HIPAA

March 9, 2023

Table of contents available upon request

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)
POLICIES AND PROCEDURES

INTRODUCTION

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without client authorization. The Rule also gives clients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. This policy shall apply to providers, and all programs at KIPDA that involve private information.

The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.
The Health Information Privacy Policies and Procedures outlined in this policy and procedure defines KIPDA's obligations to protect the privacy of individually identifiable health information that is created, received, or maintained as an agency and service/program provider. Any individual who is connected to social services' program at KIPDA as a KIPDA staff member, volunteer, provider, or community partner is obligated to protect the information of KIPDA's participants regardless of how that information exists or is encountered.

KIPDA will implement these Health Information Privacy Policies and Procedures as a matter of sound business practice; to protect the interests of KIPDA, its staff and clients/customers business associates, and those in the service provider network; and to fulfill KIPDA legal obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), its implementing regulations at 45 CFR Parts 160 and 164 (65 Fed. Reg. 82462 (Dec. 28, 2000)) ("Privacy Rule"), as amended (Federal Register: February 16, 2006 (Volume 71, Number 32, pages 8389-8433), and state law, that may provide greater protection or rights to clients than the Privacy Rule. For purposes of this policy, business associates refer to KIPDA's service provider network, ancillary services, and any organization connected to KIPDA or KIPDA's clients.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. Compliance with the requirements of the HITECH Act became enforceable on November 30, 2009, 12 months following the Act being signed into law. The requirements

of HITECH were incorporated into HIPAA in the Final Omnibus Rule, which brought HIPAA and HITECH together into the same legislation. The HIPAA Omnibus Final Rule was published on January 25, 2013, and had a compliance date of September 23, 2013. KIPDA follows updates to HIPAA and HITECH regulations and implements those changes as applicable.

DEFINITIONS

1) **Protected Health Information (PHI)**, as defined in HIPAA consists of the following:
   - Name,
   - Date of Birth,
   - Social Security Number,
   - Address,
   - Medicaid Information,
   - Medications,
   - Health Information.
   - Any other information that makes an individual recognizable
2) **Protected Financial Information**, as described in HITECH consists of:
   - Public benefits
   - Amounts of the benefits
   - Income and assets
   - Debts and creditors owed
3) **Technical Information to be Secured**:
   - Passwords and User IDs.
   - PHI when transmitting.
   - Financial information when transmitting.

REQUIREMENT TO COMPLY WITH HIPAA AND HITECH PROVISIONS

KIPDA requires that client and other personal confidential information be maintained. Staff, business associates, and service providers shall comply with the requirements of the Cabinet for Health and Family Services' confidentiality requirements and the Health Insurance Portability Act. Written or verbal information, obtained from a client by KIPDA staff or service provider, or the Kentucky Department for Aging and Independent Living shall not be disclosed in any form that identifies the person without the client's written and informed consent. This excludes the disclosure required by court order or as otherwise authorized by law.

Members of KIPDA staff, volunteers, business associates, providers, those connected to providers, and others who encounter PHI are obligated to follow these Health Information Privacy Policies & Procedures faithfully. Failure to do so can result in disciplinary action, including termination of KIPDA staff, business associate, or service providers and/or termination of affiliation with KIPDA.

These Policies & Procedures address the basics of HIPAA and the Privacy Rules that apply in KIPDA staff, business associates, and service network. The Policies and Procedures do not attempt to cover all conditions in the Privacy Rules. The Policies & Procedures sometimes refer to forms used by KIPDA to help implement the policies and to the Privacy Rules themselves when added detail may be needed.

Please note that while the Privacy Rules speak in terms of "individual" rights and actions, these Policies & Procedures use the more familiar word "client" instead; "client" should be read broadly to include prospective clients, clients of record, former clients, their authorized representatives, and any other "individuals" contemplated in the Privacy Rules.

If you have questions or concerns about any use or disclosure of individually identifiable health information or about the performance of other obligations under these Health Information Privacy Policies & Procedures, the Privacy Rule, or other federal or state law, please consult [Joanna Weiss, 502-266-5571, PRIVACY OFFICER; or Jessica Elkin, Division Director, at the same number] before you act.

GENERAL RULE: NO USE OR DISCLOSURE

A. Policy: KIPDA staff, service provider network, and business associates must not use or disclose protected health information (PHI), except as these Privacy Policies & Procedures permit or require.

ACKNOWLEDGEMENT AND OPTIONAL CONSENT

A. Policy: KIPDA staff, business associates, and service providers will make a good faith effort to obtain a written acknowledgement of receipt by the client of the agency's Notice of Privacy Practices. This effort will occur before the use or disclosure of a client's protected health information (PHI) for services, to obtain payment for provision of services, or for KIPDA program operations.

B. Policy: KIPDA staff, business associates, and service providers network's use or disclosure of PHI for KIPDA services and payment activities, and program operations may be subject to the minimum necessary requirements.

C. Policy: KIPDA staff, business associates, and service providers will become familiar with the state's privacy laws. If required by state law, or as directed by the KIPDA professional staff and privacy officer, KIPDA will also seek Consent from a client before use or disclosure of PHI for purposes of providing services as needed – in addition to providing a copy of KIPDA's Notice of Privacy Practices when required.

Procedures:

1. Obtaining Consent – If consent is to be obtained, upon the individual's first visit as a client (or next visit if already a client), KIPDA staff and/or service provider

will request and obtain the client's written consent for the agency's use and disclosure of the client's PHI for services, payment, and program operations.

2. Any consent KIPDA obtains should be in writing, preferably on a consent form. In some situations, verbal consent might be allowed. KIPDA staff, business associates, and service network will include the signed consent form in the client's chart.
3. Exceptions – KIPDA staff, business associates, and service provider network does not have to obtain the client's consent in emergency situations; when intervention is required by law; or when communications barriers prevent consent.
4. Consent Revocation – A client from whom consent is obtained may revoke it at any time by written notice. KIPDA staff, business associates, and service network will include the revocation notice in the client's chart. Documentation of revocation will be recorded on the consent form.
5. Applicability – Consent for use or disclosure of PHI should not be confused with informed consent for services.
6. This section applies to KIPDA staff and service provider network.

AUTHORIZATION

A. Policy: KIPDA, business associates, and service providers must have proper, written authorization from the client (or the client's personal representative) before the use or disclosure of a client's PHI for any purpose other than a purpose directly related to service, payment, or program operations, unless permitted or required without consent or authorization.

B. Policy: KIPDA staff and service network will use an authorization form. KIPDA will always act in strict accordance with an authorization.

Procedures:

1. Authorization Revocation – A client may revoke an authorization at any time by written notice. KIPDA staff and service network will not rely on an Authorization known to be revoked.
2. Authorization from Another Provider – KIPDA staff and service provider network will use or disclose PHI as permitted by a valid authorization received from another service/program provider.
3. KIPDA staff, business associates, and service provider network may rely on that covered entity to have requested only the minimum necessary protected PHI. Therefore, KIPDA will not make its own "minimum necessary" determination, unless the authorization is incomplete, contains false information, has been revoked, or has expired.
4. Authorization Expiration – KIPDA staff and service provider network will not rely on an Authorization known to be expired.

PROFESSIONAL JUDGEMENT AND CLIENT'S BEST INTEREST

A. Policy: KIPDA staff, business associates, and service network may use or disclose a client's PHI with the client's oral agreement though written consent is preferable. The policy is subject to all applicable requirements.

B. Policy: KIPDA staff, business associates, and service network may use professional judgment and experience with common service network to make reasonable inferences of the client's best interest in allowing a person to act on behalf of the client to pick up supplies, records, or other similar forms of PHI.

PERMITTED WITHOUT ACKNOWLEDGEMENT, CONSENT AUTHORIZATION OR ORAL AGREEMENT

A. Policy: KIPDA staff, business associates, and service network may use or disclose a client's PHI in certain urgent situations, without authorization or oral agreement. In KIPDA's service network, disclosures without acknowledgement, consent authorization, or oral agreement are not frequent. Written authorization is preferred.

Procedures: Verification of Identity:

1. KIPDA staff, business associates, and service network will always verify the identity of any client, and the identity and authority of any client's personal representative, government or law enforcement official, or other person, unknown to KIPDA, who requests PHI before it is disclosed to that person.

2. KIPDA staff, business associates, and service network will obtain appropriate identification and, if the person is not the client, evidence of authority should be provided. Examples of appropriate identification include photographic identification card, government identification card or badge, and appropriate document on government letterhead. If valid ID is not available, verify the individual's demographic information against documentation in the client's record. If the authenticity of the individual cannot be verified, they will be informed that a new request must be completed and notarized. KIPDA staff and service network will document the incident and the response.

Procedures: Uses or Disclosures Permitted under this Section:

The situations in which KIPDA staff, business associates, and service network is permitted to use or disclose PHI in accordance with the procedures set out in this Section are listed below.

1. KIPDA staff and service network must provide a client with access to any/all PHI about that client to the client or his/her personal representative upon request.
2. KIPDA staff, business associates, and service network must disclose to a client's personal representative PHI relevant to the representative's capacity. KIPDA and service providers will not disclose to a personal

representative reasonably believed to be abusive to a client any PHI reasonably believed to promote or further such abuse.

3. KIPDA staff, business associates, and service network will not use or disclose a client's PHI for fundraising purposes without the client's Authorization.
4. KIPDA staff, business associates, and service network will not use or disclose PHI for marketing without a client's Authorization unless the marketing is in the form of a promotional gift of nominal value that is provided, or face-to-face communications between KIPDA/provider and the client.
5. KIPDA staff, business associates, and service network may use or disclose PHI in the following types of situations without specific permission, provided procedures specified in the Privacy Rules are followed:
    a. For public health activities.
    b. To health oversight agencies.
    c. To coroners, medical examiners, and funeral directors.
    d. To employers regarding work-related illness or injury.
    e. To the military.
    f. To federal officials for lawful intelligence, counterintelligence, and national security activities.
    g. To correctional institutions regarding inmates.
    h. In response to subpoenas and other lawful judicial processes.
    i. To law enforcement officials.
    j. To report abuse, neglect, or domestic violence.
    k. As required by law.
    l. As part of research projects; and
    m. As authorized by state worker's compensation laws
    n. Any other appropriate and urgent situations not listed here that impact the health, safety and welfare of clients or potential clients

REQUIRED DISCLOSURES

A. Policy: KIPDA staff, business associates, and service network will disclose protected health information (PHI) to a client (or to the client's personal representative) to the extent that the client has a right of access to the PHI; and to the U.S. Department of Health and Human Services (HHS) on request for complaint investigation or compliance review.

B. Policy: KIPDA staff, business associates, and service network will use a disclosure log to document each disclosure made to HHS.

MINIMUM NECESSARY

A. Policy: KIPDA staff, business associates, and service provider network will make reasonable efforts to disclose, or request of another covered entity, only the minimum necessary protected health information (PHI) to accomplish the intended purpose.

B. Policy: There is no minimum necessary requirement for disclosures to or requests by one another in KIPDA or by a service/program provider for the provision of services; permitted or required disclosures to, or for disclosure requested and authorized by, a client; disclosures to HHS or the Commonwealth of Kentucky for compliance reviews or complaint investigations; disclosures required by law; or uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.

Procedures:

1. Routine or Recurring Requests or Disclosures – KIPDA staff, business associates, and service network will follow the policies and procedures adopted to limit the routine or recurring requests for KIPDA disclosures of PHI to the minimum reasonably necessary for the purpose.
2. Non-Routine or Non-Recurring Requests or Disclosures – No non-routine or non-recurring request for or disclosure of PHI will be made until it has been reviewed on a client-by-client basis against KIPDA criteria to ensure that only the minimum necessary PHI for the purpose is requested or disclosed.
3. Other's Requests – KIPDA staff and service provider network will rely, if reasonable for the situation, on a request to disclose PHI for the minimum necessary, if the requester is:
   a. a covered entity.
   b. a professional (including an attorney or accountant) who provides professional services to KIPDA staff and service provider network, either as a member of KIPDA or as a Business Associate, and who represents that the requested information is the minimum necessary.
   c. a public official who represents that the information requested is the minimum necessary; or
   d. a researcher presenting appropriate documentation or making appropriate representations that the research satisfies the applicable requirements of the Privacy Rules.
4. Entire Record – KIPDA staff, business associates, and service network will not use, disclose, or request an entire record, except as permitted in these Policies & Procedures or standard protocols that we adopt reflecting situations when it is necessary.
5. Minimum Necessary Workforce Use – KIPDA staff and service network will use only the minimum necessary PHI needed to perform KIPDA services and duties.

BUSINESS ASSOCIATES

A. Policy: KIPDA will obtain satisfactory assurance in the form of a written contract that KIPDA and Business Associates will appropriately safeguard and limit their use and disclosure of the protected health information (PHI) disclosed to them.

B. Policy: The Business Associate Contract Terms document contains the terms that federal law requires be included in each Business Associate Contract.

Procedures:

1. Breach by Business Associate – If KIPDA staff learns that a Business Associate has materially breached or violated its Business Associate Contract, KIPDA will take prompt, reasonable steps to see that the breach or violation is cured.
2. If the Business Associate does not promptly and effectively cure the breach or violation, KIPDA will terminate contract with the Business Associate, or if contract termination is not feasible, report the Business Associate's breach or violation to the U.S. Department of Health and Human Services (HHS).

NOTICE OF PRIVACY PRACTICES

A. Policy: KIPDA will maintain a Notice of Privacy Practices as required by the Privacy Rules.

Procedures:

1. KIPDA's Notice – KIPDA staff and service providers will use and disclose PHI only in conformance with the contents of the Notice of Privacy Practices. KIPDA will promptly revise a Notice of Privacy Practices whenever there is a material change to our uses or disclosures of PHI to legal duties, to the clients' rights or to other privacy practices that render the statements in that Notice no longer accurate.
2. Notice of Privacy Practices, as found in this policy and procedure, contains the terms that federal law requires.
3. Distribution of KIPDA's Notice – KIPDA will provide a Notice of Privacy Practices to any person who requests it and to each client no later than the date of first service delivery. Clients can be referred to the website for the Notice of Privacy Practices.
4. KIPDA will have a Notice of Privacy Practices available for clients to keep if they request it. The Notice of Privacy Practices will be provided in a clear and prominent location where it is reasonable to expect clients seeking services from KIPDA or its provider network will be able to read the Notice. This could mean a referral to KIPDA's website for reference.
5. Acknowledgement of Notice – KIPDA will make a good faith effort to obtain from the client a written Acknowledgement of receipt of the Notice of Privacy Practices when practical.

CLIENTS' RIGHTS

A. Policy: KIPDA staff and service network will honor the rights of clients regarding their PHI.

Procedures:

1. Access –

With rare exceptions, KIPDA staff and service network must permit clients to request access to the PHI that KIPDA, its staff and Business Associates maintain.

a. No PHI will be withheld from a client seeking access unless KIPDA or service provider confirms that the information may be withheld according to the Privacy Rules. KIPDA or the provider may offer to provide a summary of the information in the chart. The client must agree in advance to receive a summary and to any fee KIPDA will charge for providing the summary. KIPDA will contact Business Associates/service providers to retrieve any PHI they may have on the client.
b. Requests for access to PHI must be in writing. The method of access must be specified in the request. Access to the records will be provided in the form requested. If the form requested is not readily producible, records must be provided in readable paper copy or other form agreed to by the individual. PHI provided by email will be encrypted with decryption instructions included.
c. Access must be provided within 30 days of the request. If that is not possible, the timeframe may be extended an additional 30 days one time, by providing written notice to the individual to include the reasons for the delay and date by which access will be provided.
d. If the requested information is not available and the whereabouts are unknown, this information will be documented and the written request and returned to the individual with a copy filed in the client record.

2. Charges for copying –
   The individual will be charged the following reasonable, cost-based fees, as permitted by state law.
   a. Charges for copying, to include the cost of supplies and labor for copying (but not retrieving).
   b. Postage if the individual requests that records be mailed.
   c. Charges for preparation of an explanation or summary when requested in advance and individual agrees in advance to fees.
   d. Charges for cost of computer disk if that format is requested.
3. Amendment –
   Clients have the right to request to amend their PHI and other records for as long as KIPDA and service network maintains them.
   a. KIPDA and service network may deny a request to amend PHI or records if:
      i. they did not create the information (unless the client provides a reasonable basis to believe that the originator is not available to act on a request to amend).
      ii. KIPDA believes the information is accurate and complete; or
      iii. KIPDA does not have the information.
   b. KIPDA staff and service network will follow all procedures required by the Privacy Rules for denial or approval of amendment requests. KIPDA will not, however, physically alter or delete existing notes in a client's chart. KIPDA will inform the client when there is agreement to make an

amendment and will contact the Business Associates/service providers to help assure that any PHI they have on the client is appropriately amended. KIPDA will contact any individuals whom the client requests are alerted to any amendment to the client's PHI. KIPDA will also contact any individuals or entities of which we are aware that we have sent erroneous or incomplete information and who may have acted on the erroneous or incomplete information to the detriment of the client.

c. When KIPDA denies a request for an amendment, any future disclosures of the contested information will be marked in a way acknowledging the contest.

4. Disclosure Accounting –
   a. Clients have the right to an accounting of certain disclosures KIPDA staff and service provider network made of their PHI within the 6 years prior to their request. Each disclosure made, that is not for services, payment or program operations, must be documented showing the date of the disclosure, what was disclosed, the purpose of the disclosure, and the name and (if known) address of each person or entity to whom the disclosure was made. The Authorization or other documentation must be included in the client's record and retained for at least six years from the date created. KIPDA will use the client's file to track each disclosure of PHI as needed to enable fulfillment of the obligation to account for these disclosures.
   b. KIPDA is not required to account for disclosures made:
      i. before April 14, 2003.
      ii. to the client (or the client's personal representative).
      iii. to or for notification of persons involved in a client's service/program or payment for service/program.
      iv. for services, payment, or service/program operations.
      v. for national security or intelligence purposes.
      vi. to correctional institutions or law enforcement officials regarding inmates.
      vii. according to an Authorization signed by the client or the client's representative.
      viii. incident to another permitted or required use disclosure, or
      ix. any disclosures required by law.
   c. KIPDA will temporarily suspend the accounting of any disclosure when requested to do so pursuant according to the Privacy Rules by health oversight agencies or law enforcement officials. We may charge for any accounting that is more frequent than every 12 months, provided the client is informed of the fee before the accounting is provided. KIPDA will contact the Business Associates (if any) to assure any disclosures made by them for which KIPDA must account is included in the accounting.

5. Restriction on Use or Disclosure –
   Clients have the right to request KIPDA staff and service network to restrict use or disclosure of their PHI, including for services, payment, or program

operations. KIPDA has no obligation to agree to the request, but if there is agreement, KIPDA will comply with the agreement (except in an appropriate medical emergency). KIPDA may terminate an agreement restricting use or disclosure of PHI by a written notice of termination to the client. KIPDA will contact the Business Associates (if any) whenever KIPDA agrees to such a restriction to inform the Business Associates (if any) of the restriction and its obligations to abide by the restriction. KIPDA will document in the client's chart any such agreed to restrictions.

6. Denial of a Request –
   If access is denied, notice must be made in writing and must include the reason for denial, a description of how a complaint may be filed with the KIPDA office and a description of how a complaint may be filed with the Department of Health and Human Services.

7. Applicability –
   KIPDA staff and service network will be aware of and respect these clients' rights regarding their PHI.

STAFF TRAINING AND MANAGEMENT, COMPLAINT PROCEDURES, DATA SAFEGUARDS, ADMINISTRATIVE SERVICE NETWORKS

A. Policy: Staff Training and Management: KIPDA will train all members of KIPDA staff and the service provider network in these Privacy Policies & Procedures, as necessary and appropriate for them to carry out their functions.

KIPDA Division of Social Services and appropriate staff from the service provider network will train each new staff member within a reasonable time after the member starts. KIPDA will also retrain each staff member whose functions are affected either by a material change in KIPDA Privacy Policies and Procedures or in the member's job functions, within a reasonable time after the change. KIPDA will hold an annual HIPAA/HITECH refresher/update training for all staff in the Division of Social Services.

Procedures:

1. A sign-off form confirming staff Review of Policies and Procedures can be used to have workforce members acknowledge they have received and read a copy of these Policies and Procedures; and have received training and understand their responsibility for HIPAA/HITECH policies and procedures.

B. Policy: Sanctions, Discipline, and Mitigation: KIPDA, business associates, and the service provider network will develop, document, disseminate, and implement appropriate discipline policies for staff members who violate KIPDA Privacy Policies & Procedures, the HIPAA Privacy Rule, or other applicable federal or state privacy law.

Procedures:

1. Staff members who violate KIPDA's Privacy Policies & Procedures, the HIPAA Privacy Rule, or other applicable federal or state privacy law will be subject to disciplinary action, including termination of employment.
2. Complaints –
    a. KIPDA, business associates, and the service provider network will implement procedures for clients to make a complaint about compliance with KIPDA's Privacy Policies and Procedures or the Privacy Rules. KIPDA will also implement procedures to investigate and resolve such complaints.
    b. The Complaint form can be used by the client to lodge the complaint. Each complaint received must be referred to management immediately for investigation and resolution. KIPDA will not retaliate against any client or workforce member who files a Complaint in good faith.
3. Data Safeguards –
    KIPDA staff, business associates and service provider network will take reasonable steps to limit incidental uses and disclosures of PHI made according to an otherwise permitted or required use or disclosure.
    a. All client records and transactions will comply with the privacy and security provision of the Health Insurance Portability and Accountability Act (HIPAA).
    b. Filing cabinets containing client case files and information are to be housed in secure files (capable of locking and fire protection). File cabinets shall be unlocked at the beginning and locked at the close of the business day.
    c. KIPDA staff, business associates, and service providers who have access to or communicate about clients and his/her concerns shall ensure strict confidentiality of the information available.
        i. Staff/contractors conducting client interviews shall only be conducted in the presence of others only with explicit written consent of the client. Exceptions include: the client's inability to understand a request of consent, the need for an interpreter if the client does not speak English, or the client's inability to hear and/or speak.
        ii. Staff/Contractors shall never converse about clients in common areas at the office, in the community or at home.
        iii. Staff/Contactors shall never take client files or other client related information home or keep in their personal vehicle outside of routine work activities.
        iv. Staff/Contractors shall maintain written client information as confidential while used in the office.
        v. All protected client information shall be enclosed in a locked file box when transporting information needed to conduct business.
        vi. If client information is not returned to place of business prior to the close of the business day, staff must maintain client information in a locked file in a secured location and return to office the next business day.
        vii. When seeing more than one client in an apartment building or other congregated location, paperwork pertaining to another client shall be maintained in a locked box or secured location.

4. Misplaced or Stolen Client Information –
   KIPDA staff and service providers are responsible for protecting the personal information of all people served and encountered. If protection of PHI is compromised at any level, KIPDA and the Service Provider must adhere to policies outlined in the HHS HIPAA Rules concerning HIPAA Breaches. The following security measures must occur:
   a. Any incident of misplaced or stolen client information shall be reported immediately to the staff supervisor.
   b. An incident report shall be written by staff and noted in the client's file within twenty-four (24) hours of the incident.
   c. Clients shall be notified of missing personal information with twenty-four hours (24) of the incident or as soon as possible.
   d. The appropriate HHS Office must be notified if applicable in accordance with HIPAA Rules concerning breaches.
5. Computer Security –
   All staff and contractors shall be responsible for maintaining computer security. The following security measures must occur for all information relevant to client data.
   a. Passwords shall include one or more numerical digits and both uppercase and lowercase letters. Passwords will be changed regularly.
   b. User password protected screen savers, or lock computer function when computer is vacant.
   c. Written passwords shall never be posted under keyboards, phones or on the monitor. Where User IDs and Passwords are necessary to use a particular application (for required databases, each user will have a unique ID/Password combination; such User IDs and Passwords shall not be shared, and new IDs and Passwords will be assigned for new users.
   d. The monitor shall be tilted away from walkways and/or privacy filters may be used.
   e. Thumb drives containing electronic sensitive material shall be locked in desk drawers and/or require a password so as not to be accessed by others outside the designated user.
   f. The preferred practice for PHI and emails within KIPDA is to limit the amount of PHI being sent, and to use encryption when possible. However, KIPDA's internal server is secure, and encryption is not necessary. Business associates and service providers are encouraged to utilize secure servers and encryption software whenever sending and storing PHI.
   g. PHI data shall not be e-mailed outside of the agency unless necessary. If there is no practical alternative to emailing PHI, encryption shall be used. Encryption, using the protocol shall be followed guiding the e-mail creator and receiver in how encryption will be utilized and when encryption is necessary. It will be necessary for an outside organization or individual receiving an encrypted e-mail to utilize same encryption software to open the encrypted document.
   h. Thumb drives (flash drives) and hard drives are to be erased or destroyed prior to disposal in a waste facility.

i. Users are to empty personal waste bins on a periodic basis, and shred documents containing protected health and financial information weekly.
j. Users should check with the KIPDA Information Technology Director prior to destroying large amounts of stored PHI sensitive electronic information to see if destruction requires special attention or if it should not be destroyed due to record retention requirements.
k. Computer and e-mail privileges will be terminated immediately upon termination or resignation of an employee or contractor consistent with KIPDA policies.

6. Documentation and Record Retention –
KIPDA staff and service network will maintain in written or electronic form all documentation required by the HIPAA Privacy Rule for six years from the date of creation or when the document was last in effect, whichever is greater.
7. Privacy Policies & Procedures –
Only KIPDA Division of Social Services Director or representative may change these Privacy Policies & Procedures.

DATABREACH NOTIFICATION GUIDELINES

A. Policy: KIPDA staff will report the discovery or commission of a breach of unsecured PHI immediately and no later than 24 hours after its occurrence.

B. Policy: Following the discovery of a breach of unsecured PHI, KIPDA will notify each individual whose PHI is reasonably believed by KIPDA to have been, accessed, acquired, used or disclosed as a result of such a breach. If more than 500 people are impacted, KIPDA will also give notice to the media and to the Department of Health and Human Services (HHS) immediately. Smaller breaches will be reported to HHS annually as required to do so by federal regulation. KIPDA shall also review applicable state laws or regulations to determine what, if any, additional notice to the individual or to state officials is required.

Procedures:

1. Definitions: As used in this policy and procedure, the following terms have the following meanings:
   a. **Breach** - the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the PHI.
   Exceptions. The term “breach” does not include:
      i. Any unintentional acquisition, access, or use of PHI by a workforce member of KIPDA or person acting under the authority of KIPDA or a business associate/service provider of KIPDA if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in a further use or disclosure that would violate the HIPAA Privacy Rule. Example: If a nurse mistakenly sends an e-mail containing PHI to a billing employee and the billing employee recognizes that he/she is not the intended recipient, deletes the e-mail, and alerts the nurse of the misdirected e-mail, there has not been a breach.

However, the nurse and the billing employee must report the incident in accordance with this policy.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at KIPDA or at a business associate of KIPDA to another person authorized to access PHI at KIPDA or at the same business associate of [Provider], or an organized health care arrangement in which KIPDA participates, and the information received as a result of such disclosure is not further used or disclosed in a manner which would violate the HIPAA Privacy Rule. Example: A physician who has authority to use or disclose PHI at KIPDA by virtue of participating in the organized health care arrangement between KIPDA and its medical staff is similarly situated to a nurse or billing employee at KIPDA who also has authority to use or disclose PHI at [Provider]. If the physician mistakenly sends PHI to a nurse not involved in a patient's care, that nurse should notify the physician of the inadvertent disclosure and delete the e-mail, and the physician and the nurse must report the incident in accordance with this policy.

iii. A disclosure of PHI where KIPDA or a business associate of KIPDA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI. Example: If a nurse mistakenly hands a patient discharge paper belonging to another patient but quickly realizes her mistake and retrieves the papers, and if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, no breach has occurred. However, the nurse must report the incident in accordance with this policy.

b. **Compromises the security or privacy of the PHI** - poses a significant risk of financial, reputational, or other harm to the individual. This excludes a use or disclosure of a Limited Data Set that does not include any of the identifiers listed in 45 CFR 164.514(e)(2), date of birth, or zip code.

c. **Discovered** - in the context of a breach, the first day on which such breach is known to KIPDA or, by exercising reasonable diligence, would have been known to [Provider]. KIPDA is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of [Provider].

d. **Unsecured PHI** - PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption or destruction technologies/methodologies specified on the HHS website.

2. All workforce members of KIPDA are responsible for reporting any suspected or actual violations of the HIPAA privacy rule or [Provider]'s Privacy Manual to the Chief Privacy Officer.
3. The Chief Privacy Officer will receive reports of breaches, potential breaches, and incidents that may qualify as an exception to a breach and investigate those reports in a timely manner to determine if a violation of the HIPAA Privacy

Rule has occurred and, if so, whether the violation compromises the security or privacy of the PHI. If the Chief Privacy Officer cannot, for whatever reason, investigate a report in a timely manner, then KIPDA In-Home Services Coordinator shall be responsible for doing so. In making the determination of whether a breach has occurred, the Chief Privacy Officer or In-Home Services Coordinator should consult with legal counsel and should consider the following factors, as applicable:

a. Who impermissibly used the information or to whom the information was impermissibly disclosed? If, for example, PHI was impermissibly disclosed to another healthcare provider, then there is probably less of a risk of harm to the individual, since the recipient entity has an obligation to protect the privacy and security of the information it received.
b. Did KIPDA take immediate steps to mitigate an impermissible use or disclosure? If KIPDA obtains a recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed, and if such steps eliminate or reduce the risk of harm to the individual to less than a "significant risk," then no breach has occurred.
c. Impermissibly disclosed PHI is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, the breach probably does not pose a significant risk to the individuals whose information was on the laptop.
d. The type and amount of PHI involved in the impermissible use or disclosure. For example, if the information indicated the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the PHI includes information that increases the risk of identity theft (such as a social security number or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.

4. KIPDA shall keep documentation of all investigations for six years from the date the documentation was created.
5. If it is determined that a breach of unsecured PHI has occurred, then notice to all affected persons must be given without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by KIPDA, unless a law enforcement official requests that notification be delayed so that a criminal investigation is not impeded or so that national security is not damaged. If the request is oral, the request and the identity of the official making it should be documented and the notification may be delayed no longer than 30 days from the date of the request, unless a written request specifying a later date on which notification can be made is received within the 30-day period. If the request is initially made in writing and specifies a time for which a delay is required, KIPDA will delay the notification until that date. All documentation of law enforcement requests shall be kept six years from the date the request is made.

6. If a breach of unsecured PHI was suffered by a Business Associate or a member of the service provider network of KIPDA and the Business Associate is an independent contractor, the time for notification begins to run when the Business Associate becomes aware of the breach. Business Associate will need to notify KIPDA of the breach as soon as they are aware. If a breach of unsecured PHI was suffered by a Business Associate of KIPDA and the Business Associate is an agent of KIPDA, the time for notification begins to run when the Business Associate discovers the breach. KIPDA will request that its Business Associates cooperate with it in making the appropriate notices of breach in a timely manner, which may include requesting the Business Associate to take responsibility for any or all of the required notices. However, applicable law places the burden on KIPDA to notify individuals of a breach of unsecured PHI suffered by a Business Associate of KIPDA.
7. Written notification must be made by first-class mail to the individual or the individual's personal representative at the last known address of the individual or personal representative, as appropriate, or, if the individual agrees to receive such notice electronically and the agreement has not been withdrawn, by electronic mail. If KIPDA knows the individual is deceased and has the address of the next of kin or personal representative of the individual, KIPDA must send written notification by first-class mail to either the next of kin or personal representative of the individual. Notification may be provided in one or more mailings as information is available. In cases where urgency is required because of the possible imminent misuse of unsecured PHI, additional notice can be made to provide information to the individual affected by the breach by telephone or other means as appropriate.
8. The notice of breach must be written in plain language and include, to the extent possible:
    a. A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known.
    b. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code).
    c. The steps individuals should take to protect themselves from potential harm resulting from the breach.
    d. A brief description of what KIPDA is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
    e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.
9. If there is insufficient or out-of-date contact information that precludes written or electronic mail communication to an individual, a substitute form of notice reasonably calculated to reach the individual must be provided. Substitute notice need not be provided if there is insufficient or out-of-date contact information for the next of kin or personal representative of a deceased individual. If fewer than 10 individuals are involved, substitute notice may be provided by written or electronic mail, telephone, or other means. If 10 or more

individuals are involved, then either a conspicuous posting must be placed on [Provider]'s internet home page or a conspicuous notice must be placed in major print or broadcast media in geographic areas where the individuals affected by the breach are likely to reside. The notice must include a toll-free phone number where the individual can learn whether or not their individual unsecured PHI is possibly included in the breach. This phone number must be activated by KIPDA immediately before the posting or media notice and remain active for 90 days after the posting or media notice occurs.

10. If a breach of unsecured PHI involves more than 500 residents of a state or jurisdiction, KIPDA shall notify prominent media outlets serving that state or jurisdiction. Notice under this section must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by [Provider], unless a law enforcement official requests that notification be delayed so that a criminal investigation is not impeded or so that national security is not damaged. The media notice must include the information stated in paragraph 8 above.
11. Notice to the Secretary of HHS must be made at the same time the written notices are mailed to the affected individuals when 500 or more individuals are involved in a breach. Notice shall be given in the manner specified on the HHS web site. KIPDA will maintain a log of breaches of unsecured PHI affecting less than 500 individuals and, not later than 60 days after the end of each calendar year, notify the Secretary of HHS of breaches that occurred during the previous year in the manner specified on the HHS web site.
12. KIPDA shall also assess all applicable state laws and regulations relating to data breaches to determine if a notice is necessary under those laws and regulations and, if so, shall abide by the requirements of such laws and regulations.

STATE LAW COMPLIANCE

A. Policy: KIPDA staff and service network will comply with the privacy laws of each state that has jurisdiction over KIPDA staff and service network, or its actions involving protected health information (PHI), that provide greater protections or rights to clients than the Privacy Rules.

HHS ENFORCEMENT

KIPDA will give the U.S. Department of Health and Human Services (HHS) access to KIPDA facilities, books, records, accounts, and other information sources (including individually identifiable health information without patient authorization or notice) during normal business hours (or at other times without notice if HHS presents appropriate lawful administrative or judicial process).

KIPDA will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of KIPDA.

DESIGNATED PERSONNEL

KIPDA has designated a Privacy Officer as required by the Privacy Rule. KIPDA's privacy and security staff will consist of the individuals holding the positions of Information Technology Director (IT) and Quality Management Planner (QA). This team approach will be to ensure that HIPAA/HITECH policy will be executed, maintained, and properly conducted. IT will ensure that all technology systems that house and transmit PHI are updated as needed in accordance with regulation.