Kingdom of Saudi Arabia

National Health Information Center (NHIC)

Enabling Standards-Based eHealth Interoperability

IS0303
Saudi Health Information Exchange Policies

Version 1.0

April 21, 2016

Document Control Number: *IS0303 Saudi Health Information Exchange Policies*

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

Document Revision History

Version	Date	Type of update	Prepared/Revised by
1.0	April 21, 2016	First Release	National Health Information Center

Policy Approval Process

Subject: Saudi Health Information Exchange Policies		Approved By:
Approval Date:	Effective Date:	Revision Date(s):

1. INTRODUCTION

1.1 DOCUMENT PURPOSE

This document contains the policies and supporting definitions that support the privacy and security aspects of the Saudi Health Information Exchange (SeHE). The policies cover the following topics:

- Saudi Health Information Exchange Authentication Policy
- Saudi Health Information Exchange Consent and Access Control Policy
- Saudi Health Information Exchange Information Security Policy
- Saudi Health Information Exchange Identity Management Policy
- Saudi Health Information Exchange Audit Policy
- Saudi Health Information Exchange Purpose of Use Policy
- Saudi Health Information Exchange Breach Notification Policy
- Saudi Health Information Exchange Subject of Care Rights Policy
- Saudi Health Information Exchange Secondary Use Policy

These policies define the privacy and security requirements for the Saudi Health Information Exchange.

1.2 SCOPE

In Scope:

The scope of this document is the specification of privacy and security requirements for implementation of the SeHE.

Out of Scope:

The following is a list of content and specifications that are specifically out of scope for this document:

- Operational procedures that conform to the policies are a function of the operations and implementation and are out of scope of this document, and
- Architecture and Interoperability Specifications that are compliant with these policies are out of scope and addressed by separate implementation design documents.

1.3 HOW TO READ THIS DOCUMENT

1.3.1 Where to Find Information

This document contains twelve normative sections, as well as informative appendices for your convenience. The document is structured as follows:

Section 1: Contains an introduction to the Policy Set document. This section contains a summary of the document purpose and scope, as well as other content to help orient the

first time reader to the topic of the document and how it relates to other specifications in the SeHE System.

Section 2: Lists the terms used in the document and their official definitions.

Sections 3 – 11: Specify the policies as defined for the Saudi Health Information Exchange.

Section 12: Lists the Saudi eHealth reference documents, as well as the international standards which underpin the definitions and policies.

1.3.2 Document Conventions

Throughout this document the following conventions[1] are used to specify requirement levels:

SHALL: the definition is an absolute requirement of the specification.

(Note: "SHALL …… IF KNOWN" means that the tag must be sent. However, if there were no information, then this tag should be sent with a <nullflavor>)

SHALL NOT: the definition is an absolute prohibition of the specification.

SHOULD: there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT: there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY or **OPTIONAL**: means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

1.4 METHODOLOGY

These policies have been developed with input from various Saudi stakeholders, collected during several months through workshops and teleconferences.

[1] Definitions based upon RFC 2119

2. SAUDI HEALTH INFORMATION EXCHANGE DEFINITIONS

TABLE 2-1 DOCUMENT DEFINITIONS

Term	Definition
Access Control	A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways. [ISO/IEC 2382-8]
Accountability	Property ensures that the actions of an entity may be traced to that entity. [ISO 7498-2]
Antecedent Data	Data from an Antecedent event is an in-person proofing event that occurred previously and shall suffice as meeting the present in-person identity proofing requirements.
Anonymization	Process that removes the association between the identifying data set and the data subject. [ISO/TS 25237]
Assurance	In the context of NIST SP 800-63, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. [NIST 800-63-1]
Audit	Systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s). [ISO 27789]
Audit Log	Chronological sequence of audit records, each of which contains data about a specific event. [ISO 27789]
Audit Record	Record of a single specific event in the life cycle of an electronic health record. [ISO 27789]
Audit Record Repository (ARR)	Receives and stores audit records from sources and consumer of the Saudi eHealth Information Exchange managed health information.
Audit Trail	Collection of Audit Records from one or more Audit Logs relating to a specific Subject of Care or a specific electronic health record. [ISO 27789]
Audit Trails and Node Authentication (ATNA)	IHE profile that establishes the characteristics of a basic secure node.
Authentication	The process of reliable security identification of subjects by incorporating an identifier and its authenticator. [ISO 7498-2]
Authorization	The granting of rights, which includes the granting of access based on access rights. [ISO 7498-2]
Availability	The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2]
Breach	A Breach is a Reportable Event that, once investigated, is confirmed to have compromise the security or privacy of the Personal Health Information (PHI).
Break-Glass	"Break the glass" relates to an “emergency” and “temporary” authorization of a system user and is required to obtain access to information.
Business Associate (BA)	a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. [HIPAA]

Certification Authority (CA)	Authority trusted by one or more users to create and assign public-key certificates. [ISO-9594-8].
Collected	Obtained and persisted. [ISO/ TS 1462514265]
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 7498-2]
Covered Entity	An entity that is required to abide by the Saudi Health Information Exchange Policy.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. [NIST 800-63-1]
Data Integrity	Property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498-2]
[Data subject's] consent	Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. [ISO /IS 22857]
Data Use Agreement	Comprehensive agreement that governs the exchange of health data between participants in the Saudi Health Information Exchange.
De-identification	De-identification is the general term for any process of removing the association between a set of identifying data and the data subject. [ISO /TS -25237]
Emergency Access	Access to data for the provision of care where threat of injury or death requires special permissions or override of other controls in order to ensure uninterrupted and urgent treatment. [ISO/ TS -1462514265]
Encryption	Cryptographic transformation of data to produce ciphertext [ISO 7498-2]. A ciphertext is data produced through the use of encryption, the semantic content of which is not available without the use of cryptographic techniques. [ISO/IEC 2382-08]
External Privacy and Security Audit	Verification by someone outside of the organization that the systems are managed according to specified requirements.
Health Information Exchange Nodes (HIE Nodes)	HIE nodes are those systems (Electronic Medical Records, Public Health Information Systems) that are connected to Saudi Health Information Exchange Systems.
Health Information Management	Mainly responsible for providing medical records and healthcare information management services. [AHIMA]
Health Record	Repository of information regarding the health of a subject of care. [ISO 13606-1] Under this policy, this refers to all personal health information accessible through the Saudi Health Information Exchange.
Healthcare Organization	Officially registered organization [under the umbrella of Saudi Council of Health Services] that has a main activity related to healthcare services or health promotion. [ISO/ IS 17090]
HIE Node Authentication	Describes authenticating each computer system to the Saudi Health Information Exchange.
Identification	Performance of tests to enable a data processing system to recognize entities. [ISO/IEC 2382-8]
Identifier	Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator. [ENV 13608-1]
Individuals	Individuals include healthcare providers, non-regulated health professionals, researchers, subjects of care, and subject of care agents.
Internal Privacy and Security Audit	Verification by someone inside of the organization (Saudi Health Information Exchange or Saudi Health Information Exchange service providers) to ensure that the systems are managed according to specified requirements.

Non-Regulated Health Professional	Person employed by a healthcare organization who is not a regulated health professional. EXAMPLES: Medical receptionist who organizes appointments or a nurse's aide who assists with patient care. NOTE: The fact that a body independent of the employer does not authorize the employee's professional capacity does not, of course, imply that the employee is not professional in conducting her/his services. [ISO/ IS 17090]
Organization	Healthcare organization or a Business Associate's organization..
Organization Roles	Organization roles correspond to the hierarchical organization in an [organization] in terms of internal structures. [Neumann/Strembeck]
Participating Healthcare Subscriber (PHCS)	Any healthcare institution or health professional that has executed an effective Participation Agreement with the Saudi Health Information Exchange. This may be a Healthcare Organization, a Supporting Organization, or a Regulated Health Professional.
Personal Health Information (PHI)	Information about an identifiable person which relates to the physical or mental health of the individual, or to provision of health services to the individual, and which may include: a) information about the registration of the individual for the provision of health services; b) information about payments or eligibility for healthcare with respect to the individual; c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; d) any information about the individual collected in the course of the provision of health services to the individual; e) information derived from the testing or examination of a body part or bodily substance; f) identification of a person (e.g., a health professional) as provider of healthcare to the individual. [ISO 27799]
Portal	Web access channel to Health Information Exchange. This may be a Provider Portal supporting the PHCS or a Client Portal supporting the Subject of Care.
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. [ISO/IEC 2382-8]. In the context of the Saudi HIE, it refers to an individual's interest in limiting who has access to personal healthcare information. [HIPAA]
Privacy and Security Audit	Audit focused on assuring conformance to privacy and security practices and procedures.
Pseudonymization	Pseudonymization is a process by which identifying information of a data subject is removed while retaining a link between multiple records pertaining to the data subject. [ISO/ TS 25237]
Pseudonymization, irreversible	The process of Pseudonymization is said to be irreversible if, for any passage from identifiable to pseudonymous, it is computationally infeasible to trace back to the original identifier from the pseudonym [ISO /TS 25237]
Registration Authority (RA)	Entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA). [IETF/RFC 3647]

Registry	The Client Registry (CR) is a central storage that maintains the administrative and demographic details of all the clients (individuals, including citizens, expatriates, and visitors) who receive healthcare services in the Kingdom of Saudi Arabia. The details maintained about the client includes names, national Identifiers, gender, birth details, nationality and other relevant attributes. The information maintained about the clients will be retrieved form the corresponding source of truth. The Provider Registry (PR) is a central storage that maintains the administrative details of all the healthcare providers who deliver healthcare services in the Kingdom of Saudi Arabia. The details maintained about a provider includes names, national Identifiers, gender, specialty, organizations he works for, contact details and other relevant attributes. The information maintained about the providers will be retrieved form the corresponding source of truth. The Organization Registry (OR) is a central storage that maintains the administrative details of all the healthcare organizations operating in the Kingdom of Saudi Arabia. The details maintained about an organization includes names, national Identifiers, services, departments, type and other relevant attributes. The information maintained about the organizations will be retrieved form the corresponding source of truth.
Regulated Health Professional	Person who is authorized by a nationally recognized body [SCFHS, Saudi Commission for Health Specialties] and qualified to perform certain health services. EXAMPLES: Physicians, registered nurses, and pharmacists [e.g. Saudi-licensed practitioners] NOTE 1: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations, and other formally and nationally recognized organizations. They MAY be exclusive or non-exclusive in their territory. NOTE 2: A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognized health professional registration bodies to exist. [ISO 17090]
Remote Access	Access to the Saudi Health Information Exchange from a device connected to a HIE node and situated outside of the physical and environmental control of the corresponding PHCS. This would typically include access to a HIE node from a remote location such as from home.
Reportable Event	A Reportable Event is an action (or lack of action), suspected or confirmed, that violates Saudi Health Information Exchange policies and procedures for accessing or using PHI managed by the Saudi Health Information Exchange. Such violations may be unintentional or intentional.
Role	Set of competences and/or performances that are associated with a task. [ISO/ TS 21298]
Saudi Health Information Exchange (SeHE)	The Saudi organization known as SeHE that delivers capabilities to enable the electronic sharing of health-related information and health-related services across the country of Saudi Arabia.
Saudi Health Information Exchange Systems Service Provider	An entity operating and managing the core services supporting the Saudi Health Information Exchange systems (e.g. Provider Registry, Client Registry, Clinical Data Repository, etc.)
Saudi Health Information Exchange Systems	All hardware and software components providing the infrastructure to enable the Saudi Health Information Exchange. HIE nodes are not components of the Saudi Health Information Exchange Systems.

Secondary use of personal data (Repurposing data)	Secondary use of personal data is any use different from primary use [ISO/ TS 25237] NOTE: For example, the primary use is for treating the individual patient; we can consider that the secondary use is for purposes other than treating the individual patient, such as for research or marketing.
Security	Combination of availability, confidentiality, integrity, and accountability. [ENV 13608-1]
Security audit	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures. [ISO 7498 – 2]
Sensitive PHI	PHI Subject to heightened confidentiality requirements (at least including but not limited to mental health, substance abuse, genetic information, sexually transmitted disease, reproductive health).
Sensitivity	Measure of importance assigned to information to denote its need for protection. [ISO 13606-4]
Shall	Whenever occurs in this policy, **SHALL** means the action must be taken.
Should	Whenever occurs in this policy, **SHOULD** means it is a recommendation that an action ought to be done, but it is not required.
Special Notice / Notice of privacy practice	Notice given to patients by a Participating Healthcare Subscriber explaining the Saudi Health Information Exchange and the patient's rights regarding disclosure of PHI from the Saudi Health Information Exchange.
Sponsored Healthcare Provider	Health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her healthcare community and sponsored by a regulated healthcare organization. [ISO /IS 17090] NOTE: in Saudi Arabia, one example would be, a Healthcare Provider that is licensed in another country and contracted as a temporary provider by a local regulated healthcare organization
Subject of Care	Person who receives health related services and has health information contained within the Saudi Health Information Exchange; any person who uses or is a potential user of a healthcare service; subjects of care may also be referred to as patients, healthcare consumers or Subject of Cares [ISO/ TS 22220]
Subject of Care Agent	Parent, guardian, or other legal representative [of the subject of care] [ISO TS13606-4]
Subscriber	A party who receives a credential or token from a certification service provider. [NIST 800-63-1]
Trusted Third Party	Third party who is considered trusted for purposes of a security protocol.

3. SAUDI HEALTH INFORMATION EXCHANGE PURPOSE OF USE POLICY

3.1 PURPOSE

The purpose of this policy is to define permissible uses of the Saudi Health Information Exchange such as Patient Care, Public Health, and Quality.

3.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations who have access to the Saudi Health Information Exchange managed health records, including

- Participating Healthcare Subscriber (PHCSs),
- their Business Associates,
- any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI,
- any Saudi Health Information Exchange Systems Service Provider, and
- any other subcontractors of the Saudi Health Information Exchange.

This policy applies to all information provided to or retrieved from the Saudi Health Information Exchange systems.

3.3 POLICY

Personal Health Information (PHI) will primarily be made available on the Saudi Health Information Exchange for purposes of Treatment, Healthcare Operations, and Public Health:

3.3.1 Uses That SHALL Be Permitted

The following uses of the Saudi Health Information Exchange systems **SHALL** be permitted and **SHALL** be subject to all applicable Saudi Health Information Exchange Policies:

3.3.1.1 TREATMENT

3.3.1.1.1 Clinical Care Provision to an Individual Subject of Care

To inform individuals or processes responsible for providing healthcare services to the Subject of Care

3.3.1.1.2 Emergency Care Provision to an Individual Subject of Care

To inform individuals needing to provide healthcare services to the Subject of Care urgently and possibly needing to override the policies and consents pertaining to clinical care provision.

3.3.1.1.3 Support of Care Activities within the Provider Organization for an Individual Subject of Care

To inform individuals or processes enabling others [healthcare providers who have a legitimate right to provide care] to provide healthcare services to the Subject of Care.

3.3.1.1.4 Subject of Care Uses

To inform the Subject of Care in support of his or her own interests.

3.3.1.2 OPERATIONS

3.3.1.2.1 Health Service Management and Quality Assurance

To inform individuals or processes responsible for determining the availability, quality, safety, equity and cost-effectiveness of healthcare services.

3.3.1.3 PUBLIC HEALTH

3.3.1.3.1 Public Health Surveillance, Disease Control

To inform individuals or processes with responsibility to monitor populations or sub-populations for significant health events and then intervene to provide healthcare or preventive care services to relevant individuals.

3.3.1.3.2 Public Safety Emergency

To inform individuals with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to one or more members of the public and possibly needing to over-ride the policies and consents pertaining to Public Health Surveillance and Disease Control.

3.3.1.3.3 Population Health Management

To inform individuals or processes with responsibility to monitor populations or sub-populations for health events, trends or outcomes in order to inform relevant strategy and policy.

3.3.2 Uses That MAY Be Permitted

The following uses of the data managed by Saudi Health Information Exchange systems **MAY** be permitted and **SHALL** be subject to the Secondary Use Policy constraints or further use constraints:

3.3.2.1 RESEARCH

To support the discovery of generalizable knowledge.

3.3.2.2 EDUCATION

To support learning and professional development.

3.3.2.3 PAYMENT

To inform individuals or processes responsible for enabling the availability of resources or funding or permissions for providing healthcare services to the Subject of Care. Such uses will be subject to approval by the Council of Health Services (CHS).

3.3.3 Uses That SHALL NOT Be Permitted

The following use of the Saudi Health Information Exchange systems **SHALL NOT** be permitted unless there is a valid court order to disclose PHI:

3.3.3.1 MARKET STUDIES

To support the discovery of product or organization specific knowledge.

3.3.3.2 LEGAL INVESTIGATION OR INQUIRY

To inform persons or processes responsible for enforcing jurisdictional legislation, or undertaking legal or forensic investigation.

The following uses of the Saudi Health Information Exchange systems **SHALL NOT** be permitted at this time:

3.3.3.3 NOT SPECIFIED OR UNKNOWN

Disclosure on the basis of authorizations not requiring a purpose to be declared, or where the purpose is not known, or purposes for which the other categories in this clause do not apply (e.g. unless a purpose as described above is declared, disclosure **SHALL NOT** be permitted).

3.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

4. SAUDI HEALTH INFORMATION EXCHANGE INFORMATION SECURITY POLICY

4.1 PURPOSE

The purpose of this policy is to ensure that the information security is conducted in a manner that protects personal health information and supports the availability, confidentiality, integrity, and accountability of the Saudi Health Information Exchange shared clinical information.

4.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including

- Participating Healthcare Subscribers(PHCSs),
- Their business associates,
- Any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- Any Saudi Health Information Exchange Systems Service Provider, and
- Any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information provided to or retrieved from Saudi Health Information Exchange systems.

4.3 POLICY

1. PHCSs **SHALL** implement policies and protections for Access Control, Automatic Logoff, Audit Log, Emergency Access, Integrity, Authentication, and Encryption. A list of policies and protections **SHALL** be requested and checked when onboarding participating sites. A minimal set **SHALL** be specified in the policy, and additional requirements may be included in the Data Use Agreement.
2. All Saudi Health Information Exchange system components **SHOULD** be managed and operated in conformance with the ISO/TC 215 standard: "*ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002*".
3. Data **SHALL NOT** be deleted at any time from the Saudi Health Information Exchange. Data **MAY** be amended to accommodate corrections.
4. All Saudi Health Information Exchange Systems **SHALL** be managed in accordance with one of: ISO 27000, SAS70/ SSAE 16, supporting physical safeguards, clearance, access, supervising those with access and other core secure management practices.
5. All Saudi Health Information Exchange systems **SHALL** implement contingency and disaster recovery plans to assure availability and integrity of Saudi Health Information Exchange managed health information.
6. Retention time for Saudi Health Information Exchange managed PHI is indefinite.

7. All Saudi Health Information Exchange systems **SHALL** encrypt communications when exchanging Personal Health Information. Encryption **SHALL** minimally support one of the following:

   7.1. AES

   7.2. 3DES

8. All Saudi Health Information Exchange systems **SHALL** implement intrusion detection measures.
9. The Saudi Health Information Exchange and the PHCSs **SHALL** require personnel training in privacy and confidentiality for all personnel handling health information that is directly or indirectly involved in the support of Saudi Health Information Exchange systems.
10. A privacy/security officer **SHALL** be designated at the Saudi Health Information Exchange, as well as in the PHCSs.
11. The Saudi Health Information Exchange and the PHCSs **SHALL** implement a personnel sanction policy for inappropriate use, transmission, copy or disclosure of Saudi Health Information Exchange information and services.
12. PHCSs **SHOULD** have contingency plans in place for extended downtime periods.

4.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

5. SAUDI HEALTH INFORMATION EXCHANGE SUBJECT OF CARE RIGHTS POLICY

5.1 PURPOSE

The purpose of this policy is to define Subjects of Care and healthcare consumer expectations that will govern the design and implementation of the Saudi Health Information Exchange Systems.

5.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to the Saudi Health Information Exchange managed Personal Health Information, including:

- Participating Healthcare Subscribers (PHCSs),
- their Business Associates,
- any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI,
- any Saudi Health Information Exchange Systems Service Provider, and
- any other subcontractor of the Saudi Health Information Exchange.

This policy applies to all PHI provided to or retrieved from the Saudi Health Information Exchange systems.

5.3 POLICY

1. The Subject of Care or the Subject of Care Agent **SHALL** be able to access the Subject of Care's relevant personal health information contained within the Saudi Health Information Exchange.
    1.1. Such information **SHOULD** be available to the Subject of Care conveniently.
    1.2. Such information **SHALL** be available to the Subject of Care affordably.
    1.3. Subjects of care **SHOULD** have a means of direct, secure access to their relevant health information that does not require physician or institutional mediation.
    1.4. The Subject of Care **MAY** have access to the Saudi Health Information Exchange data through approved services. .
    1.5. All Subject of Care accessible Personal Health Information services **SHALL** assure that the identity of the Subject of Care is vetted in accordance with the Saudi Health Information Exchange Identity Management Policy.
    1.6. Subjects of Care **SHOULD** be able to supplement, and request amendment of their Personal Health Information without fees or burdensome processes.
    1.7. Annotation of information **SHALL** document proper identification of the source of the annotation.

2. The Saudi Health Information Exchange **SHOULD** make information available to Subjects of Care regarding how their personal health information could be used, who could have access to it, and under what circumstances it could be disclosed.
3. Implementation of the Health Information Exchange **SHOULD** be accompanied by a significant education program so that individuals understand how the network will operate, what information will or will not be available on the network, the value of the network, its privacy and security protections, how to participate in the exchange and the rights, benefits and remedies afforded to them. These efforts **SHALL** include outreach to those without health insurance coverage.
4. Each Subject of Care **MAY** receive information generated by the PHCS from their provider explaining the Saudi Health Information Exchange services and the Subject of Care's rights regarding use and disclosure of PHI from the Saudi Health Information Exchange systems ("Special Notice") at the Subject of Care's first visit following the provider's participation as a Saudi Health Information Exchange PHCS.
    4.1. The Special Notice **SHOULD**
        4.1.1. Be provided by a provider to a Subject of Care at least once (e.g. in the entrance of a care facility, on a facility website, or when providing an account to the consumer portal), and
        4.1.2. Contain information about the procedure to opt out from the Saudi Health Information Exchange.
    4.2. Materials **SHOULD** minimally include
        4.2.1. Information regarding purpose of the exchange,
        4.2.2. Benefits,
        4.2.3. How data are protected,
        4.2.4. How data can be used, and
        4.2.5. Contact information to the Saudi Health Information Exchange to obtain more information.
5. PHI **MAY** be shared unless the Subject of Care opts out of the Saudi Health Information Exchange.
6. All efforts **SHALL** be taken to implement and maintain systems for Health Information Exchange that protect the integrity, security, privacy, and confidentiality of a Subject of Care's information.
7. The governance of the Saudi Health Information Exchange **SHALL** be transparent.
8. Rights and process for complaints if the Subject of Care suspects a breach:
    8.1. In the case of a suspected breach, the Subject of Care that is the data subject of such a breach **MAY** request an investigation (see the Breach Notification Policy). Such a request **SHALL** be issued by the Subject of Care or by the authorized Subject of Care agent should the Subject of Care be unable to do so, and **SHALL** be directed to the Health Information Management Personnel or HIE designated resources.

8.2. In the case of a breach identified and investigated through the Saudi Health Information Exchange, the Subject of Care that is the data subject of such a breach **SHOULD** be notified.

9. Request a report of electronic disclosures:

9.1. A Subject of Care **MAY** request a report of electronic disclosures for information accessed through the Saudi Health Information Exchange where the Subject of Care is the data subject. Such a request **SHALL** be issued by the Subject of Care or by the authorized Subject of Care agent should the Subject of Care be unable to do so, and **SHALL** be directed to the local Health Information Management Personnel or Saudi Health Information Exchange designated resources. This report of electronic disclosures **SHALL** include information such as:

9.1.1. date of disclosure,

9.1.2. name of the entity or person that received the disclosure, and

9.1.3. name of the entity or person that made the disclosure.

9.2. The Subject of Care **SHOULD** be provided notification of break-glass accesses to his/her Personal Health Information. (e.g., Subject of Care notification of break-glass accesses via cell phone number or e-mail).

10. Procedures and instructions for how to opt out of the Saudi Health Information Exchange **SHALL** be provided to the Subject of Care or to the authorized Subject of Care agent should the Subject of Care be unable to review or comprehend the instructions.

11. The Subject of Care may choose to opt out of the Saudi Health Information Exchange. In order to exercise this option, the Subject of Care **SHALL** make the opt out request and deliver this request to an authorized organization. The organization **SHALL** verify the authenticity of the request, approve the request, and provide any associated counseling regarding potential clinical risks.

12. The Subject of Care **MAY** choose to opt back in to the Saudi Health Information Exchange at any time.

13. All opt out requests **SHALL** be issued by the Subject of Care or by the authorized Subject of Care agent in the event that the Subject of Care is unable to do so. The healthcare provider **MAY** process the request on behalf of the Subject of Care.

14. Personal health information **SHALL NOT** be disclosed **EXCEPT** for the purposes of:

14.1. Treatment

14.1.1. Clinical care provision to an individual Subject of Care

14.1.2. Emergency care provision to an individual Subject of Care

14.1.3. Support of care activities within the provider organization for an individual Subject of Care

14.2. Subject of care uses

14.3. Operations

14.3.1. Health service management and quality assurance

14.4. Public Health

14.4.1. Public Health Surveillance, Disease Control

14.4.2. Public safety emergency

14.4.3. Population health management

5.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

6. SAUDI HEALTH INFORMATION EXCHANGE IDENTITY MANAGEMENT POLICY

6.1 PURPOSE

The purpose of this policy is to ensure that the identities of the individuals and entities interacting with the Saudi Health Information Exchange are assured to enable a data processing system to recognize entities.

6.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including

- Participating Healthcare Subscribers (PHCSs),
- Their business associates,
- Any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- Any Saudi Health Information Exchange Systems Service Provider, and
- Any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information provided to or retrieved from Saudi Health Information Exchange systems.

6.3 POLICY

1. Healthcare Organization [e.g. hospital] and Business Associate [e.g. supporting quality management Organization] systems connecting to the Saudi Health Information Exchange systems **SHALL** be subject to Trusted Third Party Attestation for the issuance of organization system digital certificates. Self-signed certificates or those issued by another PKI **SHALL NOT** be used.
2. Individual users accessing the Saudi Health Information Exchange systems **SHALL** be subject to Trusted Attestation for the issuance of identity credentials.
3. Digital certificates used for authentication or digital signatures **SHALL** be issued by the National Center for Digital Certification.
4. Federated identity providers **MAY** apply to authenticate users to the HIE on a case by case basis.
5. Requirements for Proof of Identity for individuals are as follows:
    5.1. Identity Proofing for all individuals **SHALL** include a face-to-face attestation of the individual's identity.
    5.2. Identity proofing for all individuals **SHALL** require a valid government issued photographic identification (i.e. passport, driver's license, military ID, national ID, or Residency Permit for Non-Saudi), or a government-recognized biometric identification.

5.2.1. For Subject of Care this same proofing **SHALL** be required, but Antecedent Data (e.g. from a prior health visit) **MAY** be used as the face-to-face attestation of the individual's identity. CHS **SHALL** be responsible to determine what constitutes trustworthy antecedent data.

5.2.2. For Subject of Care agent, additional proofing **SHALL** be provided by government issued Family Card or other legal document indicating authorization to act on behalf of the Subject of Care for medical decisions.

5.2.3. Identity Proofing for Regulated Health Professional **SHALL** require evidence of a current license issued by the Saudi Commission for Health Specialties in addition to the Identity Proofing requirements that apply to all individuals (as described in 5.1 above).

5.2.4. Identity Proofing for Non-regulated Health Professionals **SHALL** require verification of employee ID or letter from employer on employer letterhead indicating current employment status where the identifier is not issued directly by the employer in addition to the Identity Proofing requirements that apply to all individuals (as described in 5.1 above).

5.2.5. Identity Proofing of a Sponsored Healthcare Provider **SHALL** require a letter from a Regulated Healthcare professional or authorized representative of a sponsoring regulated health organization to establish that they are active in their healthcare community OR evidence of current credentials issued by the Saudi Commission for Health Specialties in addition to the Identity Proofing requirements that apply to all individuals (as described in 5.1 above).

5.2.6. For other users (e.g. researchers), antecedent data **MAY** be used to provide limited access to the Saudi Health Information Exchange.

6. Identity Proofing requirements for Organization's systems are as follows:

6.1. Identity Proofing of an Organization's secure node (HIE node) **SHALL** require attestation by an individual identified by the organization as authorized to provide such attestation.

6.1.1. A letter on the entity letterhead signed by a corporate officer **SHALL** identify a representative of the entity authorized to validate and request organization or device certificates on behalf of the entity that will be used to provision HIE node certificates.

6.2. The Organization responsible for the system **SHALL** provide proof of a current license to conduct the healthcare or healthcare associated business, a valid commercial registration document, or a nationally-recognized government entity.

7. Electronic identity credentials **SHALL NOT** be issued until an agreement addressing the credential holder's requirements is completed and signed. This may for example include an agreement to terms and conditions for online registration processes for individual users.

8. Procedures for account revocation upon employee severance for any employee who was issued an individual identity credential to access the Saudi Health Information Exchange systems **SHALL** be implemented by the PHCS.

8.1. Notification to the Saudi Health Information Exchange **SHOULD** be issued within two business days.

8.2. Acknowledgment of receipt of notification **SHOULD** be issued upon receipt.

8.3. Account revocation by the PHCS and the Saudi Health Information Exchange **SHOULD** be implemented within two business days after notification.

9. Procedures for account update upon employee role modification for any employee who has been issued an individual identity credential to access the Saudi Health Information Exchange systems, **SHALL** be implemented by the PHCS.

9.1. Notification to the Saudi Health Information Exchange **SHOULD** be issued within two business days.

9.2. Acknowledgment of receipt of notification **SHOULD** be issued upon receipt.

9.3. Account update by the PHCS and the Saudi Health Information Exchange **SHOULD** be implemented within two business days after notification.

10. Subscriber [NIST 800-63-1] agreements **SHALL** include the requirement to protect the Subscriber identity credential.

11. Subscribers [NIST 800-63-1] **SHALL** notify a Saudi Health Information Exchange authorized Registration Authority if their digital identity is lost, stolen, or otherwise known to be compromised. This **SHALL** result in a revocation request and request for a new digital identity.

6.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring policy maintenance.

7. SAUDI EHEALTH INFORMATION EXCHANGE AUTHENTICATION POLICY

7.1 PURPOSE

The purpose of this policy is to ensure that systems and individuals interacting with the Saudi Health Information Exchange systems are known through the process of reliable security identification of subjects by incorporating an identifier and its authenticator.

7.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including:

- Participating Healthcare Subscriber (PHCSs),
- their business associates,
- any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- any Saudi Health Information Exchange Systems Service Provider, and
- any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information provided to or retrieved from Saudi Health Information Exchange systems.

7.3 POLICY

1. Emergency Access **SHALL** be supported by all HIE node systems accessing the Saudi Health Information Exchange as a break-glass with audit and review of these actions, in accordance with the Audit Policy. Notification to the subject of care in the event of break-glass access **SHOULD** be provided by the Security and Privacy Officer of the Saudi Health Information Exchange.
2. Automatic user logoff **SHALL** be supported by all HIE nodes accessing the Saudi Health Information Exchange. The user sessions of the HIE node **SHOULD** be automatically logged off after no more than 30 minutes of inactivity.
3. All HIE Nodes exchanging personal health information **SHALL** implement a node authentication mechanism compliant with Transport Layer Security (TLS) [Internet Engineering Task Force (IETF): Transport Layer Security (TLS) 1.0 (RFC 2246)].
4. All Saudi Health Information Exchange system remote access by individual users **SHALL** require multi-factor authentication.
5. PHCSs **SHOULD** assert multi-factor authentication for remote access to their systems (from outside of the physical control of the organization), if the accessed system enables access to the Saudi Health Information Exchange.

6. A Registry of PHCSs within the Saudi Health Information Exchange **MAY** include primary contact information of registered members, roles/privilege information, and identity attributes of providers, organizations, and systems. The primary contact information for the data in the directories supplied to the Registry **SHOULD** minimally include a primary contact name and any associated contact phone numbers.
    6.1. For Regulated Health Professionals, this information, along with health practitioner's license revocation information **SHALL** be sourced through the Saudi Commission for Health Specialties database.
    6.2. For Healthcare Organizations, this information **SHALL** be provided by the corresponding sector-regulating body.
    6.3. For employees and staff of PHCSs and their Business, this information **SHALL** be provided by the designated contact within the PHCS.
    6.4. All Non-regulated Health Professionals **SHALL** be managed as employees of healthcare organizations.
7. The Saudi Health Information Exchange **SHALL** require unique identification of the individuals (employees, care providers, subjects of care, subjects of care agents), systems (HIE node, HIE system, or the Application), and Organizations accessing the information in the Saudi Health Information Exchange.
8. The user identity, role, and affiliation must be checked for both revocation and expiration at the time of logon to the system. If any of these has been revoked or has expired, access **SHALL** be denied.
9. Any system providing access to the Saudi Health Information Exchange **SHALL** be responsible for verification of credentials. Verification implies that:
    9.1. the credential is issued by a trusted third party,
    9.2. the credential is current,
    9.3. the credential is not suspended or revoked, and
    9.4. the credential type is appropriate (for example, physician or pharmacist).

7.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

8. SAUDI HEALTH INFORMATION EXCHANGE CONSENT AND ACCESS CONTROL POLICY

8.1 PURPOSE

The purpose of this policy is to define who and how individuals and systems can access the Saudi Health Information Exchange managed data. This policy specifies means of ensuring that the resources of a data processing system can be accessed only by authorized entities (individuals or machines interacting with the Saudi Health Information Exchange system) in authorized ways. This policy also defines the circumstances in which a Subject of Care can permit or withhold the use and disclosure of the Saudi Health Information Exchange accessible health information.

8.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including:

- Participating Healthcare Subscriber (PHCSs),
- their business associates,
- any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- any Saudi Health Information Exchange Systems Service Provider, and
- any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information provided to or retrieved from Saudi Health Information Exchange systems.

8.3 POLICY

1. HIE node applications must have successfully completed access control testing conducted by Saudi Health Information Exchange approved bodies. Applications that have not yet completed this testing **MAY** be considered on a case-by-case basis.
2. Access to personal health information (PHI) through the Saudi Health Information Exchange systems requires verification of consents managed according to this Saudi Health Information Exchange Consent and Access Control Policy.
3. When the Saudi Health Information Exchange is used for purposes of treatment, the health professional seeking access **SHOULD** have a treatment relationship with the Subject of Care.
4. Saudi Health Information Exchange **SHALL** define the Specific Personal Health Information that **SHALL** be made available by each HIE node. All relevant information flows to the Saudi Health Information Exchange, except where law or policies of the PHCS prohibit it. Such PHCS policies that would be in effect **SHALL** be disclosed to the HIE during the on-boarding process. All new policies established by the PHCS after they join the HIE **SHALL** be disclosed to the HIE. If the policy is not acceptable to the HIE, the HIE **MAY** suspend access to the Health Information Exchange.

5. In the case where the Subject of Care has opted out of the Saudi Health Information Exchange, all relevant information **SHALL** continue to flow to the Saudi Health Information Exchange.
6. Once the Subject of Care has opted out of the Saudi Health Information Exchange, access to information/documents related to that subject of care **SHALL** be restricted to emergency situations,
7. Only physicians **SHOULD** be able to force access to all the data, including data for a Subject of Care that has opted out of the Saudi Health Information Exchange, by "breaking the glass", which **SHALL** trigger notification and after-the-fact review.
8. Access controls enforcement, including verification of Opt-Out status, is performed at the time of use and disclosure.
9. The individual that accesses the PHI **SHALL** be responsible for protecting that information or disseminating that information.
10. Sensitive personal health information/documents that are afforded special protection above and beyond protections afforded to generic Personal Health Information **SHALL** be marked as such.
11. The Saudi Health Information Exchange **MAY** offer transformation services to assist the PHCS with the identification of sensitive PHI based upon information source on a case-by-case basis. The method of transformation **SHALL** be approved by the Saudi Health Information Exchange governing body. This transformation **SHOULD** involve dual publication of sensitive PHI and their cleansed version in the Saudi Health Information Exchange with different sensitivity marking when the remaining PHI is significant to continuity of care.
12. A Health Professional who agrees to a restriction requested by a Subject of Care must convey such restriction to the Saudi Health Information Exchange systems using the associated policy confidentiality code object identifier (e.g. in a registered document, such as a Basic Patient Privacy Consent (BPPC) document), identifying the policy confidentiality code associated with the sensitivity type.
13. Systems providing access to information/documents in the Saudi Health Information Exchange **SHALL** enforce protections associated with content marked as sensitive.
    13.1. Sensitive personal health information **SHALL** be restricted to specialized care providers as identified by their provider role.
    13.2. Sensitive personal health information **MAY** be accessed with a "break glass" option for defined roles of health professionals as identified by the Saudi Health Information Exchange which **SHALL** trigger notification to the Security and Privacy Officer, and after-the-fact review in accordance with the Audit Policy.
    13.3. The existence of such sensitive personal health information in the Saudi Health Information Exchange **SHOULD** only be declared to defined roles of health professionals as identified by the Saudi Health Information Exchange.
    13.4. In the case of risks to the care providers (e.g., HIV), a generic warning **MAY** be issued about the risk.

14. When a Subject of Care chooses to opt out of the Saudi Health Information Exchange, this **SHALL** be recorded in the Saudi Health Information Exchange.
15. All Saudi Health Information Exchange individual users **SHALL** be associated with at least one standard healthcare role.
    15.1. Administrative personnel **SHOULD** only access administrative information.
    15.2. Clinical information is restricted to care professionals, defined by a set of roles.
    15.3. For Regulated Health Professional, the role **SHALL** be defined by the role code associated with the license as maintained by the Saudi Commission for Health Specialties.
    15.4. For Non-Regulated Health Professional, the role **SHALL** reflect one of the standard roles identified by the Saudi Health Information Exchange as determined by the PHCS responsible for the user's interactions with Saudi Health Information Exchange systems.
16. Access through "Provider Portals" or "Client Portals".is permitted subject to:
    16.1. The portal user SHALL be contractually bound to abide by all Saudi Health Information Exchange policies.
    16.2. Agreements with the portal user SHALL be executed either with the Saudi Health Information Exchange or with a Participating Healthcare Subscriber (PHCS) that is already bound to these policies.
17. Provider Registry access controls **SHALL** restrict public access to the following attribute(s), unless specifically authorized by the provider:
    17.1. email,
    17.2. mobile phone number, and
    17.3. home address.
18. All Participating Healthcare Subscribers (PHCSs) **SHOULD** establish organization policies to assure compliance with Saudi Health Information Exchange policies. These policies are subject to review and audit in accordance with the Audit Policy.

8.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

9. SAUDI HEALTH INFORMATION EXCHANGE AUDIT POLICY

9.1 PURPOSE

The purpose of this policy is to ensure that the security and confidentiality of Subject of Care data transmitted through the Saudi Health Information Exchange are monitored/tracked through privacy/security audits.

9.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including

- Participating Healthcare Subscriber (PHCSs),
- Their business associates,
- Any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- Any Saudi Health Information Exchange Systems Service Provider,
- Any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information (PHI) provided to or retrieved from Saudi Health Information Exchange systems.

9.3 POLICY

1. All Saudi Health Information Exchange systems and HIE nodes **SHALL** implement technical processes that accurately record any activity related to access, creation, modification and deletion of electronic PHI.
   1.1. HIE Node applications **SHALL** have successfully completed audit log testing, conducted by Saudi Health Information Exchange approved bodies. Applications that have not yet completed this testing will be considered on a case-by-case basis.
   1.2. HIE Node applications **SHALL** be subject to conformance testing and certification for audit log compliance by Saudi Health Information Exchange approved bodies.
   1.3. HIE Node activity **SHALL** be logged locally, and shall be maintained in a persistent database.
   1.4. HIE Node applications **SHALL** have the ability to generate an electronic report of PHI exchanged.
      1.4.1. This capability **SHALL** be demonstrated when integrating the HIE Node to the Saudi Health Information Exchange
      1.4.2. Testing of this capability **SHALL** be conducted by the Saudi Health Information Exchange.

1.5. The PHCS **SHOULD** be able to audit all access to PHI that is stored locally.

2. The Saudi Health Information Exchange systems **SHALL** support interoperability requirements conformant to ISO 27789 Audit Trails for EHRs (e.g., IHE Audit Trails and Node Authentication, ATNA).
3. The HIE nodes exchanging PHI **SHOULD** support interoperability requirements conformant to ISO 27789 Audit Trails for EHRs (e.g., IHE Audit Trails and Node Authentication, ATNA).
4. As a part of log-in monitoring, an audit log **SHALL** be created to record when a person logs on to the network or a software application of the Saudi Health Information Exchange. This includes all attempted and failed logons.
5. For purposes of information use or disclosure, privacy and security audit **SHALL** include documentation of the following :
   5.1. the date and time of the request,
   5.2. the reason for the request,
   5.3. a description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party,
   5.4. whether the request was performed as a “break-glass”,
   5.5. whether the requested information was marked as sensitive PHI,
   5.6. the ID of person/system requesting the access to PHI, and
   5.7. the ID of the person/system generating response for PHI access requests.
6. Audit logs **SHOULD** either be in human readable form or translatable by some easy-to-use tool to be in human readable form.
7. Audit logs **SHOULD** be retained for the same duration as the retention time required of Saudi Health Information Exchange managed PHI.
8. All HIE node systems and Saudi Health Information Exchange systems **SHALL** be configured to generate logs of all events (e.g. login, logoff, access events, denial events, etc.) as supported by installed products to enable further investigation and traceability.
   8.1. The audit log review of information systems **SHALL** include software applications, network servers, firewalls and other network hardware and software.
   8.2. All system logs **SHALL** be reviewed by respective organization’s privacy and security officer.
   8.3. The generated audit logs **SHALL** be reviewed on a regular basis, at least quarterly, in order to detect improper use based on audit criteria developed in advance.
   8.4. All anomalies **SHALL** be documented and appropriate mitigating action **SHALL** be taken and documented.
   8.5. The Saudi Health Information Exchange requires that this documentation **SHALL** be retained a minimum of ten years.

8.6. All system logs **SHALL** be provided to HIE Security and Privacy Officer upon request for any investigation

9. An external systems auditor is subject to approval by the Saudi Health Information Exchange governing body:

   9.1. The external systems auditor **SHALL** have no conflict of interest.

   9.2. The external systems auditor **SHALL** have qualifications and accreditations as applicable and as required by the Saudi Health Information Exchange.

10. Privacy and security audit review **SHALL** support inquiry by patients or providers. Response to privacy and security audit review **SHALL** be required of all HIE nodes and Saudi Health Information Exchange systems maintaining primary audit records related to the Saudi Health Information Exchange.

11. External audits of the Saudi Health Information Exchange **SHALL** be conducted at least annually as a minimum requirement and when any major system or business change occurs. Comprehensive audit procedures **SHOULD** be developed, documented, and available. The evaluation **SHALL** include:

   11.1. the documentation of the evaluation SHALL be retained for ten (10) years,

   11.2. the generation of a compliance audit findings report, and

   11.3. documentation that an identified deficiency

      11.3.1. has been addressed,

      11.3.2. has been addressed in order of priority, or

      11.3.3. represents a risk that the organization is willing to accept (e.g., unlikely to occur, minimal damage to the organization, expensive to mitigate).

12. The Saudi Health Information Exchange audit record repository system **SHALL** support the following queries either for all instances or constrained to activity originating from an HIE Node:

   12.1. list all users that accessed or modified a given Subject of Care's information over a period of time,

   12.2. list all Subjects of Care whose health information was accessed by a given user/system over a given period of time,

   12.3. list all break-glass events,

   12.4. list all access events where the user is not listed as a provider in any patient records, and

   12.5. list events that request information marked as sensitive.

13. For purposes of data authentication the use of a valid date/time stamp is required.

   13.1. All HIE nodes exchanging PHI **SHALL** implement the time synchronization mechanism specified by the Saudi Health Information Exchange to assure that timestamps and audit logs are synchronized.

14. Audit logs repository **SHALL** be secured in accordance with the Saudi Health Information Exchange Information Security Policy. Access to system audit log analyzing tools and audit logs **SHALL** be safeguarded to prevent misuse or compromise.
15. Saudi Health Information Exchange audit logs access **SHALL** be restricted only to privacy and security officers approved by the Saudi Health Information Exchange governing body.

9.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

10. SAUDI HEALTH INFORMATION EXCHANGE BREACH NOTIFICATION POLICY

10.1 PURPOSE:

The purpose of this policy is to define policy surrounding identification, investigation, notification, and mitigation of a breach within the Saudi Health Information Exchange system.

10.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, to all individuals and organizations that have access to Saudi Health Information Exchange managed health records, including

- Participating Healthcare Subscriber (PHCSs),
- their business associates,
- any subcontractors of business associates that perform functions or provide services involving the use and disclosure of personal health information,
- any Saudi Health Information Exchange Systems Service Provider, and
- any other subcontractor of Saudi Health Information Exchange.

This policy applies to all personal health information provided to or retrieved from Saudi Health Information Exchange systems.

10.3 POLICY

10.3.1 Access Monitoring

1. The Saudi Health Information Exchange privacy and security officer or designee **SHALL** monitor PHCSs access to the Saudi Health Information Exchange at least monthly by reviewing the Saudi Health Information Exchange systems audit reports.
2. The Saudi Health Information Exchange privacy and security officer **SHALL** contact the PHCSs to review any suspicious activity. In case of a Reportable Event, the privacy and security officer of the PHCS **SHALL** investigate the suspicious activity and generate a report of the event (see 10.3.2).

10.3.2 Events Notification

1. The Saudi Health Information Exchange and PHCSs are obligated to create a notification of all Reportable Events involving the PHI managed by the Saudi Health Information Exchange.
   1.1. The PHCS's individual **SHALL** notify the organization's privacy and security officer(s) within two (2) business days of the discovery of a Reportable Event.
   1.2. The PHCS privacy and security officer(s) or PHCS designated person **SHALL** communicate the review of the Reportable Event to the Saudi Health Information

Exchange within two (2) business days of notification, documenting whether or not there is a need for further investigation.

2. Subject of care initiated notification of Reportable Events **MAY** be accepted by the Saudi Health Information Exchange privacy and security officer.
3. The Saudi Health Information Exchange **SHALL** establish and publish a process for filing reports to inform and guide those required or eligible to file Saudi Health Information Exchange related Reportable Events. This process will take into account the private nature of Subject of Care reportable events. All reports **SHALL** follow the aforementioned process.

10.3.3 Reportable Event Review and Breach Investigation

1. The privacy and security officer of the Saudi Health Information Exchange or designated person receiving the Reportable Event Report **SHOULD** log the Reportable Event, acknowledge receipt of the Reportable Event Report to the person or system filing it, inform the affected PHCS privacy and security officer(s) of the event if they do not already have knowledge of it, and begin a review of the event.
2. Upon receipt of a Reportable Event Report, the report **SHALL** be reviewed by the Saudi Health Information Exchange privacy and security officer to determine whether or not a review is required.
3. If it is determined that no further action is needed, this determination **SHALL** be communicated to the originator of the Reportable Event Report, thus terminating the review process. Such decisions are subject to review through internal or external audit. Time and scope constraints for the review and mitigation actions taken on the Reportable Event Report of a confirmed breach will depend on the nature of the risk and sensitivity of information.
    3.1. In the case of an imminent threat to data security in the Saudi Health Information Exchange systems, the Saudi Health Information Exchange privacy and security officer **SHALL** take immediate actions to secure the data.
    3.2. Suspension of access privileges **MAY** be enforced until the source has mitigated the issue locally or possibly permanently as considered on a case-by-case basis.
    3.3. PHCS **SHALL** fully cooperate with the Saudi Health Information Exchange Security and Privacy Officer in identification and mitigation of the threat that could result in a breach event.
    3.4. Once the review is done, the Saudi Health Information Exchange privacy and security officer **SHALL** determine whether a violation of privacy and security policies, procedures, or relevant law has occurred.
4. The Saudi Health Information Exchange privacy and security officer and the PHCS privacy and security officer(s) involved in the incident **SHALL** collaborate to develop, approve, and implement the mitigation plan to proactively prevent a similar Breach from re-occurring.
5. Breach Investigation Report **SHALL** be prepared documenting the facts gathered from the review, event mitigations, and measures to be taken to prevent recurrence of such an event.
    5.1. The Breach Investigation Report **SHALL** be completed within thirty (30) calendar days of receiving the reportable event report by the Saudi Health Information Exchange. This

timeframe **MAY** be extended for another 30 days upon Saudi Health Information Exchange privacy and security officer approval.

5.2. This Breach Investigation Report **SHALL** be communicated to the originator of the Reportable Event Report.

5.3. This report **SHALL** be retained for a minimum of ten (10) years.

10.3.4 Notification of Privacy Breach

1. In circumstances where it has been determined that a Reportable Event constitutes a privacy breach, the Saudi Health Information Exchange **SHALL** notify the PHCSs whose information was subject to the unauthorized acquisition, access, use, or disclosure, no later than ten (10) business days following the discovery of the breach.
2. If a breach occurs at the PHCS, then any required public notification is the responsibility of the PHCS. If the breach occurs at the Saudi Health Information Exchange level, then the responsibility is of the Saudi Health Information Exchange to report the breach, or, in some situations (e.g. where it is determined that it is important for the communication to be initiated by the healthcare provider organization rather than the Saudi Health Information Exchange), to report to the PHCS, which **SHALL** in turn make any required public notifications. Such notification **SHALL** be made within thirty (30) days following discovery of the breach.
3. The notification to the affected individual(s) **SHALL** contain, to the extent possible, the following:
   3.1. a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known,
   3.2. a description of the types of PHI that were involved in the breach (such as full name, national identification number, date of birth, home address, etc.),
   3.3. the steps individuals should take to protect themselves from potential harm resulting from the breach,
   3.4. a brief description of what the PHCS and the Saudi Health Information Exchange are doing to further investigate the breach, to mitigate harm to individuals, and to protect against any further breaches, and
   3.5. contact procedures for individuals to ask questions or learn additional information, which **SHALL** include a telephone number, an e-mail address, a web site, or postal address.
4. Breaches involving a single Individual and breaches involving small numbers of individuals **SHOULD** be reported to the Subject of Care. Breaches affecting large numbers of individuals, typically more than five hundred and involving continuous risk, **SHOULD** be reported publicly. Such decision **SHALL** be made by the privacy and security officer in collaboration with the Saudi Health Information Exchange governing body and law enforcement authorities.
5. Public notification of a breach **SHALL** include the time and date of the breach occurrence and the identification of each individual whose PHI is involved

10.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

11. SAUDI HEALTH INFORMATION EXCHANGE SECONDARY USE POLICY

11.1 PURPOSE

The purpose of this policy is to establish the conditions, if any, under which personal health information on the Saudi Health Information Exchange may be used for purposes other than direct patient care (as defined in the Purpose of Use Policy).

11.2 SCOPE/APPLICABILITY

This policy applies to the Saudi Health Information Exchange, and to all individuals and organizations that have access to the Saudi Health Information Exchange managed health records, including:

- Participating Healthcare Subscriber (PHCSs),
- their Business Associates,
- any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI,
- any Saudi Health Information Exchange Systems Service Provider,
- any other subcontractor of the Saudi Health Information Exchange, and
- any party requesting to use the Health Information Exchange managed information for secondary use as described below.

This policy applies to all PHI provided to or retrieved from the Saudi Health Information Exchange.

11.3 POLICY

1. Both local PHCS and HIE designated IRBs **SHALL** comply with the regulations as presented in the document titled "National Committee of Bioethics Implementing Regulation of Law of Ethics on Living Creatures". This document is produced by King Abdul Aziz City of science and technology.

2. Personal health information on the Saudi Health Information Exchange **MAY** be made available for purposes other than Treatment, Operations and Public Health, as defined in the Purpose of Use Policy, under the following conditions:

   2.1. Designated ethics committee (i.e., Medical Research Board; local IRB) approval **SHALL** be considered on a case-by-case basis.

   2.2. Any additional approval requirements and other proposal criteria requesting access to such data **SHALL** be determined and published by the designated ethics committee.

   2.3. The designated ethics committee **MAY** publish criteria (e.g., may have a minimum necessary content for the proposal).

2.4. The Saudi Health Information Exchange Privacy and Security Officer or designee **SHALL** be a member of the designated ethics committee.

2.5. Research data extracts or views **SHALL** be managed by the Saudi Health Information Exchange or a Saudi Health Information Exchange approved subcontractor.

2.6. A Data Use Agreement for Personal health information between the research organization/individual and the Saudi Health Information Exchange **SHALL** be established. The Data Use Agreement **SHALL** include the following requirements:

2.6.1. shall comply with "National Committee of Bioethics Implementing Regulation of Law of Ethics on Living Creatures"

2.6.2. The data use and access **SHALL** be limited to the specified purpose cited in the approved proposal.

2.6.3. Additional authorizations and consents of study subjects **MAY** be required, as defined by the designated ethics committee. Where authorizations and consents are required, the Saudi Health Information Exchange **SHALL** have access to the authorizations and consents

2.6.4. The designated ethics committee **MAY** require that the data be de-identified with or without re-identification capabilities.

2.6.5. In the case where a view is provided to the data set that would be managed by the Saudi Health Information Exchange, the party requesting the data **SHALL** identify designated individuals that access the data for the approved purpose.

3. De-identified health information **MAY** be released from the Saudi Health Information Exchange under the following conditions:

3.1. De-identification methods **SHALL** undergo a re-identification risk assessment of the proposed data extract.

3.2. Designated ethics committee (i.e., Medical Research Board; IRB) **MAY** consider the request on a case-by-case basis.

3.3. The designated ethics committee **MAY** offer criteria that will allow documentation of de-identified data sets that are not subject to case-level consideration and approval (e.g. re-identification risk criteria of routine de-identified information sets)

3.4. The user of data subset **SHALL** disclose the de-Identification method.

3.5. A Data Use Agreement for De-identified health information between the research organization/individual and the Saudi Health Information Exchange **SHALL** be established. The Data Use Agreement **SHALL** include the following requirements:

3.5.1. The data use and access **SHALL** be limited to the specified purpose cited in the approved proposal.

3.5.2. The requesting party **SHALL** be required to provide contract assurances that no attempt **SHALL** be made by it to re-identify the de-identified PHI from the Exchange provided for the approved data use.

3.5.3. In the case where a view is provided to the data set that would be managed by the Saudi Health Information Exchange, the party requesting the data **SHALL** identify designated individuals that access the data for the approved purpose.

3.5.4. If approved, de-identified data extracts or views **SHALL** be prepared by Saudi Health Information Exchange Health staff or a Saudi Health Information Exchange Health approved subcontractor with due consideration of protections to be applied to all processed data.

3.5.5. Reversible Pseudonymization provisions for the extract SHALL be subject to approval by the designated ethics committee to be reviewed on a case-by-case basis.

4. The Saudi Health Information Exchange **SHALL** make available a record of all approved requests for identified PHI, de-identified health information, anonymized health information, and pseudonymized health information from the Saudi Health Information Exchange.

4.1. The record of all approved requests **SHOULD** be reviewed with the same frequency as audit report requirements as specified by the Audit Policy.

4.2. The record of all approved requests **SHALL** include:

4.2.1. the date of the data release,

4.2.2. the entity to which the data was released,

4.2.3. a summary of the research or analysis involved, and

4.2.4. Approval Reference Number.

4.3. Such record **SHOULD** be retained for at least ten (10) years after the release of the information.

11.4 POLICY MAINTENANCE

The Saudi Health Council (SHC) is responsible for monitoring and maintenance of policies.

12. REFERENCED DOCUMENTS

TABLE 12-1 INTERNAL REFERENCES

DOCUMENT OR STANDARDS	DESCRIPTION
UC0001 Saudi eHealth Patient Identification Interoperability Use Case	This Use Case describes the capability to match a patient with his/her identity. This capability is accessible to various "edge" applications including point of care systems and business applications. It uses a set of patient demographic attributes (name, birth date, gender, etc.) and a unique nation-wide identifier called a Health ID. A Health ID is registered for Saudi citizens, residents, displaced people, GCC nationals and visitors/pilgrims. This Health ID is used for the unique identification of a patient and his/her health records. This Health ID and associated demographic attributes are managed centrally by a "patient client registry" system so that the information may be widely accessed via queries against such a registry.
UC0002 Saudi eHealth Provider Identification Interoperability Use Case	This Use Case describes the ability to access information about health professionals and the organizations where they practice. This information is centrally managed by a national healthcare provider directory; the directory which supports searches for providers and organizations and conveys authoritative attributes related to them. This information describes organizations that provide patient care, such as public and private hospitals, primary care centers, laboratories, pharmacies, etc. It is used by these organizations and by the business applications.

TABLE 12-2EXTERNAL REFERENCES

DOCUMENT OR STANDARD	DESCRIPTION
"An integrated approach to engineer and enforce context constraints in RBAC environments" – [Neumann/Strembeck - 2004]	Presents an approach that uses special purpose role-based access control (RBAC) constraints to base certain access control decisions on context information.
American Health Information Management Association (AHIMA) -- Health Information 101	http://www.ahima.org/careers/healthinfo (retrieved January 13, 2014)
ENV 13608-1:2000 Health Informatics - Security For Healthcare Communication - Part 1: Concepts And Terminology	Defines a methodology for defining, selecting and expressing a communication protection profile (CPP) specification, and provides a standard way to express healthcare user needs in relation to communication, and a standard method of successive refinement of policy statements that help to identify standardised security implementation specification that can be used to meet the security needs. Security aspects contained in the communication protection profile include confidentiality, integrity, availability and auditability.
IETF/RFC 3647 -- Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework	Presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice statement.

IHE IT Infrastructure (ITI) Technical Framework – Volume 1 (ITI TF-1) Integrations Profiles, Final Text Section 9: Audit Trail and Node Authentication (ATNA)	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability. May be obtained at http://www.ihe.net/Technical_Frameworks/#iti
ISO 17090-1:2013 Health informatics -- Public key infrastructure	Defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish digital certificate-enabled secure communication of health information.
ISO 27789:2013 -- Health informatics -- Audit trails for electronic health records	Specifies a common framework for audit trails for electronic health records (EHR), in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains.
ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002	Defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard.
ISO 7498-2:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture	Provides a general description of security services and related mechanisms, which can be ensured by the Reference Model, and of the positions within the Reference Model where the services and mechanisms may be provided. Extends the field of application of ISO 7498 to cover secure communications between open systems. Adds to the concepts and principles included in ISO 7498 but does not modify them. Is not an implementation specification, nor a basis for assessing the conformance of actual implementations.
ISO/IEC 2382-8:1998 Information technology -- Vocabulary -- Part 8: Security	The purpose of ISO/IEC 2382 is to provide definitions that are rigorous, uncomplicated and which can be understood by all concerned. The scope of each concept defined has been chosen to provide a definition that is suitable for general application. In those circumstances, where a restricted application is concerned, the definition may need to be more specific.
ISO/IEC 27000:2009 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	Provides an overview of information security management systems, which form the subject of the information security management system (ISMS) family of standards, and defines related terms.
ISO/TS 13606-4:2009 Health informatics -- Electronic health record communication -- Part 4: Security	Describes a methodology for specifying the privileges necessary to access EHR data. This methodology forms part of the overall EHR communications architecture defined in ISO 13606-1.
ISO/TS 14265 Health Informatics — Classification of purposes for processing personal health information	Defines a set of high-level categories of purposes for which personal health information can be processed. This is in order to provide a framework for classifying the various specific purposes that can be defined and used by individual policy domains (e.g. healthcare organizations, regional health authorities, jurisdictions, countries) as an aid to the consistent management of information in the delivery of healthcare services and for the communication of electronic health records across organizational and jurisdictional boundaries.
ISO/TS 21298:2008 Health informatics -- Functional and structural roles	Defines a model for expressing functional and structural roles and populates it with a basic set of roles for international use in health applications. Roles are generally assigned to entities that are actors. This will focus on roles of persons (e.g. the roles of health professionals) and their roles in the context of the provision of care (e.g. subject of care).

ISO/TS 22220:2011 Health informatics -- Identification of subjects of health care	Indicates the data elements and structure suited to accurate and procedurally appropriate and sensitive identification of individuals in healthcare in a face-to-face setting supported by computer technology, or through interactions between computer systems. It provides guidelines for improving the positive identification of subjects of care within and between healthcare organizations.
ISO/TS 25237:2008 -- Health informatics -- Pseudonymization	Contains principles and requirements for privacy protection using pseudonymization services for the protection of personal health information. ISO/TS 25237:2008 is applicable to organizations who make a claim of trustworthiness for operations engaged in pseudonymization services.
NIST Special Publication 800-63-1 -- Electronic Authentication Guideline	This recommendation provides technical guide lines for Federal agencies implementing electronic authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions.
SAS70	(see SSAE N0. 16)
SSAE No. 16. Reporting on Controls at a Service Organization	Supersedes the guidance for service auditors in Statement on Auditing Standards No. 70, Service Organizations, provides guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers.