# 16a. PROTECTION OF Confidential client information

* 1. POLICY TITLE: Protection of Confidential Client Information
		1. Officially Adopted: March 1, 2018
		2. Effective Date: April 1, 2018
		3. Signed:

##  Kelli Nomura, Behavioral Health Organization Administrator

* 1. PURPOSE: To define the principles, expectations and requirements regarding the access, use, and disclosure of individual client information by and to King County Behavioral Health and Recovery Division (BHRD) staff, contracted service providers, and other individuals or organizations. The policy covers all forms of information access and communication including verbal, written, and electronic. This policy does not cover BHRD personnel or payroll records.
	2. RESPONSIBILITIES: BHRD is a health care component of King County, a hybrid entity under the Health Insurance Portability and Accountability Act (HIPAA). Within BHRD, Substance Use Disorder (SUD) Involuntary Treatment Services, and Crisis and Commitment Services (CCS) function as health care providers. Some parts of BHRD function as a health care plan. Some parts of BHRD are neither provider nor plan. BHRD is responsible for ensuring that the use and disclosure of protected health information (PHI) within and by BHRD adheres to all federal and state regulations.
		1. BHRD is exempt from the King County Privacy Policy.
		2. The BHRD Privacy Officer has the lead responsibility within BHRD for the development and implementation of this policy.
			1. The Privacy Officer may designate persons to assist in this function.
			2. All privacy policies and procedures created to meet the requirements of 45 Code of Federal Regulations (CFR) 164 Subpart D Notification in the Case of Breach of Unsecured Protected Health Information, Subpart E Privacy of Individually Identifiable Health Information, and 42 CFR Part 2, Confidentiality of Alcohol and Drug Patient Records shall be documented prior to implementation.
			3. Documentation of all privacy policies and notices shall be retained by the Privacy Officer for six years beyond the date when it was last in effect.
			4. Documentation of breaches of unsecured PHI, risk assessments, and all efforts to address them shall be retained by the Privacy Officer six years from the date of the event.
		3. The BHRD Complaint Officer has the lead responsibility within BHRD for the review of complaints from BHRD staff, clients, and others and the provision of further information about matters covered by the Notices of Privacy Practices. Communications regarding complaints, when required to be in writing, will be retained by the Complaint Officer for six years beyond the date when it was created.
		4. The designated King County Information Technology (KCIT) Security Team representative has the lead responsibility within BHRD for the development and implementation of the policies and procedures required by 45 CFR 164 Subpart C Security Standards for the Protection of Electronic Protected Health Information.
			1. All security policies and procedures created to meet the requirements of HIPAA will be documented prior to implementation.
			2. Documentation of all security policies shall be retained for six years beyond the date when each was last in effect.
			3. Documentation of all security breaches or other security incidents and efforts to address them shall be retained for six years from the date of the event.
		5. BHRD individual staff shall receive training appropriate to their job functions regarding privacy and security policies and procedures. All staff are responsible for complying with these policies and procedures. When a staff person encounters a situation not covered by these policies and procedures, he/she shall consult with the Privacy Officer before taking action.
		6. BHRD contracted providers are responsible for their own compliance with privacy and security laws and regulations.
	3. CONFIDENTIALITY POLICY AND PROCEDURES:
		1. Goals
			1. To protect the privacy, security, integrity, and availability of all PHI created, received, maintained, or transmitted by BHRD.
			2. To ensure that all access, use, disclosure, and requests of individual client information meet all State and Federal requirements.
			3. To protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
		2. Categories of client information
			1. Protected health information (PHI)
				1. For the purposes of this policy, PHI is information that:

Is created or received by a health care provider or health plan;

Relates to the past, present, or future physical or mental health (MH) 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;

Identifies that individual or, with respect to which there is reasonable basis to believe the information can be used to identify the individual; and

Is transmitted or maintained in any form or medium by a provider or health plan.

* + - * 1. Electronic protected health information (ePHI) is that subset of PHI that is transmitted or maintained electronically.
				2. Photographs and other images of a client are considered PHI and are therefore subject to all the protections of PHI.
				3. PHI does not include:

Education records covered by the Family Educational Right and Privacy Act; or

Employment records held by BHRD in its role as an employer.

* + - 1. Designated record set
				1. A designated record set is a group of records maintained by BHRD which includes PHI and is used for the purpose of enrollment, assessment, treatment, billing, care management, or any other decisions about an individual.
				2. See Attachment A, Appendix 1: Designated Record Set.
			2. De-identified information
				1. De-identified individual client information is information wherein the individual is not identified and there is a reasonable basis to believe the information cannot be used to identify the individual. As de-identified information is considered not to be individually identifiable health information, it is no longer PHI.
				2. De-identified individual client information may be used or disclosed without the protections required for identifiable individual client information, as long as any means of re-identifying the information, if such means exists, is kept confidential.
				3. To determine that PHI is not identifiable, BHRD shall:

Remove from the information the identifiers of the individual, relatives, employers, or household members described in 45 CFR 164.514(b); or

Have someone knowledgeable in statistics and scientific principles determine that it is so and document methods and analyses used for the opinion.

* + - * 1. King County Identification (KCID) and authorization numbers shall always be removed for information to be considered de-identified.
				2. BHRD may assign a code or other means to re-identify de-identified information if the code or other means is not used or disclosed for any other purpose.
			1. Limited data set
				1. A limited data set is PHI that excludes the specific identifiers of an individual or his/her relatives, employers, or household members as listed in Attachment A, Appendix 2: Limited Data Set from 45 CFR 164.514(e).
				2. A limited data set may be used or disclosed only for the purpose of research, public health, or health care operations.
			2. Data Sharing Agreements
				1. BHRD may disclose a dataset that is either limited or containing PHI only after an appropriate data sharing agreement has been executed (Appendix 21 Data Sharing Agreement and Appendix 22, Data Sharing Agreement for Limited Data Set). The data sharing agreement shall:

Establish the purpose for which the data will be used;

Confirm that the purpose is research, public health, or health care operations;

Stipulate that the data may not be used for any purpose not designated in the agreement;

Establish who is permitted to use or receive this data;

Establish the safeguards the recipient will have in place to ensure the data is used or disclosed only as agreed;

Require that the recipient report to BHRD any use or disclosure not permitted by the agreement; and

Require that the recipient shall not attempt to identify the clients described by the data set or attempt to contact these individuals.

* + - * 1. Data sharing agreements shall be approved by the Privacy Officer as well as BHRD management.
				2. Data sharing agreements are centrally filed and maintained by the BHRD fiscal staff.
			1. Should BHRD become aware of a violation of a data sharing agreement, the Privacy Officer shall take reasonable steps to end the violation. If such steps are unsuccessful, the Officer may:
				1. Restrict any further disclosure of data to the recipient; or
				2. Report the problem to the Secretary of Health and Human Services.
		1. Consent
			1. Consent is a client’s permission for BHRD to disclose PHI for purposes of treatment, payment, and/or healthcare operations.
			2. Written client consent shall be obtained whenever required by State law or 42 CFR Part 2.
			3. A parent, guardian, or personal representative may consent to the use or disclosure of the client’s information when allowed by law. A guardian or personal representative and, in some cases, a parent shall be asked to provide documentation of the relationship to the client.
			4. To be valid, a consent must be:
				1. Written;
				2. Signed and dated by the client (or, if allowed or required, the parent, guardian, or other legal personal representative);
				3. Identify the information to be disclosed in a specific and meaningful fashion; for 42 CFR Part 2 records, it is permissible to state “All of my substance use disorder records”;
				4. Identify the purpose of the disclosure;
				5. Identify the person to whom the information is to be disclosed (i.e., the recipient); for compliance with 42 CFR part 2, the client can list of any of the following:

The name of the recipient;

The name of the entity that has a treating provider relationship with the individual;

The name of the entity with which the individual does not have a treating provider relationship and which is a third-party payer; and/or

The name of the entity without a treating provider relationship, plus:

Name of individual participants;

Name of entity participants who have treating party relationship; and/or

General designation of individual or entity participant or class of participants who have treating party relationship (e.g., “all my treating providers”);

* + - * 1. Identify the entity that is making the disclosure;
				2. Include an expiration date or an expiration event that relates to the client or the purpose of the use or disclosure. Disclosures regarding persons under the supervision of the Department of Corrections (DOC) shall expire at the end of the term of supervision, unless the client is part of a treatment program that requires the continued exchange of information until the end of the period of treatment; and
				3. Include a statement on revocability.
			1. Consents for children
				1. For children under 13, a parent or guardian must sign all consents for release of information.
				2. For children age 13 and over, the person who must consent is determined by the type of treatment described in the records.

Inpatient SUD treatment records may be released only with the consent of the child and a parent (or guardian).

Inpatient MH treatment records may be released only with the consent of the child.

Outpatient SUD or MH treatment records may be released only with the consent of the child.

* + - 1. To obtain consent, BHRD staff may use a form in Attachment A, Appendix 3: Authorization for Use and Disclosure of Protected Health Information. These forms must be reapproved by the HIPAA Privacy Officer annually.
			2. BHRD staff may revise a form in Attachment A for repetitive use in particular circumstances. Any such forms used shall be approved by the HIPAA Privacy Officer annually.
		1. Authorization
			1. An authorization is a client’s permission for BHRD to use or disclose PHI.
				1. Written client authorization for the use or disclosure of the individual’s health information shall be obtained whenever required by law.
				2. An authorization is not required when the purpose of the use or disclosure is treatment, payment, or health care operations.
				3. There are some situations in which an authorization is not required, as indicated below under Disclosures.
			2. A parent, guardian, or personal representative may authorize the use or disclosure of the client’s information when allowed by law. A guardian or personal representative and, in some cases, a parent shall be asked to provide documentation of the relationship to the client.
			3. A client may not be refused enrollment or treatment if he/she refuses to sign an authorization.
			4. To be valid, an authorization must be:
				1. Written;
				2. Signed and dated by the client (or, if allowed or required, the parent, guardian, or other legal personal representative);
				3. Identify the information to be disclosed in a specific and meaningful fashion; for 42 CFR Part 2 records, it is permissible to state “all of my substance use disorder records”;
				4. Identify the purpose of the use or disclosure. When the authorization is initiated by a client, the client may state “at the request of the individual” rather than describe his/her purpose;
				5. Identify the entity who will use the information or to whom the information is to be disclosed; for compliance with 42 CFR part 2, the client can list of any of the following:

The name of the recipient;

The name of the entity that has a treating provider relationship with the individual;

The name of the entity with which the individual does not have a treating provider relationship and which is a third-party payer; and/or

The name of the entity without a treating provider relationship, plus:

Name of individual participants;

Name of entity participants who have treating party relationship; and/or

General designation of individual or entity participant or class of participants who have treating party relationship (e.g., “all my treating providers”).

* + - * 1. Identify the entity who is using or disclosing the information;
				2. Include an expiration date or an expiration event that relates to the client or the purpose of the use or disclosure, except:

Disclosures regarding persons under the supervision of the DOC shall expire at the end of the term of supervision, unless the client is part of a treatment program that requires the continued exchange of information until the end of the period of treatment; or

The authorization shall expire 90 days after the signing when an authorization permits the disclosure of health care information to a financial institution or an employer of the client for purposes other than payment, unless renewed by the client;

* + - * 1. Include a statement on revocability:

Include how to revoke and exceptions to right to revoke; or

Refer the client to a BHRD Notice of Privacy Practices for more information on revocation;

* + - * 1. Include a statement that information used or disclosed may be subject to redisclosure by the recipient and no longer be protected, with the exception of SUD information that may not redisclosed without specific client consent;
				2. Include a statement that BHRD will not condition treatment, payment, enrollment, or eligibility for benefits on the individual’s providing authorization with the following exception: SUD services will be denied if a client refuses to sign authorization (Attachment A, Appendix 3B: BHRD SUD ROI) for BHRD to receive PHI.
				3. Include a statement that the client is entitled to a copy of the signed authorization.
			1. Authorization for children
				1. For children under 13, a parent or guardian must sign all authorizations for release of information.
				2. For children age 13 and over, the person who must authorize is determined by the type of treatment described in the records.

Inpatient SUD treatment records may be released only with the authorization of the child and a parent (or guardian).

Inpatient MH treatment records may be released only with the authorization of the child.

Outpatient SUD or MH treatment records may be released only with the authorization of the child.

* + - * 1. BHRD may withhold information from a parent or guardian if there is a known history of abuse or neglect of the child by this parent or guardian or there is other reason to believe that giving access to the child’s information will endanger the child.
			1. To obtain authorization, BHRD staff may use a form in Attachment A, Appendix 3: Authorization for Use and Disclosure of Protected Health Information. These forms must be reviewed by the BHRD Privacy Officer annually.
			2. BHRD staff may revise a form in Attachment A for repetitive use in particular circumstances. Any such forms used shall be reviewed by the BHRD Privacy Officer annually.
		1. Minimum necessary
			1. When accessing, using, disclosing, or requesting client PHI without client authorization, the information accessed, used, disclosed, or requested shall be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, except in those circumstances where a deviation from this restriction is legally allowed.
			2. The minimum necessary restriction is not required by law when:
				1. The disclosure is directly to the client or to the personal representative of the client;
				2. The disclosure has been authorized by the client;
				3. The disclosure is to a health care provider for the purpose of providing treatment to the client;
				4. The request is for the purpose of BHRD CCS staff providing treatment to the client;
				5. The use or disclosure is required by law and such use or disclosure is limited to the relevant requirements of such law;
				6. The use or disclosure is required to comply with HIPAA, 42 CFR Part 2; or
				7. The disclosure is to the Secretary of Health and Human Services who is investigating a privacy complaint or conducting an audit of our compliance with privacy requirements.
			3. For access and use without a client’s consent or authorization by BHRD staff:
				1. BHRD shall reasonably safeguard access to PHI by those staff who are not defined as needing such information for their job functions;
				2. For the access and use of PHI without client consent or authorization, BHRD staff are restricted as follows:

Access and use is based on staff’s “need to know” related to his/her role and assigned responsibilities within the division. Access and use may be defined as individual PHI and/or reports developed from individual PHI;

Allowed access and use does not imply the authority to share information with other staff in the division who do not have the approved access;

Access and use of electronic PHI requires the approval by the staff’s supervisor and the Privacy Officer;

A supervisor may access and use information that is accessed or used by staff he/she supervises;

When staff requires information for routine but infrequent use, time-limited access shall be granted;

When staff requires information in order to temporarily assume the responsibilities of another staff, time-limited access shall be granted; and

Access and use is restricted according to Attachment A, Appendix 4: Maximum Potential Access to and Use of PHI by BHRD Staff Without Client Authorization or Consent.

* + - * 1. Procedure for access and use

All BHRD staff job descriptions shall include a description of the PHI the staff may need to access for assigned tasks, if more restricted than that described in Attachment A, Appendix 4.

Access by BHRD staff to electronic PHI requires a completed application to the Privacy Officer. See Attachment A, Appendix 17B: Application for Access to Information Systems BHRD Staff.

Staff who must compile and share PHI as part of his/her job functions shall do so in accordance with established internal BHRD procedures a restricted file maintained on a secure drive.

Staff who compiles PHI as part of his/her job functions and need not share it with others may store it on his/her home drive on the network. However, PHI may not be placed on a workstation’s C drive or on any equipment or media personally owned by a BHRD staff person.

Preferred means for the communication of PHI are phone call, confidential voicemail, encrypted email, secure fax, or mailed/couriered paper, disc, or compact disc.

PHI transmitted by email must use encryption methods approved by the KCIT Security officer. Password protection of an attachment may not be substituted for encryption.

Exceptions to encryption may be allowed when:

Encryption is not available; and

The only PHI are KCID, Authorization number, Docket number (in the case of involuntary commitment court records), and agency ID numbers; and

Additional requirements for PHI in emails:

When receiving an email and any attached documents, these must be immediately removed from the inbox to a personal folder; or “fully” deleted; and

When sending an email, the subject line must include the words “Confidential PHI” to ensure ease of redaction should there be a public disclosure request. The sent email and any attached documents must be immediately removed from the sent items folder to a personal folder, or “fully” deleted.

Encrypted email is not an alternative to using the secure access folders for transmitting/receiving “large” files containing individually identifiable information and/or PHI.

No PHI may be included in text messages, instant messaging or in net meeting transmissions.

* + - 1. For access and use of PHI without a client’s authorization or consent by King County staff outside of BHRD
				1. The director and staff of the Department of Community and Human Services (DCHS), who are outside BHRD, may access or use the minimum necessary PHI for the purpose of health care operations. Such requests shall first be approved by the Privacy Officer in consultation with the BHRD director or assistant director(s).
				2. Staff of other county departments or offices may not access or use PHI without a business associate agreement or memorandum of understanding.
				3. Persons on the Behavioral Health Advisory Board may not access or use identified PHI.
			2. For disclosure by BHRD staff without a client’s authorization, the Privacy Officer shall ensure that the minimum necessary restriction is applied whenever required by law.
				1. The minimum necessary restriction for routine releases

The Privacy Officer shall review for approval each routine and recurring disclosure of PHI to ensure it meets the minimum necessary restriction, when that restriction applies.

Once a routine release is approved by the Privacy Officer, the disclosure may recur as needed without additional approval unless the disclosure changes as to recipient, purpose, content, or any other aspect of the disclosure.

See Attachment A, Appendix 5: Routine Disclosures of PHI by BHRD Staff without Client Consent or Authorization for a list of routine disclosures. Disclosures for treatment, payment or healthcare operations do not need to be tracked for the purpose of an accounting.

* + - * 1. The minimum necessary restriction for non-routine releases

The Privacy Officer shall review each non-routine request for disclosure of PHI to ensure it meets the minimum necessary restriction.

When the request for information comes from the following persons or entities, the specifically requested information may be assumed, at the discretion of the Privacy Officer, to be the minimum necessary:

Public officials who may receive PHI without client authorization, when the official represents that the information requested is the minimum necessary for the stated purpose;

Another covered entity;

A staff person of a business associate of another covered entity who is providing professional services to the covered entity, when the person represents that the information requested is the minimum necessary for the stated purpose; or

A researcher whose research has been approved by the BHRD Evaluation and Research Committee.

For all other non-routine releases, the following guidelines apply:

A whole clinical record shall not be used or disclosed unless the entire record is specifically justified as the amount that is reasonably necessary for the stated purpose;

A limited data set may be considered the minimum necessary information for disclosure when there is a limited data set sharing agreement (Attachment A, Appendix 22: Data Use Agreement for Limited Data Set) and the data are for research, public health, or health care operations;

All elements in an electronic transaction under 45 CFR Part 162 are considered necessary when one element in an electronic transaction is required; and

All contractually required disclosure of individual client information is considered the “minimum necessary.”

Some non-routine releases will need to be covered by a data-sharing agreement.

* + - 1. When BHRD staff request PHI of another provider, plan, or any other source without a client’s authorization, the individual staff shall ensure that the minimum necessary restriction is applied whenever required by law.

Guidelines for the determination of minimum necessary for the request for PHI are as follows:

* + - * 1. A whole clinical record shall not be requested unless the entire record is specifically justified as the amount that is reasonably necessary for the stated purpose. A whole clinical record may be requested for use during an on-site audit;
				2. A limited data set may be considered the minimum necessary information for request when there is a data use agreement and the data are for research, public health, or health care operations;
				3. All elements in an electronic transaction under 45 CFR Part 162 are considered necessary when one element in an electronic transaction is required; and
				4. All contractually required requests of PHI are considered the “minimum necessary.”
		1. Disclosures
			1. All disclosures of PHI by BHRD staff to persons, who are not approved for its access and use, as described above, shall occur according to State and Federal law.
			2. Consent or authorization is required for the disclosure of SUD PHI, unless there is a medical emergency as defined in 42 CFR Part 2.
			3. Consent or authorization is not required for the disclosure of MH PHI:
				1. To the individual;
				2. To the legal personal representative of the individual;
				3. To the parent, guardian, or other person acting in loco parentis, as allowed by law;
				4. To a health care provider or entity for the purpose of treatment, payment, or health care operations:

For the purpose of treatment, the fact of enrollment in the Behavioral Health Plan, the identity of the treatment agency, and the identity of the case manager may be released without authorization or consent to the health care providers or entities. Additional information may be released in certain situations. See Attachment A, Appendix 6: Redisclosure of Information for Enrolled Clients; and

Other disclosures for the purpose of treatment may require a consent;

* + - * 1. To a public health authority for the purpose of preventing or controlling disease, injury, or disability;
				2. To a public authority authorized by law to receive reports of child or vulnerable adult abuse or neglect:

To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirement of such law;

To the extent that the disclosure is authorized by law and BHRD feels the disclosure is necessary to prevent serious harm to the individual or other potential victims;

When such a disclosure is made, no information (e.g., the identity of the caller) may be given that indicates the client is known to have a past or present SUD, should this be the case for elder abuse or neglect; or

When a disclosure has been made, the BHRD staff person making the disclosure must inform the client (or parent, guardian, or personal representative) unless it is determined by a BHRD licensed professional that:

Informing the client would place him/her at risk of serious harm; or

Informing the parent, guardian, or personal representative would place the client at further risk;

* + - * 1. To the Food and Drug Administration (FDA) for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity;
				2. To a health oversight agency, as authorized by law;
				3. To a health oversight agency and another entity investigating a claim of public benefits not related to health;
				4. To an individual or organization in response to a lawful court order (court orders and subpoenas should be referred to legal review);
				5. To law enforcement, and only when allowed or required by law, this includes:

Reports of child or vulnerable adult abuse, as noted above;

Disclosures in response to a lawful court order, as noted above;

Disclosures made in the event of a crisis or emergent situation, for the purpose of averting a serious threat to public health or safety; or

Reporting a crime on BHRD premises;

* + - * 1. To the target of a threat, when the person is reasonably able to prevent or lessen the threat;
				2. To correctional institutions as necessary for treatment or for the protection of the health and safety of others, only if the client is an inmate residing in an institution;
				3. To the State Department of Corrections (DOC):

For the purposes of completing presentence investigations or risk assessment reports, supervision of an incarcerated offender or offender under supervision in the community, planning for and provision of supervision of an offender, or assessment of an offender’s risk to the community; and

For the purpose of containing an emergency or locating an offender, in which case information related to MH services delivered to the offender and, if known, information regarding where the offender is likely to be found. Information released in response to an oral request is limited to known whereabouts of the offender and the fact of current receipt of services;

* + - * 1. To the Federal government for specialized government functions;
				2. To researchers for research activities approved by the BHRD Evaluation and Research Committee;
				3. To a coroner, medical examiner, or funeral director; or
				4. Incidental to a use or disclosure that is legally allowed.
			1. In addition to the above, disclosures without authorization may be made in a disaster, if the following conditions are met:
				1. If the client is present, he/she is given an opportunity to object, or
				2. If the client is not present or is incapacitated, BHRD staff determine that the disclosure is in the best interests of the client or the disclosure is necessary to allow an authorized disaster relief entity to perform its function.
			2. Disclosures made with or without authorization are not considered a violation if the disclosure is made by a whistleblower who:
				1. Believes in good faith that BHRD has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by BHRD potentially endangers one or more clients, staff persons, or the public, and
				2. The disclosure is made to a health oversight agency or public health authority authorized by law to oversee BHRD or to the whistleblower’s own attorney.
			3. Disclosures to the following are required, whether or not an authorization is obtained:
				1. To the person;
				2. To the person’s parent, guardian, or legal personal representative (when only that person may consent to the client’s care);
				3. To the Secretary of Health and Human Services; or
				4. To a person or organization, pursuant to a lawful court order.
			4. Routine disclosures permitted by law shall only follow the approval of the Privacy Officer. See Attachment A, Appendix 5 for approved routine disclosures.
			5. Non-routine disclosures permitted by law shall be made on case-by-case basis, based on a decision made in consultation with the Privacy Officer. See Attachment A, Appendix 7: Request for Client Information without Authorization.
			6. Procedure for disclosures of PHI
				1. Prior to the disclosure of any PHI, the BHRD staff who is being asked to disclose information shall ask the Privacy Officer to determine the following:

That the disclosure meets all requirements for consent or authorization:

If a consent or authorization is required, the Privacy Officer shall further determine that the document is valid (Attachment A, Appendix 8: Form for Invalid Authorizations); and

If a person requesting information claims that consent or authorization is not required, he/she must cite the legal authority by which he/she can receive PHI without client permission;

That the requester’s identity is confirmed. Guidelines for verification are:

Client hand-delivers the authorization and presents a picture identification card confirming his/her identity;

The signature on the consent or authorization can be matched to a client signature on file;

The consent/authorization form or any accompanying cover letter is on recognizable letterhead; or

Notarized signature on the authorization;

That no business associate or data sharing agreement is required; and

That minimum necessary standards are met.

* + - * 1. When the above requirements for disclosure are met, the PHI is prepared for disclosure.
				2. The BHRD staff person shall then disclose the information. For disclosures to a client, the client may request receiving confidential communications by alternative means or at alternative locations, if he/she clearly states that the disclosure could endanger him/her. See Attachment A, Appendix 9: Request to Communicate by Alternate Means or at an Alternate Location.
				3. If the disclosure is made on the basis of a BHRD authorization (Attachment A, Appendices 3, 3A, 3C, 3D, 3E, or 3F) and signed by the client, the client is given a copy of the authorization.
				4. Documentation of a disclosure shall occur in all instances whereby the disclosure would need to be reported in a client-requested accounting. See Attachment A, Appendix 10: Log of Disclosures without Client Consent or Authorization.
				5. Documentation of a disclosure shall occur for all disclosures by CCS except disclosures to third-party payors (Revised Code of Washington [RCW] 70.02.020).
				6. Documentation of disclosures not required in an accounting and not required by staff of CCS may occur.
				7. Any documentation of a disclosure shall include the following:

For non-routine disclosures of PHI of an individual client, the BHRD staff making the disclosure shall document:

The date of the disclosure;

The staff making the disclosure;

The recipient of the PHI;

The means of disclosure (e.g., phone, mail, email, fax);

A description of the information disclosed;

The purpose of the disclosure; and

The authority allowing the disclosure;

For those disclosures required to be logged on Attachment A, Appendix 10, the log suffices for the documentation of that disclosure; and

For routine disclosures with consent or authorization:

Review the consent or authorization with the Privacy Officer or site designee to determine that all of the required fields are present; and

For Offender Re-entry Community Safety Program (ORCSP) consents, compare with the required elements and determine that all of the blanks have been completed. Take any questions to the Privacy Officer.

* + - * 1. For clients with a paper record kept at BHRD, the documentation of a disclosure shall be kept in this record. For clients without a paper record, the documentation shall be kept in a combined file.
				2. When the Privacy Officer approves only part of a request for disclosure, only the information approved shall be disclosed. When this occurs, the Privacy Officer shall place in the client record an explanation for the partial approval.
				3. When an authorization for disclosure is denied, the authorization is returned to the requester with an explanation for the denial. A copy of the authorization and the denial letter is filed in the client file.
			1. BHRD staff that do not use or access PHI as defined under the Minimum Necessary section above may not access PHI without a client consent or authorization.
		1. Redisclosure of Substance Use Disorder (SUD) Information
			1. Redisclosure occurs when individual client information, disclosed to an individual or organization with or without authorization, is disclosed to another individual or organization.
			2. Redisclosure of individual client SUD information is prohibited by 42 CFR Part 2 except with a proper consent or authorization.
			3. All disclosures must be stamped: “This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.”
		2. Revocations of consents or authorizations for disclosure
			1. When a request for a consent or authorization revocation is received, the revocation request is forwarded to the Privacy Officer who shall do the following:
				1. Verify the identity of the requester by comparing the signature on the revocation request with the original consent or authorization;
				2. Write “VOID” in large red letters across the original consent or authorization with the date and initials of the staff; and
				3. File the revocation request with the original consent or authorization.
			2. A client may use Attachment A, Appendix 11: Request to Revoke Consents to request a revocation.
			3. When a request for a disclosure of PHI is received referencing a previously received consent or authorization, the BHRD staff receiving the request shall ask the Privacy Officer to determine that the consent or authorization remains valid. Information may be disclosed only if the previously received consent or authorization has not been revoked and has not expired. The procedure is the same as for other disclosures.
		3. Privacy and Security Committee
			1. The Privacy and Security Committee:
				1. Develops and implements privacy and security policies and procedures;
				2. Reviews and modifies as needed policies and procedures related to electronic technology as technology changes;
				3. Monitors adherence to procedures; and
				4. Reviews and approves training curriculum for new staff at point of hire as well as curriculum for ongoing training to current staff.
			2. The committee is chaired by the Privacy Officer. Both the Complaint and Security Officers are committee members. Other BHRD staff may be appointed to serve on this committee.
		4. Business Associates
			1. A business associate relationship exists with an individual or business when that individual or business uses or discloses PHI in performing a function or activity on behalf of BHRD.
			2. A business associate that is internal to the County shall enter into a memorandum of understanding, which clearly states the necessary privacy and security protections for PHI. The memorandum of understanding must meet the requirements of a business associate agreement.
			3. When the purpose of the business association is other than the provision of treatment, BHRD shall require that business associates enter into a business associate contract.
			4. Should BHRD staff become aware of a material breach or violation of the business associate’s obligation under the contract, BHRD shall provide an opportunity for the business associate to cure the breach or end the violation. If the business associate does not cure the breach or end the violation within the time specified by BHRD, the business associate contract shall be terminated.
			5. Establishing business associate arrangements
				1. All staff shall report to the Privacy Officer any time they are considering the development of a business relationship with another individual or organization that will collect or use PHI to conduct BHRD-related work, to determine if a business associate agreement is required.
				2. When developing a business associate agreement, staff shall ensure that the contract or agreement:

Defines what, if any, PHI will be collected and/or used to conduct BHRD-related work;

Utilizes the King County Agency Services Contract boilerplate, or the approved Business Associate Agreement template (Appendix 20):

The contract boilerplate or business associate agreement address requirements to:

Use appropriate safeguards and comply, where applicable, with subpart C of the Security Rule, with respect to electronic protected information, to prevent use or disclosure of the information other than as provided for by its contract or business associate agreement;

Report breaches of unsecured PHI as required by the data-breach-reporting rule;

Obtain written agreements with subcontractors who create, receive or maintain ePHI to comply with Security Rule; and

Comply with the Privacy Rule to the extent that the business associate is to carry out a covered entity’s obligation under the Privacy Rule (for example, providing individuals with access to health information);

Is not modified or changed without the approval of the Privacy Officer and counsel;

Is subject to on-site audits; and

Allows for the Privacy and Security Officers to review the associate’s privacy and security policies and/or other supporting information on request.

* + - 1. Requests that a business associate disclose PHI
				1. Should the business associate collect PHI that is used in the performance of its work for the division but is not submitted to the division, the business associate is responsible for complying with all privacy and security practices related to PHI disclosure.
				2. Should the business associate have submitted all PHI collected to the division, it may refer disclosure requests to the division.
		1. Client rights related to PHI
			1. Notice
				1. Each client for whom BHRD receives PHI in our role as plan or provider shall receive a Notice of Privacy Practices which describes:

How we access, use, and disclose PHI without client consent or authorization;

How we protect client privacy; and

Client privacy rights and how to exercise them.

* + - * 1. For children under age 13 and others legally unable to consent to treatment, the notice shall be given to the client’s parent, guardian, or legal personal representative.
				2. BHRD shall not use or disclose individual client information in a manner inconsistent with the notice.
				3. In most cases, a Notice shall be given to each client prior to receiving services.
				4. The Notices shall contain all elements defined in 45 CFR Part 164.520 and shall include a statement that we reserve the right to make a change in how BHRD handles PHI.
				5. Whenever BHRD plans to change how it handles PHI such that the Notices shall no longer be accurate, an updated version shall be developed and distributed as required by law prior to the planned change.
				6. Only the Privacy Officer may change notices.
				7. All notices, including those currently in effect and those in effect in the past, shall be kept on file by the Privacy Officer.
				8. Procedures for the distribution of Notices:

BHRD staff shall distribute the BHRD Behavioral Health Plan Notice of Privacy Practices with the Notices of Service Authorization or Service Change as specified in Section 03, Attachments B, C, and E. When services are initially authorized; and

Annually when authorized to have services continued.

When BHRD has made a material change to the Notice of Privacy Practices, the change must be prominently posted, or a copy of the revised Notice on the website by the effective date of the change; and

Provide a copy of the revised Notice, or information about the change and how to request a copy of the revised Notice, in the next annual mailing.

The BHRD Behavioral Health Plan Notice of Privacy Practices shall be distributed by BHRD staff to clients authorized for community psychiatric inpatient care.

Crisis and Commitment Services (CCS) shall:

## Distribute the BHRD CCS Notice of Privacy Practices to clients at the time of the evaluation. Should a client be assessed on more than one occasion, he/she shall receive a notice at the start of each assessment;

Document the date the notice was received by the client; and

Obtain a written acknowledgment of receipt of the notice by the client or the good faith effort to obtain the acknowledgment including why it was not obtained (e.g., “client refused”).

* + - * 1. Posting on website

A copy of BHRD, CCS, and CDITS Notice of Privacy Practices shall be posted on the BHRD website.

Each subsequent revised version shall be posted with the dates in effect clearly specified.

Each version (identified by effective date) shall be posted no later than the date on which it becomes effective.

* + - 1. Requests to copy or inspect under HIPAA
				1. A client may request to inspect or copy his/her own designated record set.
				2. For copies, the client may be assessed a fee of 15 cents a page.
				3. To request to inspect or copy one’s own confidential information, a client must make the request in writing.

The client may use a fully completed Attachment A, Appendix 3 for this purpose.

The client may submit instead a request containing all the elements in Attachment A, Appendix 3.

* + - * 1. The client shall submit the request to the Privacy Officer or designee, who shall determine if there is any information which shall not be released under the law.
				2. Within 15 working days, the Privacy Officer shall respond to the request to copy or inspect either by fulfilling the request or explaining to the client why the request cannot be granted.
				3. BHRD may deny the request if the information was compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding. Such a denial may not be appealed.
				4. BHRD may also deny the request when a licensed mental health professional (MHP) has determined that:

The access requested is reasonably likely to endanger the life or safety of the client or another person;

The access requested is likely to cause harm to another person referenced in the records; and

The access is requested by the client’s personal representative and the access requested is likely to cause harm to the client or another person.

## These denials may be appealed.

* + - * 1. An appeal request shall be made in writing.
				2. The appeal is reviewed by a licensed health care professional who did not participate in the original decision to deny.
				3. BHRD shall comply with the appeal decision.
				4. BHRD shall act on an appeal request within 30 days. The response shall be in writing unless the client has requested an alternative format.
			1. Requests to amend
				1. To request to amend one’s own PHI, a client shall make a request in writing.

The client may use a fully completed Attachment A, Appendix 12: Request to Amend or Correct Protected Health Information for this purpose.

The client may submit instead a written request containing all the elements in Attachment A, Appendix 12.

* + - * 1. The client submits the request to the Privacy Officer or designee, who shall forward the request to an appropriate BHRD licensed health care professional.
				2. BHRD may deny the request when a licensed health professional has determined that:

The information is accurate and complete;

BHRD was not the originator of the information, unless the originator is no longer available to directly act on the request;

The information the client amended is not part of the designated record set; or

The information was compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding.

* + - * 1. BHRD shall act on the client’s request ten working days after receipt of the request.
				2. If the request is approved, BHRD shall:

Inform the client that the amendment has been approved. The response shall be in writing unless the client has requested an alternative format;

Identify the information in the designated record set that is affected by the amendment and either append the information or provide a link to the amendment; and

Inform the entities with which BHRD has disclosed this information that the information has been amended;

* + - * 1. If the request is denied, BHRD shall provide the client with a written denial that contains:

The basis for the denial;

The individual’s right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

A statement that, if the individual does not submit a statement of disagreement, the individual may request that BHRD provide the individual’s request for amendment and the denial with any future disclosures of the information that is the subject of the amendment; and

A description of how the client may complain to BHRD or to the Secretary of Health and Human Services, with specific names (or titles) and phone numbers.

* + - 1. Requests to restrict
				1. A client may request that BHRD restrict the access, use, and disclosure of his/her PHI. To do so, a client shall make a request in writing as follows:

The client may use Attachment A, Appendix 13: Request to Restrict Access, Use, or Disclosure of Protected Health Information for this purpose; or

The client may instead submit a written request containing all elements in Attachment A, Appendix 13.

* + - * 1. The client submits the request to the Privacy Officer or designee.
				2. The Complaint Officer shall respond to the request within 30 days. The response shall be in writing unless the client has requested an alternative format.
				3. BHRD is not required to agree to requested restrictions. However, when BHRD does agree, the restriction shall be followed.
			1. Requests for an accounting
				1. A client may request an accounting of disclosures of his/her PHI made by BHRD in the six years prior to the date on which the accounting is requested, except for disclosures:

To carry out treatment, payment, and health care operations;

To the client;

Incidental to a use or disclosure otherwise permitted or required;

Pursuant to an authorization;

To persons caring for the client in a disaster;

For national security or intelligence purposes allowed by law;

To correctional institutions or law enforcement officials as allowed by law;

As part of a limited data set as defined above; or

That occurred prior to April 14, 2003.

* + - * 1. An accounting shall consist of the following information about each disclosure (Attachment A, Appendix 10):

The date of the disclosure;

The staff person making the disclosure;

The recipient of the PHI;

The means of disclosure (e.g., phone, mail, email, fax);

A description of the information disclosed;

The purpose of the disclosure; and

The authority allowing the disclosure.

* + - * 1. To request an accounting of the disclosures of one’s PHI, a client must make a request in writing.

The client may use a fully completed Attachment A, Appendix 14: Request for an Accounting of Disclosures for this purpose.

The client may submit instead a written request containing all the elements in Attachment A, Appendix 14.

* + - * 1. The client submits the request to the Privacy Officer or designee.
				2. The Complaint Officer shall respond within 60 days.
			1. Complaints about privacy
				1. A client may lodge a complaint about:

BHRD compliance with HIPAA;

BHRD privacy policies and procedures; or

BHRD staff compliance with BHRD privacy policies and procedures.

* + - * 1. Complaints about privacy must be in writing, with the signature of the complainant, contact information for the complainant, and the date of the complaint.
				2. The Complaint Officer shall respond to all complaints with:

A written acknowledgment of receipt of the complaint, within five days of receipt;

A review and investigation of the complaint;

A plan of action to prevent any recurrences of problems revealed by the review and investigation; and

A final written response to the complainant regarding the disposition of the complaint.

* + - * 1. In both the acknowledgement letter and the final response, the complainant shall be informed of his/her right to complain directly to the Secretary of Health and Human Services and how to do so.
				2. The Complaint Officer shall keep a record of each complaint and its disposition.
				3. The Complaint Officer shall report all complaints about a breach of privacy to the Privacy Officer.
				4. The Complaint Officer shall prepare a summary of privacy complaints periodically for review by the Privacy Officer and BHRD administrative staff.
				5. Complaint summaries shall be used to improve personnel training and policies and procedures.
			1. BHRD staff shall not retaliate against any client exercising any right regarding his/her PHI allowed under these policies and procedures.
			2. For any mailed correspondence with clients, BHRD staff shall use envelopes that do not reference mental illness or substance use.
		1. Personnel
			1. All BHRD staff, volunteers, and student interns receive a copy of the current BHRD confidentiality and security policies and procedures, appropriate to their role, and complete Attachment A, Appendix 15: Oath of Confidentiality within 30 days of their commencement of work with the county, except under exceptional circumstances.
			2. The completed Oaths shall be forwarded to DCHS Human Resources and maintained in each person’s personnel file.
			3. Initial training must be completed within a reasonable timeframe after a new staff starts employment.
			4. Additional training or reminders shall be provided to staff, volunteers, and student interns:
				1. At least annually;
				2. Whenever a need becomes apparent; or
				3. Whenever significant changes are made to these policies or procedures.

When significant changes have occurred, only those staff whose functions are affected need be retained.

The retraining occurs within 30 days after the change becomes effective.

* + - 1. The Privacy Officer is responsible to review content and timely occurrence of trainings.
			2. Records of trainings shall be kept for at least six years, documenting content and attendees.
				1. The Privacy Officer shall maintain documentation of trainings, and
				2. A log of staff completing training is available.
			3. Staff may report to the Complaint Officer:
				1. Any concern with BHRD confidentiality and security policies and procedures; or
				2. Any failure by BHRD staff, volunteers, student interns, or persons outside BHRD to follow the BHRD confidentiality and security policies and procedures.
			4. BHRD shall not retaliate against staff making a complaint or report to the Complaint Officer.
			5. Staff Sanctions
				1. Sanction of staff may occur for:

Failure to attend required trainings; or

Failure to abide by BHRD confidentiality and security policies and procedures.

* + - * 1. Sanction of staff may not occur for:

Whistle blowing, as allowed by law;

Reporting to law enforcement, as allowed by law, when staff have been victims of crime;

Making a complaint to a supervisor or the Complaint Officer;

Complaining to the Secretary of Health and Human Services;

Participating in an investigation, compliance review, proceeding, or hearing; or

Opposing any practice that the staff has a good faith belief is illegal, if the manner of opposition is reasonable.

* + - 1. The staff person’s supervisor, and DCHS Human Resources staff, in
			 consultation with the Privacy Officer and in accordance with current King
			 County personnel policies, shall determine appropriate sanctions. Depending
			 on the circumstances, sanctioning may consist of:
				1. Required retraining;
				2. Formal warning that the staff may lose the privilege of accessing and using confidential information;
				3. Loss of the privilege of accessing and using confidential information; or
				4. Suspension or termination of employment.
			2. The Privacy Officer shall provide documentation of violations to DCHS
			 Human Resources to be placed in the staff’s personnel file.
			3. DCHS Human Resources shall maintain centralized documentation of all
			 sanctions.
			4. Civil penalties may be assessed by the Secretary.
			5. Criminal penalties may be pursued by the Federal Department of Justice.
		1. Data Requests for Healthcare Operations, Evaluation and Research
			1. All data requests for evaluation and/or research activities will be reviewed and given consideration.
				1. Data requests from external sources will be processed as specified in the BHRD Evaluation and Research Committee policies and procedures.
				2. Requests for data from external sources will be processed as specified in BHRD Internal policies and procedures.
			2. Data for evaluation and research that requires disclosure outside of BHRD is based on a written agreement (i.e., business associate, data sharing or memorandum of agreement) that has been approved by the Privacy Officer.
			3. The Privacy Officer may consult with the BHRD Privacy and Security Committee or Management prior to approving data sharing agreement.
			4. A data request application is required when data from a source external to BHRD is needed for healthcare operations, i.e., care coordination, quality improvement activities or program evaluation and/or research studies. The completed application will be reviewed and approved by the Privacy Officer and Management prior to submitting the request to the external source.
		2. Marketing

As BHRD shall not engage in marketing practices, no access, use, or disclosure of PHI will occur for this purpose.

* + 1. Compliance reviews

The Secretary of Health and Human Services may conduct reviews to determine if BHRD is complying with Federal privacy and security laws.

* + - 1. At the request of the Secretary, BHRD shall provide all documentation demonstrating compliance in our policies, procedures, and practices.
			2. Should a finding occur that BHRD is not in compliance, the Privacy Officer shall develop a corrective action plan and implement the needed changes.
		1. Security of PHI on paper
			1. Clinical or care management records:
				1. Shall reside in a secure designated location at each of the following sites: the Chinook Building, Emergency Services Patrol office, and Harborview Medical Center Psychiatric Emergency Services (PES);
				2. Shall include portions of the designated record set as well as information that is not part of the designated record set;
				3. Shall include both MH and SUD PHI, filed according to the source of the information so that information from MH providers is separated from information from SUD providers;
				4. Shall include all paper files the division has on the client or reference the location of additional paper files; and
				5. Shall be locked at the end of the working day, with access by designated staff only. (Services that operate around the clock, such as CCS, may develop other criteria for when paper files need to be locked up.)
			2. Fax (facsimile) machines
				1. PHI shall be received or sent only on fax machines placed in secure locations.
				2. Unless it is a regularly used number, staff shall verify the accuracy of a fax number prior to transmission.

When the fax number has been recently received from a reliable source, it can be considered verified.

Other fax numbers can be verified by calling the recipient or faxing the recipient a verification request (which contains no PHI).

* + - 1. Shredding

Paper documents to be shredded shall be kept in secured designated areas.

* + - 1. When a breach of PHI (including ePHI) reported to have occurred, the Privacy and/or Security Officer shall investigate the incident and employ appropriate timely actions as established by internal KCIT procedure. Additionally, for breaches of ePHI, the requirements of Chapter 42.56 RCW shall be followed.
				1. The Privacy and/or Security Officer shall make recommendations to the Privacy and Security Committee, and BHRD Management Team, as needed, to prevent future breaches of PHI.
				2. When applicable for persons or organizations outside BHRD, sanctions for reportable breaches may include termination of access privileges, termination of contracts, fines, and/or criminal prosecution.
	1. SECURITY POLICY AND PROCEDURES:

The HIPAA Security Rule specifically focuses on the safeguarding of ePHI. The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of ePHI. All covered entities under HIPAA shall comply with the HIPAA Security Rule, which established a set of security standards for securing ePHI.

Each security measure of the HIPAA Security Rule can be categorized as being an administrative, physical, or technical safeguard.

**Administrative Safeguards**

* + 1. Security Management Process (§164.308(a)(1))

**HIPAA Standard**: *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

* + - 1. The Privacy and Security Committee shall periodically identify all database applications that access ePHI.
			2. In collaboration with the KCIT Security Team, periodic assessments of internal risk will be conducted.
			3. KCIT shall use software tools to help identify security violations.
		1. Assigned Security Responsibility (§164.308(a)(2)

**HIPAA Standard**: *Identify the security official who is responsible for the development and implementation of the policies and procedures required.*

* + - 1. The BHRD Security Officer will be designated by the King County Chief Information Security and Privacy Officer.
			2. Security Officer responsibilities are described in part 3.5 of this section.
		1. Workforce Security

**HIPAA Standard**: *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*

* + - 1. Access to ePHI for BHRD staff is determined by the minimum necessary standard in Attachment A, Appendix 4: Maximum Potential Access to and Use of PHI by BHRD Staff without Client Authorization or Consent, supervisor approval, professional credentials, job description, and assigned job tasks.
			2. Access to ePHI for persons who are not BHRD staff as follows:
				1. No persons who are not BHRD staff may access SUD PHI without the client’s consent.
				2. Persons who are not BHRD staff may access ePHI as follows:

At provider agencies under contract to BHRD to provide behavioral health services, the following employees may view ePHI as allowed by Federal rules and regulations: MHPs, chemical dependency professionals (CDP), chemical dependency professional trainees (CDPT), or registered counselors for the purpose of providing treatment, or other personnel for the purpose of performing administrative functions such as audits, information management, or program evaluation. Specific access is defined in Attachment A, Appendix 16:, Disclosure of the Minimum Necessary Electronic PHI to Providers without Client Authorization or Consent

* + - 1. Termination of access to ePHI
				1. Electronic client information access expires when a person terminates employment, undergoes a change in job responsibilities such that he/she no longer needs that access, and/or loses access privileges due to a failure to adhere to BHRD privacy and security policies.
				2. Supervisors shall notify the Privacy Officer or designee at least five days before such a change occurs so access may be terminated or revised.
		1. Information Access Management (§164.308(a)(4))

**HIPAA Standard**: *Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.*

* + - 1. Persons who require access to electronic client information shall apply in writing.
				1. The person completes the application in Attachment A, Appendices 17A and 17B.
				2. The application is reviewed and, if appropriate, approved by the person’s immediate supervisor and, if applicable, the site supervisor.
				3. The application is submitted to BHRD support staff, who log the request into the electronic access request (EAR) database, check for initials and appropriate signatures.
				4. Support staff will forward the application to the Privacy Officer or designee for approval.
				5. The Privacy Officer or designee will complete the approval process and upon approval, a help desk ticket is created. The Privacy Officer submits the help desk ticket to the KCIT Service Center for processing.
				6. The Privacy Officer signs and dates the application, and returns the completed form to the BHRD support staff for processing and filing.
				7. KCIT Service Center completes the request for electronic access and a resolved help desk ticket is sent to the Privacy Officer. This resolved ticket is automatically forwarded to the BHRD support staff to notify first time users and file the completed applications.
			2. State databases
				1. For application to access the Department of Social and Health Services (DSHS) Mental Health Division (MHD) Intranet, staff completes Attachment A, Appendix 19 and forward it to IS staff for the appropriate signature. The IS staff will then forward to support staff for processing. The MHD Intranet requires each user to change his/her password every 60 days. DSHS approves each individual application.
				2. For application to access the State DBHR’s TARGET database, BHRD staff obtains the application from the designated support staff person. DBHR approves each individual application.
				3. For application to access the DSHS ProviderOne web portal, staff completes an EAR form, entering “ProviderOne” in the section titled “Other.” Supervisor and Privacy Officer approve each application.
				4. For application to access the DSHS Research and Data Analysis PRISM system, staff complete Appendix 23, and forward it to the BHRD Privacy Officer for approval and processing.
			3. Renewal of access privileges for BHRD applications
				1. Electronic client information access shall be renewed at least annually.
				2. Notification for renewal will be sent to each staff 30 days prior to expiration.
				3. To renew access, all procedures in part 5.4.1 of this section are repeated.
			4. Termination of access privileges
				1. To terminate access, Attachment A, Appendix 17B: Application for Access to Information Systems is submitted by the employee or his/her supervisor to the Privacy Officer, who will process the termination.
				2. Termination of access is tracked in the EAR database.
		1. Security Awareness and Training (§164.308(a)(5))

**HIPAA Standard**: *Implement security awareness and training program for all members of its workforce (including management).*

* + - 1. Policies and procedures for the training of all staff on privacy and security are found in part 4.12 of this section.
			2. BHRD staff shall receive technical training as needed to implement the technical security safeguards.
		1. Security Incident Procedures (§164.308(a)(6))

**HIPAA Standard**: *Implement policies and procedures to address security incidents.*

A security breach for ePHI shall be addressed as described in part 4.16.4 of this section and in accordance with KCIT Security and Privacy policies as adopted by the County and approved by the County Chief Information Security Officer (available at <http://kcweb.metrokc.gov/oirm/policies.aspx>).

* + 1. Contingency Plan (§164.308(a)(7))

**HIPAA Standard**: *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*

* + - 1. Data Backup
				1. KCIT Backup Services shall perform daily backups of the network and database servers. Weekly full backups of the network and database servers are kept off-site for one year and the tapes encrypted using National Institute Standards and Technology (NIST) standards.
				2. The most recent backup tapes shall be transported to an off-site facility at least three times per week.
			2. Disaster recovery plan for ePHI
				1. The BHRD Emergency/Disaster Recovery Plan is found in the BHRD Internal Policy Manual.
				2. Data and system recovery backup tapes shall be tested at least annually to ensure backup media and hardware integrity.
			3. Emergency mode operations
				1. CCS is the critical BHRD business unit.
				2. When ePHI is not available for CCS use, paper files shall be used.
		1. Evaluation (§164.308(a)(8))

**HIPAA Standard**: *Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.*

* + - 1. The Privacy and Security Committee shall conduct an annual review of the Confidentiality and Security policies and procedures in response to environmental or operational changes affecting the security of ePHI.
			2. The review shall use a standardized risk assessment tool developed in conjunction with the King County Designated Health Care Components (DHCC) workgroup.
		1. Business Associate Agreements and Other Arrangements (§163.308(b)(1))

**HIPAA Standard**: *A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.*

* + - 1. Each BHRD contract shall contain boilerplate language incorporating the requirements for business associates described in part 4.10 of this section.
			2. Contractors are required to pass down these requirements to any subcontractors.
			3. Boilerplate language shall be updated whenever changes in laws require it.

**Physical Safeguards**

* + 1. Facility Access Controls

**HIPAA Standard**: *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. (Note: Supports the Information Access Management Administrative Standard and the Access Control Technical Standard.)*

* + - 1. Physical security shall be maintained at all sites by the use of locked doors (either combination or keyed locks) where feasible.
				1. Key distribution shall be monitored to ensure physical security.

Keys shall be given to staff only when required to fulfill a job responsibility.

Keys shall be retrieved from staff whenever that person leaves BHRD employment or job responsibilities no longer require key access.

Keys shall be changed as often as necessary to ensure physical security.

Detailed procedures for the distribution of keys are found in the BHRD Internal Policy Manual and DCHS policies.

* + - * 1. Electronic information systems shall be kept behind locked, unlabeled doors.
			1. When doors must remain unlocked, a receptionist shall be available to authorize entry to secure areas. Entry shall be granted as follows:
				1. King County employees who are displaying ID badges issued by King County staff shall be permitted to enter on request.
				2. All other visitors, and King County employees who do not display a King County ID badge must sign in and out at the reception desk and wear a visitor ID badge while on the floor.
				3. Visitors coming to see a specific staff person shall be accompanied to and from that staff person’s office by a BHRD employee, unless the employee waives that requirement as the person is well known and felt to be low risk.
			2. Facility areas in which PHI is most readily available (i.e., CCS) shall have additional security barriers, such as a sign stating “Designated Personnel Only Beyond This Point.” Personal visits and non-work related business and conversations must be conducted outside the designated work area.
			3. Data wiring closet access is limited to building management and designated personnel, according to job function.
			4. Physical maintenance records impacting physical security shall be maintained by the DCHS or building management.
		1. Workstation Use (§164.310(b))

**HIPAA Standard**: *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*

* + - 1. KCIT shall maintain and inventory of workstations and County-owned portable devices and either their locations within the BHRD facilities or the staff person to which they are assigned.
			2. The functions of any workstation shall be determined by the job responsibilities and access rights of the staff person to which it is assigned. Workstations may be used only for work-related activities.
			3. Workstations within cubicles or offices must be physically located to minimize the viewing of PHI by any passers-by. This also applies to workstations at all BHRD remote sites.
		1. Workstation Security (§164.310(c))

**HIPAA Standard**: *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

* + - 1. On-site workstations shall comply with part 5.11.3 above.
			2. At home:
				1. The computer should be physically located to minimize the viewing of PHI by other residents or visitors to the home.
				2. BHRD user log-in IDs and passwords shall be kept private from other home computer users.
				3. ePHI data files shall not be copied to any home computer hard drive.
			3. In ESP vans
				1. Laptops shall be secured into van workstations.
				2. The computer screen should be physically oriented to minimize the viewing of PHI by clients in the van.
				3. BHRD user log-in IDs and passwords shall be kept private from clients.
				4. Current county-approved secure encrypted network tunnel shall be used.
				5. All policies related to laptops, notebooks, and tablet computers apply.
		1. Device and Media Controls (§164.310(d)(1))

**HIPAA Standard**: *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*

* + - 1. When BHRD staff transport media with PHI, it shall either be kept in a secured area or in the presence of the BHRD staff person.
			2. Couriers
				1. Only approved couriers may be used.
				2. Media containing PHI must be placed in secure containers for courier transport and marked confidential.
				3. Signatures must be obtained upon delivery of PHI. No PHI may be left without a signature from the recipient.
			3. Delivery Services
				1. For FedEx deliveries, return receipt signatures must be requested.
				2. For USPS, “signature confirmation” and “return receipt” shall be requested at the post office.
				3. UPS shall not be used for delivery of PHI.
			4. Staff may not put ePHI on personally owned portable devices including, but not limited to handhelds/PDAs, Ultramobile PCs, flash memory device (e.g., USB flash drives, personal media players/recorders), portable hard disks, cell phones, CDs, disks, DVDs, and laptop/notebook computers.
				1. Any staff person who wants to download their email messages.

Personally owned portable devices or cell phones must be password-protected.

Encrypted email must not be opened on personally owned devices.

* + - * 1. ePHI shall not be sent via wireless networks unless pre-approved by the Privacy and Security Committee.
				2. Staff who have remote access (e.g., Citrix), may not use email encryption unless the software application is installed on their office workstation.
			1. All County-owned portable equipment, such as a laptop/notebook/tablet computers shall be encrypted in accordance with requirements in the BHRD and KCIT policies. Additionally, the following shall occur:
				1. All laptop/notebook/tablet computers shall require a password to be booted up;
				2. Leaving a laptop/notebook/tablet computer unattended in a vehicle is forbidden; and
				3. ePHI shall not be sent via wireless networks unless pre-approved by the Privacy and Security Committee.
			2. BHRD staff shall not copy ePHI to County-owned portable devices including, but not limited to handhelds/PDAs, Ultramobile PCs, flash memory device (e.g., USB flash drives, media players/recorders), portable hard disks, cell phones, CDs, disks, DVDs, and laptop/notebook computers without the approval of the Security Officer.
			3. PHI on portable media created for delivery outside of BHRD shall be encrypted.
				1. The encryption code shall not be transported or delivered on the same media or in the same package as the media containing the PHI.
				2. The media shall be labeled “Contains confidential health care information” and “if found, return to BHRD” with BHRD mailing address.
				3. The procedure for creating the disk is in Attachment A, Appendix 18: BHRD Procedure for Making a CD Containing PHI.
			4. The BHRD KCIT Data Center will be responsible for hard drive destruction for the servers in the standard virtual environment
				1. Hard drives for reuse shall be reformatted.
				2. Hard drives for disposal shall be physically crushed and/or degaussed.
				3. CDs, DVDs, and back-up tapes shall be cut, scratched, shredded, or otherwise destroyed.
			5. Records on the disposal (including equipment donation) of ePHI equipment and media shall be maintained for at least six years.

**Technical Safeguards**

* + 1. Access Controls (§164.212(a)(1))

**HIPAA Standard**: *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4). (Note: Supports the Information Access Management Administrative Standard and Facility Access Controls Physical Standard.)*

* + - 1. BHRD will comply with KCIT policies. These policies have been reviewed and adopted by the county and approved by the County Chief Information Security Officer and are available at <http://kcweb/oirm/policies.aspx>.
			2. See part 4.5 above on Minimum Necessary for a description of the policy and procedures describing in what conditions a person may have access to PHI and how such access is granted.
			3. Each approved BHRD information system user shall be assigned a unique network and database login user ID.
			4. Each approved user shall have a password, which shall be:
				1. At least eight characters long. Additional strong password format requirements shall be implemented based on the capability of the network server and database server;
				2. Changed at least every 90 days;
				3. Expired if not changed or used in 90 days; and
				4. Not disclosed to other persons.
			5. Logins
				1. After three unsuccessful login attempts to the network, the user shall be denied access to the network for 15 minutes.
				2. Unsuccessful login attempts shall be tracked and monitored.
				3. For remote logins, automatic log off shall occur after 45 minutes for providers and two hours for BHRD staff.
				4. Each BHRD and provider staff person shall be held accountable for all access to BHRD databases gained through the use of that staff person’s unique user login identification code and password.
			6. Log outs
				1. Password-protected screen savers in cubicles or multi-staff areas shall be activated to come on after five minutes of no use.
				2. Password-protected screen savers in enclosed offices shall be activated to come on after no more than 10 minutes of no use.
				3. Staff shall log off and shut down all workstations and equipment at the end of their working day, unless otherwise directed.
		1. Audit Controls (§164.312(b))

**HIPAA Standard**: *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

* + - 1. Access by individuals to all applications containing ePHI shall be monitored. Information collected shall include the identity of the individual, the name of the application, and the entry and exit times to the application.
			2. From this information, the Privacy and Security Committee shall review reports looking at the following:
				1. Large total hours of access in a day to applications containing ePHI;
				2. More than one access at the same time to any given application by the same individual; and
				3. Access to applications before 7 a.m. or after 6 p.m. by persons whose work responsibilities are unlikely to require such access.
		1. Integrity (§164.312c)c )1))

**HIPAA Standard**: *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

* + - 1. Security measures to protect ePHI from improper alteration and destruction shall include:
				1. Access to software that allows the addition, alteration, or destruction of ePHI shall be limited to those persons who require these functions to fulfill their job responsibilities.
				2. PHI submitted electronically by batch shall be validated according to the business rules in the King County Behavioral Health Plan (KCBHP) Data Dictionary and the KCBHP Policies and Procedures. Submitted data that cannot be validated will be rejected and the provider submitting the data will be alerted via an error report of the need to correct and resubmit.
				3. Malicious software protections

KCIT shall maintain the latest protection from malicious software (anti-virus, anti-worm, etc.) on the network and on individual workstations.

Providers with access to BHRD databases shall also maintain the latest protection from malicious software on networks and individual workstations.

BHRD employees shall not download software or any other items off the internet onto a BHRD workstation without pre-approval by KCIT.

BHRD employees shall install no software nor use any devices at BHRD workstations without pre-approval by KCIT.

Only Microsoft Windows screensavers may be used. A staff may use his/her own photographs on a screensaver by either emailing the photograph to his/her workstation or installing the photography from a dish that IS staff have scanned prior to the installation.

* + - * 1. A firewall is maintained and administered for all county functions by the KCIT.
		1. Person or Entity Authentication (§164.312(d))

**HIPAA Standard**: *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

* + - 1. Each provider staff person application for access shall be authenticated by use of an official site supervisor list of those who can sign applications for each provider site.
			2. BHRD shall use passwords as the primary means to validate user identity. Passwords are required to access the Novell network and any application that accesses PHI.
			3. All passwords will adhere to the policies described in part 5.10 Access Controls.
		1. Transmission Security ((§164.312(e)(1))

**HIPAA Standard**: *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*

* + - 1. A provider may use only BHRD-approved software for the transmission of ePHI over a public network.
			2. All data transmission software shall provide the ability to encrypt data before transmission.
			3. ePHI data transmitted between the Washington State DSHS and/or Health Care Authority (HCA), and BHRD shall be done using software specified by the State.
	1. REFERENCES:

Federal Law, Regulations, and Policy including any successor, amended, or replacement laws, regulations, or policies

* 42 CFR Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records
* 45 CFR Part 46 Protection of Human Subjects
* 45 CFR Parts 160 Public Welfare and Human Service – General Administrative Requirements
* 45 CFR Parts 162 Public Welfare and Human Service – Administrative Requirements
* 45 CFR Part 164 Public Welfare and Human Service – Security and Privacy

Washington State Law, Regulations, and Policy including any successor, amended, or replacement laws, regulations, or policies

* Chapter 388-04 WAC – DSHS – Protection of Human Research Subjects
* Chapter 388-877B WAC – Certification Requirements for Chemical Dependency Treatment Service Providers
* Chapters 388-865, 388-877, 388-877A WAC – DSHS – Mental Health – Community Mental Health and Involuntary Treatment Programs
* Chapter 10.77 RCW – Criminal Procedure – Criminally Insane
* Chapter 13.50 RCW – Juvenile Courts and Juvenile Offenders – Keeping and Release of Records by Juvenile Justice or Care
* Chapter 42.56 RCW – Public Officers and Agencies – Public Records Act
* Chapter 70.02 RCW – Public Health and Safety – Medical Records – Health Care Information Access and Disclosure
* Chapter 70.96A RCW – Public Health and Safety – Treatment for Alcoholism, Intoxication and Drug Addiction
* Chapter 71.05 RCW – Mental Illness – Mental Illness
* Chapter 71.24 RCW – Mental Illness – Community Mental Health Services Act
* Chapter 71.34 RCW – Mental Illness – Mental Health Services for Minors

Other

* Evaluation and Research Committee, BHRD Policies and Procedures, Section 16, Attachment B