Cabinet for Health and Family Services

Office of Inspector General

Division of Kentucky Health Information Exchange (KHIE)

Table of Contents

Policies – Introduction

The following policies apply to the access, use, and disclosure of protected health information by Participants of the KHIE. These are the policies adopted by the Office of Inspector General (OIG), Division of KHIE, according to the language found in the Participation Agreement signed by participants in the KHIE. According to the Participation Agreement, the KHIE may change or amend the Policies in a manner consistent with the Participation Agreement. The Participant shall be given notice of any proposed and final changes and Participants shall be given an opportunity to comment on such proposed and final changes. Any change to a policy is effective thirty days after the change unless an earlier effective date is required to address a legal requirement, a concern relating to privacy or security of Data, or an emergency. KHIE can also postpone the effective date of a policy if additional implementation time is needed.

KHIE believes the nine principles defined in "The Architecture for Privacy in a Networked Health Information Environment"[1] are essential for protecting privacy and developing a comprehensive privacy-protective architecture in a networked environment. The principles are as follows:

1. **Openness and Transparency**
   There should be a broad and universal practice of transparency in the way data is handled. Individuals should be able to establish what information exists about them in the data and in databases.
2. **Purpose Specification and Minimization**
   Data should never be collected without the subject of the data knowing why it is being collected and how it will be used. Data should only be used for the purpose for which it was collected.
3. **Collection Limitation**
   The collection of data should be obtained by lawful and fair means and with the knowledge and consent of persons.
4. **Use Limitation**
   A minimization requirement would strictly limit whether data collected for one purpose could be reused in another context. Such use should not be permissible without the explicit consent of individuals.
5. **Collection Limitation**
   The collection of data should be obtained by lawful and fair means and with the knowledge and consent of persons.

6. Collection Limitation

The collection of data should be obtained by lawful and fair means and with the knowledge and consent of persons.

7. Use Limitation

A minimization requirement would strictly limit whether data collected for one purpose could be reused in another context. Such use should not be permissible without the explicit consent of individuals.

8. Individual Participation and Control

Consistent with the scope of individual rights in HIPAA, an individual has a vital stake in, and needs to be, a participant in determining how his or her information is used.

Individuals should be seen as key participants in the process of information collection and dissemination, and not as mere subjects or passive spectators.

9. Data Integrity and Quality

Mechanisms need to be developed to address data corruption and for establishing accountability among those who maintain records. Individuals should have clear avenues to view all information that has been collected about them and to ensure that the information is accurate, complete, and timely.

10. Security Safeguards and Controls

Reasonable security safeguards must be built against loss, unauthorized access, destruction, use, modification, or disclosure of personal information. In addition, all data collectors and disseminators should be mandated to immediately disclose any security breach through a direct communication to those consumers affected.

11. Accountability and Oversight

There must be mechanisms to ensure that the responsibility for privacy and privacy violations is identifiable, and that remedial action can be taken.

12. Remedies

There should be legal and financial means to remedy any privacy or security breaches.

Participant Obligations

The **Scope** of all policies pertinent to **Participant Obligations** applies to all Participants and their Authorized Users, including all persons providing contractor services.

The **Division of KHIE** is responsible for the **maintenance** of these policies.

Division of KHIE Obligations

The **Scope** of all policies pertinent to the **DIVISION OF KENTUCKY HEALTH INFORMATION EXCHANGE (KHIE) OBLIGATIONS** applies to all Division of KHIE employees and contractors, including all persons providing contractor services.

The **Division of KHIE** is responsible for the **maintenance** of these policies.

2 These principles are based upon the Organization for Economic Co-operation and Development's (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines
The mission of OECD is to promote policies that will improve the economic and social well-being of people around the world.

These principles guide the DHI policies to the extent HIPAA, HITECH, state and federal laws allow. In some instances, current technology will not allow full implementation of the principles; however, these principles guide the policies. The following terms are used in the policies:

Definitions

American Recovery and Reinvestment Act means the appropriations bill signed into law on February 17, 2009.

Authorized User means an individual authorized by a Participant under a DHI Participation Agreement to use the Kentucky Health Information Exchange to access or provide Data for a Permitted Use.

Business Associate shall have the definition assigned to Business Associate under HIPAA by 45 C.F.R. § 160.103.

Cabinet for Health and Family Services or CHFS means the program cabinet of the Commonwealth of Kentucky established by K.R.S. § 12.250.

Covered Entity shall have the definition assigned to Covered Entity under HIPAA by 45 C.F.R.§ 160.103.

Data means patient health information provided to KHIE by a Participant.

Exchange means the Kentucky Health Information Exchange (KHIE), the health information Exchange provided by DHI. The Exchange provides connection options for the capability to exchange key clinical information among Participants.

Help Desk means the service provided to Participants by KHIE to assist with questions concerning the functions and operation of the exchange.

HITECH means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

HIPAA means the Health Insurance Portability and Accountability Act of 2013.

IP address means internet protocol address.

KHIE Portal means the web-based portal that enables an Authorized User to see a patient's health information aggregated from multiple sources presented in a customizable, functional and easy-to-use format.

National Institute of Standards and Technology means the non-regulatory federal agency within the U.S. Department of Commerce.

Operations shall have the definition assigned to Health Care Operations under HIPAA as limited by 45 C.F.R. §164.506(c)(iv).

Participant means a Health Care Provider, as defined in 45 C.F.R. § 160.103, who is also a Covered Entity as defined by HIPAA, the Kentucky Department for Medicaid Services or the Kentucky State Laboratory, Division of Laboratory Services. The Participant must have entered into a DHI Participation Agreement and have not terminated the Participation Agreement.

Participation Agreement means the agreement between the DHI and Participants to contribute Data to the Kentucky Health Information Exchange.

Payment shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA regulations.

Permitted Use is defined in relationship to the use made by the type of Participant and outlined in the Participant Agreement.

All Permitted Use by a Participant is such that patient authorization is not required under HIPAA; and

i. To facilitate the implementation of "meaningful use" criteria as required under the American under the American Recovery and Reinvestment Act of 2009 and its related federal regulations, as permitted by HIPAA; and

1. Public health activities and reporting as permitted by applicable law, including the HIPAA regulation at 45 CFR § 164.512(b) or 164.514(e); and
2. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Data exchanged, or such individual's personal representative as described in 42 CFR § 164.502(g) of HIPAA.

Privacy Officer shall have the definition assigned to it by the HIPAA regulations at 45 CFR §164.530(a)(1).

Privacy Rule means those provisions of 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164 of the HIPAA regulations that regulate the privacy of individually identifiable health information.

Protected Health Information shall have the definition assigned to Protected Health Information in 45 C.F.R. § 160.103 of the HIPAA regulations.

Security Rule means those provisions of 45 C.F.R. Part 160 and Subparts A and C of Part 164 of the HIPAA regulations that regulate the security of individually identifiable health information.

Treatment shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA regulations.

PARTICIPANT OBLIGATIONS

Compliance with Law and Policy

1. Laws: Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including but not limited to, those protecting the confidentiality and security of protected health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

2. KHIE Policies: Each Participant shall, at all times, comply with KHIE policies. KHIE's policies may be revised and updated, as deemed necessary. KHIE shall notify Participants of all policy changes. Notification can be made by posting policies on the KHIE website. Each Participant is responsible for ensuring it follows the most recent version of KHIE policies.

3. Participant Policies: Each Participant is responsible for ensuring that it has the appropriate and necessary internal policies for compliance with applicable federal, state, and local laws as well as KHIE policies.

4. Participant Criteria: Each Participant shall itself be a HIPAA "Covered Entity" and, thus, subject to both its individual legal duty as a regulated Covered Entity under HIPAA and its contractual obligations under its Participation Agreement.

5. User Criteria: Authorized Users are individuals who have been granted access authority. Each Authorized User derives his or her permission to access and use the system from a Participant. Therefore, each Authorized User must maintain a current relationship to a Participant in order to use the system. Authorized Users must therefore be: (i) Participants (for example, an individual physician) or a member of the workforce of a Participant, (ii) an individual Business Associate or workforce of such Business Associate, or (iii) an individual contractor or subcontractor of a Business Associate or workforce of such contractor or subcontractor.

6. Application to business associates and contractors: Participants shall make this policy applicable to their Business Associates and to the contractors and subcontractors of their Business Associates, as they deem appropriate through the terms of their Business Associate agreements.

Notice of Privacy Practices

Each Participant may develop and maintain a notice of privacy practices (the "Notice") concerning electronic exchange of protected health information with the KHIE. The Notice should describe the uses and disclosures of protected health information contemplated through the Participant's participation in KHIE.

Content: Any such Notice should meet the content requirements set forth under the HIPAA Privacy Rule, comply with applicable laws and regulations, and provide notice of the Participant's activity in the KHIE. Participants may individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through the KHIE.

Dissemination and Individual Awareness: Each Participant may have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual, which policies and procedures shall comply with applicable laws and regulations.

Participant Choice: Participants may choose a more proactive Notice distribution or patient awareness process than provided here and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting KHIE.

Permitted Use of Data

Participant and its Authorized Users will use KHIE only for a Permitted Use. Participant will, and will require its Authorized Users, to comply with the Participation Agreement and all applicable laws and regulations governing the privacy and security of Data received through the Exchange. If Participant includes Data obtained through KHIE in a patient's medical record, Participant may use such Data only for those uses as defined below. Participant and Division of KHIE acknowledge that Participant will make Data available for access through the Exchange only for a Permitted Use and will request Data only for a Permitted Use.

All Participants must be covered entities under HIPAA, and, therefore, individually subject to regulation and penalties of federal and state authorities.

A permitted use of the Kentucky Health Information Exchange is defined as outlined on the most current KHIE Participant Agreement (PA).

Data Exchange and Data Submission

By engaging in Data exchange, Participant agrees that:

1. The Data provided by Participant can be related to and identified with source records maintained by Participant.
2. Participant, at its own expense, will maintain Data backup and retention to maintain records of Data submitted to KHIE.
3. Participant, at its own expense, will provide and maintain the equipment, software, services and testing necessary to use KHIE, except for the software provided by the Division of Health Information.
4. If Participant deems it necessary, Participant will maintain, at its own expense, records of Data accessed by the Participant through KHIE and used by the Participant for Treatment. Participant will determine in what manner, if any, the records accessed by Participant are incorporated into the medical record of the patient.

Data Provided

Participant, with the exception of Kentucky State Laboratory, agrees to make available the following Data to the Exchange to the extent technologically feasible and to the extent created and maintained by Participant and the Division of KHIE:

I. All of its hospital-specific inpatient data, including subsequent corrections or additions, as defined and required by the KHIE Participant Connectivity Guide, as amended from time to time.
II. All of its outpatient surgical data, including subsequent corrections or additions, as described in the KHIE Participant Connectivity Guide, as amended from time to time.
III. All emergency room Data.
IV. All ambulatory care Data.
V. All medical office-specific patient data, including subsequent corrections, as amended from time to time,
VI. All diagnostic testing results, including but not limited to radiological testing and laboratory testing results; and
VII. Listing of patient prescribed medications.

Kentucky State Laboratory, Division of Laboratory Services, agrees to make available all the following data:

VIROLOGY
Hepatitis B Surface Antigen
Hepatitis B Surface Antibody
Hepatitis B Core Antibody
Hepatitis A IgM
Varicella IgG (EIA)
Measles IgG (EIA)

Measles IgM (EIA)
Mumps IgG (EIA)
Herpes IgG
Cytomegalovirus IgG (EIA)
West Nile IgG (EIA)
West Nile IgM (EIA)
Herpes Shell Vial Testing
Herpes DFA slide testing
Norovirus PCR
Toxoplasmosis
VDRL Syphilis Screen
Rubella IgG (EIA)
Rubella IgM (EIA)
Rabies Panel
RCC – Rabies Cell Culture
Prenatal Profile
Viral Isolation Fluid- Non Influenza
Viral Isolation Swab- Non Influenza
Influenza PCR

BACTERIOLOGY
Salmonella grouping and typing
Shigella
Campylobacter
E. Coli
Miscellaneous Enteric Pathogens
VIB – Vibrio
Miscellaneous Bacteria Identification
Pinworm
Ova and Parasites
Neisseria meningitides

MYCOBACTERIOLOGY
Tuberculosis (raw specimen)
Tuberculosis (culture isolate)

CLINICAL CHEMISTRY
Lipid Profile
Total Cholesterol
Fasting or Random Glucose
Glucose 1hr/ 50 gram
Glucose Postpartum Fasting
Glucose Tolerance Test (Prenatal)
Glucose Tolerance Test (Postpartum)

MOLECULAR
Chlamydia and Gonorrhea

ENVIRONMENTAL
Water Bacteriology
Fluoride
Fluoride (Public Water System)
Fluoride (Supplement Program)

NEWBORN SCREENING
Division of Laboratory Services (DLS) screens infant blood spot specimens for over 40 different disorders.

Privacy, Security, and Accuracy

Participant will maintain sufficient safeguards and procedures, in compliance with HIPAA, to preserve the security and privacy of the Data. The Participant is responsible for maintaining appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of personal health information (PHI) according to HIPAA standards found at 45 CFR § 164.530(c). Efforts to safeguard PHI must be appropriate to the situation and in regard to effort and expense. Participants are responsible for ensuring their processes and practices are in compliance with the HIPAA Security Rule.

Policy: Incident Response and Mitigation

KHIE will implement policies and procedures for establishing communications in response to events that are potential incidents; mitigating the adverse effects of incidents; and providing notifications regarding incidents, as required by federal and state laws.

1.1 Incident Response Team. KHIE will utilize its own Issues Task Force, the Cabinet for Health and Family Services' (hereafter, CHFS) Privacy Officer and the Office of Application Technology's (hereafter, OATS) Security Team to manage incident response and mitigation.

1.1.1 Issues Task Force is made up of the KHIE Deputy Executive Director; KHIE Division Director; KHIE Project Manager; KHIE PM (Onboarding); KHIE Technical Lead; KHIE PM (Outreach Coordinators); KHIE PM (Public Health Reporting); OATS Branch Manager (Electronic Records Info Systems Branch, ERISB); Information Security Analyst (OATS Security); Security System Architect (OATS Security); KYIR PM; HIE Vendor Representative.

Procedure

1. To investigate and mitigate a given incident, KHIE will utilize its Issues Task Force, the CHFS Privacy Officer, and the OATS Security team and, in addition, may appoint or request assistance from KHIE staff, Participant's staff, OATS contractors, and the KHIE vendor.

1.2 **Discovering and Reporting Potential Incidents.**

1.2.1 **Discovery by KHIE Staff, OATS Contractors, KHIE Business Associates, or KHIE HIE Vendor.** Anyone who discovers or receives information about or is responsible for a potential incident must immediately report the event to the KHIE Deputy Executive Director and/or the KHIE Division Director, either of whom will convene the Issues Task Force to initiate mitigation.

Issues Task Force is made up of the KHIE Deputy Executive Director; KHIE Division Director; KHIE Project Manager; KHIE PM (Onboarding); KHIE Technical Lead; KHIE PM (Outreach Coordinators); KHIE PM (Public Health Reporting); OATS Branch Manager (Electronic Records Info Systems Branch, ERISB); Information Security Analyst (OATS Security); Security System Architect (OATS Security); KYIR PM; HIE Vendor Representative.

Procedure

1. Whoever discovers the incident shall report it to the KHIE Deputy Executive Director and the KHIE Division Director.
2. The KHIE Deputy Executive Director and/or KHIE Division Director shall convene the Issues Task Force.
3. The KHIE Division Director shall notify the CHFS Chief Privacy Officer.
4. OATS Branch Manager shall report the potential incident to the OATS Security Team which will engage the Incident Response Team. The OATS Security/Incident Response Team will take the lead to investigate and mitigate the incident and will provide guidance until the incident is resolved.
5. The KHIE HIE vendor will conduct the necessary system monitoring audits and investigations.

1.2.2 **Discovery by Participant Staff, Participant Business Associates, or Subcontractors**. Each Participant shall establish procedures for reporting potential incidents within its organization. A Participant aware of a potential incident involving KHIE or confidential information belonging to or entrusted to KHIE must report the event to KHIE within five (5) business days.

Procedure

1. The Participant's Privacy Officer, Security Officer, or other incident response point of contact, in accordance with the Participant's own policies and procedures, shall investigate and conduct an incident risk assessment and begin mitigating the incident.

Direct Secure Email and Trusted Registered Agent

This policy is only applicable to those Participants receiving Direct Secure Email services.

Each Participant receiving Direct Secure Email services shall designate a Trusted Registered Agent to provide identity-proofing services for the Division of KHIE.

Any Participant that meets the definition of a hospital, as defined by 902 KAR 20:016, shall designate the hospital's Privacy Officer as the Trusted Registered Agent.

The identity proofing services shall require, at a minimum, that the identity of all Direct Secure Email users is verified using forms of government identification, as authorized by the Division of Health Information. This policy shall be revised to comply with the identity proofing of NIST Level of Assurance 3 requirements (as specified in NIST SP 800-63-3, dated June 2017, updated December 2017).

Any change to the Trusted Registered Agent shall be reported to KHIE.

Web Services Access for Substance Abuse and Alcohol Abuse Records

This policy is only applicable to those Participants accessing KHIE by Web Services and displaying a Continuity of Care Document (CCD) in the Participant's electronic medical record or hospital information system.

By engaging in Web Services Data Exchange, Participant agrees that:

> Any CCD displayed by the Participant that includes 42 CFR Part 2 information shall include the prohibition on redisclosure required by 42 CFR 2.32.

DIVISION OF KENTUCKY HEALTH INFORMATION EXCHANGE OBLIGATIONS

Use and Disclosure of Information

The Division of KHIE will not disclose Data or Data Exchange Information to any non-Participant third parties except as: (i) provided by the Participation Agreement; (ii) directed in writing by the originating Participant; or (iii) required by order of any court with appropriate jurisdiction over the Division of KHIE. The Division of KHIE may disclose Medicaid and Other Source Data as permitted under applicable law. The Division of KHIE may access Data and

Data Exchange Information only for the operation of the Exchange, including collecting Medicaid or Other Source Data for the master patient index/record locator service, testing, verifying performance, and providing success measurements to the federal government for the Medicaid Transformation Grant or any other federal grant awarded to any agency within the Cabinet for Health and Family Services of the Commonwealth of Kentucky and funded by the American Recovery and Reinvestment Act. The Division of KHIE may use Data that has been de-identified pursuant to 45 CFR §164.514 to measure the success of the Medicaid Transformation Grant or any other federal grant awarded to any agency of the Cabinet of Health and Family Services of the Commonwealth of Kentucky funded by the American Recovery and Reinvestment Act, if the use is compliant with HIPAA.

Use of Data-Audit Logs

The Division of KHIE will maintain records of the date, time, and records accessed by a Participant through KHIE.

If necessary to comply with the Division of KHIE, KHIE's contractual and regulatory obligations as a business associate, the Division will produce audit logs that will provide data with the following fields of information:

1. Name of provider.
2. Data accessed.
3. Date and time of access.
4. Description of data accessed and, if necessary to comply with applicable laws and regulations, and if technically possible, specific data fields accessed.
5. Source IP address of the data request.
6. Designation IP address of the data request.

The Division of KHIE will maintain a master patient index, a record locator service, and Medicaid and Kentucky State Lab Data as part of KHIE for the benefit of the Participants. Except as provided above, the Division of KHIE will not maintain, and will not be responsible for, either maintaining records of the content of any Data Exchange between Participants or inspecting the content of such Data.

If necessary to comply with the Division of KHIE, and its contractual and regulatory obligations as a business associate, the Division will maintain and produce audit logs that will provide data with the following fields of information for Commercial Laboratory Services connections:

1. Name of provider requesting laboratory order.
2. Date and time of order request.
3. Source IP address of laboratory order.
4. Date and time of order response.
5. Source IP address of provider receiving laboratory results.

Any vendor contracting with the Division of Health Information will respond to a request for audit logs in the following manner:

a) A request for an audit log with the data fields listed above may be requested by the Division of Kentucky Information's Deputy Executive Director or KHIE Division Director.
b) The request for an audit log shall be delivered to the Project Manager for the vendor on site at the principal Division of Health Information Kentucky location.
c) In the event of a breach, as defined by 45 CFR §164.402, the vendor shall deliver the audit log response within 3 days of the request. The response shall be delivered to the individual that requested the audit log.

The Division of Health Information will respond to a request for an accounting of disclosures of protected health information made by a Participant as set forth in 45 CFR §164.528 as follows:

a) A request for an audit log with the data fields listed above may be requested by the Division of Kentucky Information's Deputy Executive Director or KHIE Division
b) Director.
c) The request for an audit log shall be delivered to the Technology Vendor's Project Manager for the vendor.
d) The vendor shall deliver the audit log response within 30 days of the request. The response shall be delivered to the Deputy Executive Director or KHIE Division Director who requested the audit log. KHIE will ensure delivery of the log to the Participant.

Offsite Access to KHIE Files

Access to KHIE files by KHIE employees and contractors will be limited to access via CHFS-owned computers only.

Any employee or contractor requiring access to the KHIE, other than at his designated CHFS worksite, will be required to be granted such access by the KHIE Division Director or Deputy Executive Director.

Service Level Agreements (SLA) Help Desk Response Times and Problem Resolution

KHIE will operate a Help Desk service or will use the services of its technology vendor that ensures all incoming calls are answered within one minute including "hold" time and ensures that callers will not be placed on hold, ring busy, or go unanswered for more than 30 seconds.

1. KHIE will make available Help Desk service reports to Participants by the 10th of each month that include:
    a. Average answer times
    b. Average hold times
    c. Abandoned calls
    d. Call volume by category

2. Description of how requests logged at the Help Desk will be graded are as follows:

    a. **Severity Level 1 Problem** is defined as an event that halts or has a significant impact on use of KHIE's system including the following:
        i. Any event that significantly disrupts or threatens to disrupt KHIE availability to a Participant.
        ii. Any online application outage that significantly impacts KHIE availability.
        iii. Consistent degradation of performance (response time or function) of KHIE that significantly impairs service to a Participant.
        iv. Any repeating, unresolved incidents that have material impact on the service availability, operations, or use of KHIE by Participants.
        v. An issue that causes or results in a security incident.
    b. **Severity Level 2 Problem** is defined as a situation in which KHIE's system has lost some level of functionality but is still accessible by Participants; the lost functionality does not materially impact a Participant's use of KHIE or KHIE's services; however, a workaround does not exist.
    c. **Severity Level 3 Problem** is defined as a situation in which KHIE has lost some level of functionality but is still accessible by Participants; the lost functionality does not materially impact Participant's use of KHIE or KHIE's services; a workaround does exist.
        i. Specific problem/issue for single user
        ii. Application/system workflow marginally impacted
    d. **Severity Level 4 Problem** is defined as a situation in which KHIE has complete functionality and normal operations are not impeded; KHIE's services are still accessible by Participants. The request is an end-user inquiry only.

3. Notification and Communication of Emergency Response
    a. **Service Level Severity 1** is critical in keeping all parties integrated and working and thus, is handled first. KHIE ensures resolution of emergency issues in the following ways, based on the target user's role with the KHIE:
        i. KHIE will use continuous effort to resolve the problem until an official fix is installed, tested, and KHIE's services are back to normal operations.

ii. KHIE will escalate any Severity Level 1 problems that remain unresolved after 4 hours to the next level of KHIE's organization and will continue to escalate ongoing problems every four hours thereafter.

b. **Severity Level 2 Problems** will have a target resolution of 24 hours to 3 days, dependent on the corrective actions required to return KHIE to normal operations. KHIE will report these corrective actions and resolution timeframes will be communicated to participating healthcare providers and commercial laboratories. After forty-eight (48) hours, KHIE will escalate the problem, in accordance with severity level escalation procedures above.

c. **Severity Level 3 Problems** will have a target resolution of 48 hours to 5 days, dependent on the corrective actions required to return the software to normal operations. KHIE will assign sufficient resources to resolve the problem during the business hours of 8 a.m. and 8 p.m. Eastern Standard Time (EST) (adjusted for daylight savings time) on a mutually agreed upon target resolution timeframe. After seventy-two hours (72), KHIE will escalate the problem, in accordance with the severity level escalation procedures above.

d. **Severity Level 4 Problems** will have a target resolution determined separately for each problem by the affected healthcare provider or commercial laboratory and KHIE.

4. Response Time Calculation is the total amount of time it takes KHIE to respond to a request, calculated from the earlier of (a) the time a request arrives at KHIE via telephone call or email regarding the problem or (b) the time KHIE otherwise discovers the problem, until: 1) the appropriate technician or administrator begins to address the request, and 2) contact is made to the requesting party with a status update if the problem was not addressed on the initial call.

KHIE shall notify Participants pursuant to the following Problem Resolution Response Table:

Problem Severity Level	Notification	Minimum Update Frequency and Method of Update
1	within 1 hour after discovery by KHIE	Every two hours by email and telephone
2	within 3 hours after discovery by KHIE	Every five hours by email
3	within 12 hours after discovery by KHIE	Every 12 hours by email
4	by next business day after discovery by KHIE	Every 24 hours by email

Service Level Availability System Downtime-Scheduled and Unscheduled

The KHIE system shall have scheduled down time for KHIE's performance of system maintenance, backup, and upgrade functions. The scheduled downtime period will be between 7:00 p.m. EST and 9:00 p.m. EST each Friday. Scheduled downtimes may also occur on Saturdays when a longer period of time is necessary to perform the maintenance and onboarding releases.

Scheduled down time shall be defined as the time elapsed from the time that KHIE services are unavailable to fully perform operations to when the services become available to fully perform operations.

KHIE will maintain logs of system scheduled downtime and outages. These logs will be available to Participants and upon request.

KHIE may, in its reasonable discretion, determine that maintenance is required outside this scheduled downtime period. In that event, KHIE shall give forty-eight hours advance notice of such required maintenance work. Any maintenance performed according to this notice shall be considered part of the scheduled downtime.

KHIE will establish a software upgrade and version release approach that implements needed system maintenance and enhancements without introducing harm or problems to the operational system.

Disaster Recovery Planning

KHIE will develop, test, and maintain at all times, an appropriate KHIE Disaster Recovery Plan.

1.1 It will include necessary procedures and reconciliation provisions, the necessary software, data storage, and computer equipment, either directly or indirectly through a third-party vendor, to enable KHIE to resume full-service availability to Participants within forty-eight (48) hours from the onset of a major disruption in normal health information exchange operations.

2.1 Upon request, KHIE agrees that it shall provide Participants with a copy of KHIE's official Disaster Recovery Plan.

Notice of Privacy Breach

The Division of KHIE personnel and contractors will maintain the privacy and security of protected health information (PHI), consistent with The Division of KHIE policies and all applicable laws and regulations. The Division of KHIE follows HIPAA requirements for logging security incidents. Additionally, the Division of Health Information investigates potential security breaches, as defined under HITECH, and complies with all reporting requirements, as outlined under the HITECH Act.

Any Division of KHIE personnel and contractors who suspect an information security incident must report the incident to their supervisor within 1 hour of discovery. CHFS IT follows a controlled process to log, investigate, and report all security incidents. The Division of KHIE adheres to this procedure and all federal requirements regarding the investigation, management, and reporting of information regarding security incidents and/or security breaches.

The Division of KHIE will notify the Participant of potential HIPAA violations consistent with the requirements of this policy and according to the Business Associates Agreement between the Division of Health Information and Participant.

1.1 Definition of "Breach": The term "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises, i.e., poses a significant risk of financial, reputational or other harm to the individual, the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

1.1.2 The term "Breach" does not include:

(i) Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the Division of KHIE or a Business Associate if: such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or

(ii) individual, respectively, with the Division of KHIE or a Business Associate; and such information is not further acquired, accessed, used, or disclosed by any person; or

(b) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at the KHIE facility, operated by the Division of KHIE, or a Business Associate to another similarly situated individual at the same facility; and

(c) Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed by any person without patient authorization.

2 "Secured PHI" is rendered unusable, unreadable and indecipherable; thus the Division of KHIE will establish a breach notification process applicable to "Unsecured PHI".

1.2 "Unsecured PHI" is PHI that is not:

- secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals or

- secured by a technology that is developed or endorsed by a standards developing organization accredited by the American National Standards Institute.

1.3 In the event the Division of KHIE discovers a breach of Unsecured PHI, the Division will notify:

(a) each Participant entity whose Unsecured PHI has been or is reasonably believed by the Division of Health Information to have been accessed, acquired, or disclosed as a result of such breach.
(b) The notification requirement applies to any Unsecured PHI

accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used or disclosed by the Division of KHIE. The notification requirements also apply to breaches committed by the Division of KHIE or one of its Business Associates.

1.4 For purposes of this Policy, a Breach will be treated as discovered by the Division of Health Information or one of its Business Associates as of the first day on which the Breach is known to the Division of KHIE or one of its Business Associates, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or agent of the Division of KHIE or one of its Business Associates, respectively or should reasonably have known to the Division of KHIE or one of its Business Associates to have occurred.

a. Whether a Breach compromises the privacy or security of PHI, the Division of KHIE will perform a risk assessment to evaluate:

i. the nature of data elements breached,
ii. the likelihood that the PHI is accessible and useable by unauthorized persons;
iii. what physical, technical, and procedural safeguards were employed by the Division of KHIE;
iv. whether the PHI is at a low, moderate, or high risk of being compromised;

v. the likelihood that unauthorized individuals will know the value of the information and use or sell it;
vi. the level of potential harm:

- Broad reach of potential harm (blackmail, disclosure of private facts, disclosure of sensitive PHI, mental pain and emotional distress, address information for victims of abuse, humiliation, identity theft).
- Likelihood harm will occur (which depends on manner of actual breach and types of data such as SS#, passwords, mother's maiden name, and information useful for identity theft).
- If identity theft or fraud is a risk, review and consider purchasing theft identity insurance for individuals.
- The Division of KHIE's ability to mitigate risk of harm and contain the breach, including consideration of appropriate countermeasure, such as monitoring systems for misuse of the PHI and monitoring for patterns of suspicious behavior that the Division of KHIE can implement.

1.5 The Division of KHIE's Leadership Team (Deputy Executive Director, Division Director, and Project Managers) shall document the process and results of any Risk Assessment. The Deputy Executive Director shall retain such forms for at least a six-year period, in accordance with CHFS's Document Retention Policy.

Employee and Contractor Access to Protected Health Information (PHI)

Any KHIE employee or contractor who has access to Protected Health Information (PHI) shall use the minimum necessary information based on job function and purpose. This Policy is intended to comply with HIPAA requirements for the minimum necessary standard. Nothing under this policy is intended to impose any duty upon any Division of Health Information or KHIE employee or contractor other than those duties imposed under HIPAA and other applicable state and federal law. In the event there is a conflict between this policy and HIPAA, the requirements of HIPAA will apply.

If any employee or contractor has questions or concerns regarding protected health information within the Division of Health Information, they may contact the KHIE Division Director.

General: KHIE has employees and contractors who have the need to access PHI to carry out their duties. The Division of KHIE will make reasonable efforts to limit the access to PHI in accordance with the level of access needed, regardless of job duty.

No employee or contractor shall access any individual's PHI except to perform legitimate employment and contractor activities on behalf of the Division of KHIE.

Any KHIE employee or contractor needing access to PHI to carry out a legitimate activity of employment or contractor work by the Division of Health Information or KHIE to which the employee or contractor otherwise does not generally have access by reason of his normal job function should obtain the permission of the Division Director before accessing any PHI.

KHIE Employee and Contractor Access to KHIE Test and Production Environments

Access to the KHIE test and production environments is limited to Division of KHIE and KHIE employees and contractors who are authorized to access these environments. Any Division of KHIE or KHIE employee or contractor with access to the test or production environments must be granted access to these environments by designated KHIE staff.

Designated KHIE staff will monitor staff access and maintain an up-to-date list.

Individuals with access shall be prohibited from (1) sharing their usernames and/or passwords with others and from (2) using the usernames and/or passwords of others. The use of another's

credentials to access KHIE in any capacity is prohibited. All users are responsible for all activities related to their unique credentials.

The Division of KHIE shall immediately suspend, limit, or revoke access authority to KHIE staff when there is a change in job responsibilities or employment status of an individual with granted access. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued administrative authority for individuals who no longer need access.

KHIE Participant Access to UAT and PMT Environment that contains Protected Health Information (PHI)

Any KHIE Participant (or authorized users thereof) who requires access to the KHIE UAT and PMT environments (which contains Protected Health Information) for testing and validation purposes shall use the minimum necessary information to accomplish the purpose of testing and validation. This Policy is intended to comply with HIPAA requirements for the minimum necessary standard. Nothing under this policy is intended to impose any duty upon any KHIE Participant (or authorized users thereof) other than those duties imposed under HIPAA and other applicable state and federal law. In the event there is a conflict between this policy and HIPAA, the requirements of HIPAA will apply.

General: Data validation and testing are critical components of data collection and are therefore of great relevance to health information exchange. Data validation and testing are processes which allow Participant's authorized users to ensure the quality of the data the healthcare organization is submitting to KHIE is valid and complete. Data validation is vital to ensure accuracy and reliability.

If KHIE Participants (or authorized users thereof) have questions or concerns regarding protected health information, they may contact the KHIE Division Director.

The KHIE Participants have the need to access PHI to carry out testing and validation to ensure the data is accurate. The Division of KHIE will make reasonable efforts to limit the access to PHI in accordance with the level of access needed, according to job duty.