facility access necessary to protect PHI is addressed in Administrative Policy A-21, Building Access and Security.

3. **Information Technology Security.** Information technology security procedures are addressed in Administrative Policy A-1, Information Technology Resources.

4. **Security Incident Procedure.** If time permits and if there is no immediate danger, employees who leave their normal work area during an emergency should:

    a. File sensitive documents in a secure location.

    b. Close programs that contain EPHI.

    c. Disconnect electrical equipment including desktop and laptop computers.

E. Implementing Procedures: Complaint Records in Environmental Health

1. **Maintenance of Information.** Information revealing the identity of persons who file complaints with the District is exempt from public inspection and copying if 1) disclosure would endanger the person's life, physical safety, or property, or 2) the person, at the time of filing the complaint, indicates a desire for nondisclosure. Efforts to ensure confidentiality will include, but not be limited to, the following:

    a. All complaint records shall be stored in a manner assuring privacy and affording reasonable barriers to access by the public, press, or employees without the "need to know."

    b. Records containing complainant information shall be stored and destroyed in a fashion consistent with District records retention and information technology security policies.

    c. Complaint records shall remain the property of the District.

d. Information from complaint records identifying the complainant shall not be released without the consent of the complainant (parent or legal guardian - where applicable for minors) in accordance with the following:

   i. Complaint forms shall include a block on the form indicating whether the complainant desires disclosure or nondisclosure of his or her identity. If the complainant does not indicate this desire to the District employee receiving the complaint, the employee shall affirmatively ask a question regarding disclosure or nondisclosure before completing the form. To avoid the appearance of bias toward disclosure or nondisclosure, the employee shall give the complainant the option to choose either disclosure or nondisclosure.
   ii. Anytime the identity of a complainant is requested, the employee shall consult with a manager or supervisor prior to proceeding with a course of action.
   iii. For any previous complaints where the identity of the complainant is requested, and the complainant did not indicate a desire for disclosure or nondisclosure at the time the complaint was filed, the District will resolve these requests on a case-by-case basis. The employee shall consult with a manager or supervisor should this occur.

e. Communications and documentation from the Kitsap Public Prosecuting Attorney's Office that are identified as "attorney-client privileged" shall be considered confidential and shall not be filed as a public record. Confidential communications and documentation shall be filed or stored separately from the main program files.

2. **Examination and Copying of Records. The District must respond to any request for a public record within five business days by producing the record, denying the request, or providing a reasonable estimate of the additional time necessary to respond to the request.**

3. **Employee Acknowledgment.** All employees, contractors, interns, and volunteers will review and sign a Statement of Confidentiality that is retained in his/her personnel file. Violations of this confidentiality policy may result in disciplinary action; willful violations may result in disciplinary action up to and including immediate dismissal. A copy of the District's Statement of Confidentiality form is attached.

4. **Training.** Information about this subsection of the policy/procedure will be discussed during employee orientation and reviewed annually. Training will also be provided to all staff as necessary whenever a material change in this subsection of the policy/procedure is made.

F. Policy Review History

Initial Approval	4/8/03
Revised	1/4/06, 12/1/08, 5/9/14
Reviewed	N/A

KPHD Policy L-2: Protecting Confidentiality of Health Information

Attachment A

State and Federal Law Permits or Requires Disclosure of Protected Health Information Without Patient Authorization Under the Following Conditions:

DISCLOSED TO:	FOR PURPOSE OF:	MAY BE DISCLOSED BY:
Public health authority (local, state or federal)	Preventing or controlling disease or serious harm to people	Member of communicable disease team or designee
Persons who may have been exposed to certain communicable diseases	Preventing or controlling communicable disease	Member of communicable disease team or designee
Child Protective Services	Preventing child abuse or neglect	Any staff member
Adult Protective Services	Preventing abuse or neglect of vulnerable adults	Any staff member
Law enforcement authority	Preventing abuse or serious harm to the individual or other potential victim, when an immediate enforcement activity depends upon disclosure and would be adversely affected by waiting until the individual is able to agree to the disclosure Reporting crimes Other law enforcement purposes including identification and location of people, identification of a crime victim, or about decedents for investigation of deaths	• Health Officer • Member of Management Team • Prosecuting Attorney
Legal authority	Responding to an order of a court, or in response to a subpoena, discovery request, or other lawful process	• Program Manager or designee • Prosecuting Attorney
Coroners, medical examiners and funeral directors	About decedents for investigation of deaths	Vital Records Registrar or any Deputy Registrar
Public Human Resources representatives	Processing worker accident or injury reports and / or Workers' Compensation claims	Any supervisory / management staff
Schools or Healthcare Providers	Schools documenting immunization status or to healthcare provider giving ongoing immunization series to individual	Member of immunization team or designee
Authorized public or private disaster relief entities	For disaster relief purposes	Any supervisory / management staff or designee
Military and authorized federal officials	For national security and intelligence purposes	Health Officer