Policy and System Operation Manual

July 23, 2019

For questions about these policies, contact the Executive Director of South Dakota Health Link (executive-director@sdhealthlink.org).

Table of Contents

Introduction

The South Dakota Health Link Policy and System Operation Manual contain policies and practices for the South Dakota Health Link Information Network. In order to become a South Dakota Health Link Participant, an organization must agree to adopt this Manual and the South Dakota Health Link Participation Agreement.

Overview

South Dakota Health Link provides "*Point of Care*","Direct", and "*Clinical Event Notifications*" services for members. Members may include, but not limited to, physicians, hospitals, clinics, laboratories, payers, and other healthcare providers.

South Dakota Health Link "*Point of Care*" services support exchanging electronic personal health information securely among South Dakota Health Link participants at the "*Point of Care*" real time.

Secure "*Point of Care*" allows but is not limited to:

- Access to patient health records across the network of community providers.
- The sharing of critical health information.
- The availability of critical, life-saving information important to managing a medical emergency.
- Access to a patient's care summary, lab results, and transcribed radiology reports.
- Event notification.

"*Point of Care*" features:

- Virtual and/or physical data consolidation and sharing.
- Real-time clinical decision support.
- Electronic health records exchange.
- Web or integrated access for all stakeholders (24/7).
- HL7 Global Messaging Standards for most data exchange.

The "Direct Project" developed a set of specifications to enable a secure, scalable, standards-based mechanism for universal transport and addressing of health care information. The Applicability Statement for Secure Health Transport includes (but is not limited to) use of X.509 certificates, S/MIME, MDNs, RFC5322 payload formatting, email-like endpoint addresses, and an SMTP backbone protocol. The XDR and XDM for Direct Messaging specification is used for use of XD metadata with XDR and XDM as well as conversion mechanisms for data traversing both XDR and SMTP.

"Clinical Event Notifications" (Notify) is a flexible, user-configured solution that puts the power of real-time notifications in the hands of clinicians and care managers for monitoring and reporting noteworthy care events. Health care providers subscribe to receive notifications when a patient is admitted/discharged/or transferred from a hospital or emergency department, ensuring the right health care decisions are made efficiently and effectively. Health care providers can customize their subscription to ensure that they receive the information they want, how they want it, and when they want it. The subscription allows them to identify patient populations and furthermore, determine what conditions they want to be notified about for those patients, identify how they want to be notified, and identify if they want to receive notifications as they happen or as a summarized report.

Participation Obligation

South Dakota Health Link maintains the minimum criteria by which participants may be approved for joining South Dakota Health Link community. Such criteria include maintaining the authority to enforce compliance with the policies.

South Dakota Health Link will make every effort to ensure credibility of information exchange between participants. A participant of South Dakota Health Link joins a community of trust to allow secure communication and exchange of information between other trusted participants. Participants of South Dakota Health Link will participate through the South Dakota Health Link Participation Agreement.

Joining South Dakota Health Link provides secure exchange of information and management necessary for trust amongst participants.

Only members joining South Dakota Health Link can share or exchange information with any other organizations associated with South Dakota Health Link.

South Dakota Health Link supports a model in which the certificates are unique to individual or domain addresses for example (member@member.sdhealthlink.net). Participants joining South Dakota Health Link shall meet the Registration Authority and Certificate Authority (if applicable) requirements of this policy found in Appendix A inclusive, and agree to adhere to the Provider Directory requirements found in section 2 of this policy manual. Furthermore, any participant that joins South Dakota Health Link must confirm their commitment to comply with Health Insurance Portability and Accountability Act (HIPAA) rules and regulations as set forth in 45 CRF parts 160 and 164, and as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) §§ 13400 – 13424, 42 U.S.C. §§ 17921 – 17954 (2009).

Section 1: *Point of Care* Exchange Services

Health Care Providers Participating in South Dakota Health Link

Each participant shall, at all times, comply with all applicable federal and state laws and regulations, including, but not limited to those protecting the confidentiality and security of Protected Health Information (PHI) and establishing individual privacy rights. Each participant shall comply with changes or updates to interpretations of such law and regulations to ensure compliance.

Each participant shall, at all times, comply with all applicable policies and procedures. The South Dakota Health Link Policy and System Operation Manual may be revised and updated annually. Each Participant is responsible for ensuring it has, and is in compliance with the most recent version of the South Dakota Health Link Policy and System Operation Manual which can be found at www.sdhealthlink.org/sdhlpolicy/.

Each participant is responsible for ensuring to have the requisite, appropriate, and necessary internal policies for compliance with HIPAA, HITECH and applicable laws of the state of South Dakota. In the event of a conflict between South Dakota Health Link Policy and System Operation Manual and participant's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security. Participants shall enforce their policies and procedures by appropriately sanctioning individuals within its workforce and staff who violate its policies, South Dakota Health Link Policy and System Operation Manual, or federal or state law.

Each Participant shall have policies and procedures to promote the integrity of the PHI he/she maintains and makes available to South Dakota Health Link, in addition to the accuracy, relevance, and completeness of such PHI. ("Under no circumstances shall an individual be denied treatment on the basis that he or she chooses to Opt-Out.")

Patient consent to Opt Out from South Dakota Health Link

All Patients of a Participating Organization will be automatically enrolled in South Dakota Health Link, and no affirmative action needs to be taken by a patient to establish his or her Consent. A Patient shall be deemed to have given his or her Consent to participate until and unless the Patient affirmatively Opts-Out of South Dakota Health Link.

If a Patient does not Opt-Out of South Dakota Health Link, his or her PHI will generally be disclosed in response to a specific request, query, or inquiry, made by a Participating Organization for a permissible purpose. However, a Patient's PHI will not be disclosed in response to such an inquiry when it contains sensitive health information for which a specific authorization is required even if a Patient does not Opt-Out.

A Patient who does not want his or her PHI to be disclosed to other Participating Organizations may Opt-Out by following the procedures available in Appendix B. If a Patient does Opt-Out, his or her Protected Health Information will not be disclosed through South Dakota Health Link's Point of Care Exchange for any permissible purpose.

South Dakota Health Link uses Clinical Event Notifications to alert a patient's health care provider of certain events such as emergency department or inpatient visits. **Patients may not Opt-Out of Clinical Event Notifications.**

Each Participating Organization may provide every Patient with educational material about its participation in South Dakota Health Link during the Patient's first visit or encounter with that Participating Organization after it enrolls in South Dakota Health Link. This educational material may be provided in writing, and in any other format (on-line presentation, oral presentation, foreign language presentation, etc.) designed to ensure that its contents are communicated to and understood by the Patient. Educational material is available at http://www.sdhealthlink.org/.

If a Patient elects to Opt-Out of the Health Information Exchange, the educational material will provide them with the process to document his or her decision to Opt-Out. This standard Opt-Out form is available at http://www.sdhealthlink.org/; this form must be signed by the Patient and his or her provider or notary public.

A Participating Organization must allow a Patient to Opt-Out at any time, even after having already been enrolled in South Dakota Health Link. However, any exchange of PHI that may have occurred prior to a Patient's decision to Opt-Out will not be reversed.

The Participating Organization will comply with the consent decision made by a parent or legal guardian for his or her minor child to Opt-Out of South Dakota Health Link.

All decisions made by Patients to Opt-Out of South Dakota Health Link will be communicated by the patient to South Dakota Health Link to ensure compliance with each Patient's decision to Opt-Out. It is necessary for the properly executed Opt-Out form itself to be sent to South Dakota Health Link.

A Participating Organization will not deny care to any Patient solely because he or she elects to Opt-Out of South Dakota Health Link.

Patient can revoke his or her decision to Opt-Out of South Dakota Health Link. The patient will have to complete the standard Opt-In Form available at http://www.sdhealthlink.org/. This form should be signed by the Patient and signed by his or her provider or notary public. Once the Opt-In form has been executed by the Patient and communicated to South Dakota Health Link, he or she will be enrolled in the Health Information Exchange from that date forward.

South Dakota Health Link Information Security

The ability to protect electronic Protected Health Information (ePHI) through strong information security is critical to establishing trust in exchanging ePHI. There are well-established best practices in information security across multiple industry contexts that are available for participants to follow.

South Dakota Health Link shall accomplish an appropriate level of security by meeting or exceeding industry standards for the protection and safeguarding of ePHI, and South Dakota Health Link vendor(s) will document the efforts made to achieve and maintain proper security. South Dakota Health Link may engage a third-party expert or service to review its security processes to ensure high levels of security are maintained.

Maintaining the security, confidentiality, integrity and availability of health information is South Dakota Health Link's top priority. In addition to state and federal standards and regulations, South Dakota Health Link follows these guiding practices:

- Maintain comprehensive record of all actions involving patient records.
- Keep all patient records private and confidential unless there is documentation that allows access.
- By default, the only authorized access to patient information is by the person or organizational component that created the information or made the original request.
- Confidentiality, security and integrity of patient information trumps process.
- Software must not conflict with common high-availability practices.

The following are example processes that support HIPAA and HITECH privacy and security regulations.

Point of Care Exchange Application.

The system identifies users by user ID, classifies them by type, and authenticates them with a password and an optional second factor such as token-based authentication. An administrator can assign user names or users can self-assign user names during a self-service registration process. If self-assigned, the system creates a provisional user profile and places it in a work queue for the application or security administrator to review. The administrator reviews provisional user registrations and approves or denies them based on the organization's required process. Users are classified by a type that defines a basic set of functional and data type access authorities. Many of these security attributes can be adjusted individually to create users with authority profiles that have been tailored to meet user and environment specific needs.

Users can create a password or the system can assign them one. Administrators can configure the system to require passwords to meet specific construction requirements

and to require user renewal on an established basis. Administrators can also set up the system to require two factor authentications such as SecureID™, biometric or other token based technology such as Radio Frequency Identification RFID. Additionally, administrators can set up the system to accept authentication credentials from an external source such as Light Weight Directory Access Protocol LDAP or Active Directory.

Role-based Access

A physician or staff member's role in the organization determines their level of access to a patient's clinical data in *Point of Care* Exchange. The role-based permissions security authorization occurs at the application level. A system administrator can create various user roles (for example, Physician, Clinical Staff, and User Admin), and then assign various application access levels to these roles. For example, a Physician or Clinical Staff role may have access to view patient clinical information, whereas a User Admin role may be limited to only the administrative functions for adding new users and viewing application usage reports.

Point of Care Exchange distinguishes between two main groups of users: providers and staff. Providers have access to data based on their relationship to the data. Staff receives access based on their relationship to the provider. A variety of options are available on the organizational level to limit which patients and which types of data provider and staff users have access to. Access can be refined further on the individual user level, thus supporting personalization.

Users can have access to patient information based on organizational and individual-user maintenance settings. Areas of control include:

- Which patients a user can access.
- What type of data from a visit or encounter a user can access.
- Whether or not the user can access confidential information.
- What types of clinical data are available to the user.
- Which features of the application are available to the user.

Point of Care Exchange also distinguishes administrative users from other users. Providers and staff can be designated as administrators. Two levels of administrative users exist in the system: administrators and delegated user administrators. Administrators control access settings on both the organizational level and the user level. They control access to patients and data, security settings, and referral capabilities. They can also set up new users and control what types of data and which features of the application the user has access to. Delegated user administrators control access settings on the user level alone. See Appendix D for the role settings.

Other roles will be created to meet the changing needs of South Dakota Health Link and to meet the evolving group of organization types who may become participants of South Dakota Health Link.

The first time a user logs into the *Point of Care* Exchange, they will be presented with the end-user license agreement (EULA). See Appendix E for a copy of the EULA.

Consent and Access Rights

South Dakota Health Link considers all patient records to be confidential unless and until there is documentation that allows access. This documentation may be in the form of a recorded direct patient consent at the Participant level, or an indirect consent received through relationships indicated in HL7 transactions.

- Indirect Consent-Result transactions normally identify the requesting doctor or organizational component. This information can function as an indirect consent for this doctor or organizational component to access unrestricted portions of a patient's health record.
- South Dakota Health Link's Patient Consent framework supports opt-out patient consent model, which an HIE may configure according to its policies.
- For the opt-out consent method, a patient has to opt-out before their data is excluded (the default status is that patient data is included (made accessible) until the patient opts-out). Opt-out settings enable reversing the patient setting, should the patient choose to participate at a later stage.

Operational Security

South Dakota Health Link protects information in an operational environment through a combination of physical and logical approaches. The first approach to operational security is to locate the physical infrastructure in a secure location. This secure location provides physical barriers to access and redundant environmental support systems such as power and air conditioning.

Logical security restricts access to data and application logic through a series of dedicated networks, security appliances and firewalls. For example the database server connects to the application server in a way that only allows access to data through the data abstraction layer. Application servers have two network adapters, one to access a dedicated link to the data abstraction layer and another to connect to web servers contained behind a firewall in a Demilitarized Zone (DMZ). This "DMZ" is the only area where external sources can access services.

Encryption

South Dakota Health Link protects data while in-transit and while at-rest via multiple mechanisms such as SSL, PKI, one-way hashing of certain data types such as user passwords, and symmetric encryption of clinical data at-rest.

South Dakota Health Link uses the following encryption to protect data during transmission:

- South Dakota Health Link encrypts data transmissions using 128 bit TLS or SSL encryption.
- South Dakota Health Link secures connections to its servers for transmission and receipt of HL7 data with a LAN to- LAN IPSec VPN.
- South Dakota Health Link secures inquiry/CONNECT with the following measures:
    - 128 bit 2-way-SSL with mutual authentication
    - Uses PKI for certificates and OCSP/CRLs for revocation

Non-Repudiation

South Dakota Health Link uses various security measures to ensure non-repudiation, including strong authentication of users and contributing systems, and encryption to ensure data integrity.

- The system requires strong user authentication to validate access. The system identifies *Point of Care* Exchange application users by user ID, classifies them by type, and authenticates them with a password and an optional second factor.
- South Dakota Health Link establishes point-to-point interfaces with data contributors, as well as secured communications between Novo Agents and the Grid, to ensure that information flowing into the system comes directly from those contributors.
- To ensure data integrity throughout the Care Collaboration Suite, South Dakota Health Link uses a combination of mechanisms such as SSL, PKI, one-way hashing of certain data types such as user passwords, and symmetric encryption of clinical data at-rest. We also use highly secured web services (signed with X.509 certificates) throughout our Service Oriented Architecture.

Breach/Event Detection and Reporting

Unsecured PHI, generally, is PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals.

With respect to unsecured PHI, South Dakota Health Link's operations and policies shall at all times adhere to HIPAA and ARRA/HITECH, including any regulation or guidance pertaining to unsecured PHI, breach and reporting obligations.

Breach means the unauthorized acquisition, access, use, or disclosure of PHI which compromises security or privacy of the information, except where an unauthorized person coming in contact with such information would not reasonably have been able to retain it. Breach does not include unintentional acquisition, access, or use of PHI by a participant if made in good faith in the scope of employment, and the PHI was not further acquired, accessed, used or disclosed by any person.

South Dakota Health Link shall adhere to breach notification procedures found in Appendix C Section IV Subsection 3 of this document.

For any breach, South Dakota Health Link may contract with a third party to conduct an analysis of the cause of the breach, and potential corrective actions or remediation steps to make the system more secure in the future.

The Information Security Officer shall periodically perform a review of breaches and other security events in order to identify areas for improvement in the system. Such review shall take place no less frequently than quarterly.

Network Monitoring and Breach Notification

South Dakota Health Link protects against external breaches by maintaining perimeter firewalls, IDS solutions and 24/7/365 monitoring through our network operations center (NOC). In the event of a breach, South Dakota Health Link will follow all applicable federal and state breach notification laws, rules and regulations. South Dakota Health Link will immediately notify the affected parties and begin the remediation process. We report any incident to South Dakota Health Link's Information Security Officer, and complete a full documentation cycle to ensure that the incident does not reoccur.

Compliance with HIPAA, State, and other Federal Laws

The proposed South Dakota Health Link solution fully supports HIPAA, and new legislation such as HITECH (including the new data breach notification provisions), as well as applicable regulations and even stringent federal NIST standards.

Consumer Complaints

Individual Complaints

Any individual may submit a complaint about an access, use, or disclosure of PHI through the System to South Dakota Health Link, the Participant that maintains the PHI, or the Secretary of the Department of Health and Human Services (HHS) in Washington, DC. If the individual wants to file a formal complaint with South Dakota Health Link, he or she should be directed to the South Dakota Health Link Privacy Officer. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to the Office for Civil Rights website (www.hhs.gov/hipaa). The South Dakota Health Link Privacy

Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

Duty to Investigate

Each Participant shall promptly investigate reported or suspected privacy breaches of Participant's System interface. Upon learning of a reported or suspected breach, the Participant shall notify South Dakota Health Link and any other Participant whom the notifying Participant has reason to believe is affected or may have been the subject of unauthorized access, use, or disclosure. South Dakota Health Link shall have the right to participate in the investigation and to know the results and any remedial action taken, except that South Dakota Health Link need not be notified of specific workforce disciplinary actions short of termination of an employee.

Each investigation shall be documented. At the conclusion of an investigation, a Participant shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to South Dakota Health Link. South Dakota Health Link may use examples of breaches for education and for policy and other safeguard development; however, South Dakota Health Link will not disclose the names of individuals or organizations involved in the breach.

Incident Response

South Dakota Health Link shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by South Dakota Health Link. The incident response system may include the following features, each applicable as determined by the circumstances:

1. Cooperation in any investigation conducted by the Participant or direct investigation by South Dakota Health Link.
2. Notification of additional Participants or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach.
3. Cooperation in any mitigation steps initiated by the Participant.
4. Furnishing audit logs and other information helpful in the investigation.
5. Developing and disseminating remediation plans to strengthen safeguards or hold Participants or authorized users accountable.
6. Where appropriate, take steps to comply with the HIPAA Breach Notification Rule.
7. Any other steps mutually agreed to as appropriate under the circumstances.

8. Any other steps required under the incident reporting and investigation system contained in the South Dakota Health Link Security Policies.

Cooperation in Investigations

South Dakota Health Link shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, when the investigation implicates South Dakota Health Link conduct, or the conduct of another Participant or authorized user, or the adequacy or integrity of System safeguards.

Each Participant shall cooperate with South Dakota Health Link in any investigation of South Dakota Health Link or of another Participant into South Dakota Health Link 's or such other Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by South Dakota Health Link or the other Participant, when the investigation implicates such Participant's compliance with South Dakota Health Link policies or the adequacy or integrity of System safeguards.

Non-retaliation for Filing a Complaint

South Dakota Health Link will not intimidate, threaten, coerce, discriminate, penalize, or take other retaliatory action against an individual who exercises his/her rights under HIPAA or against any individual who participates in a process governed by the Privacy Regulations. This prohibition also applies to:

- Individual complaints filed with South Dakota Health Link, a Participant, or the Secretary of HHS.
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the HIPAA Privacy Regulations.
- Opposing any act or practice of South Dakota Health Link, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the HIPAA Privacy Regulations, or otherwise violate applicable law.

No Waiver

No individual will be asked to waive his/her HIPAA rights, including the right to file a complaint about the use or disclosure of his/her PHI.

Duty to Mitigate

Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of a violation of applicable laws, regulations, and/or these policies related to the unauthorized access, use, or disclosure of Protected Health Information through the System, and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participant notification to the

individual or Participant request to the party who improperly received such information to Cooperation in Mitigation.

A Participant that has caused or contributed to a privacy breach or that could assist with mitigation of the effects of such breach shall cooperate with South Dakota Health Link and with another Participant that has the primary obligation to mitigate a breach in order to help mitigate the harmful effects of the breach. This obligation exists whether the Participant is directly responsible or whether the breach was caused or contributed to by members of the Participant's workforce or by its Business Associates or contractor or their workforce.

Notification to South Dakota Health Link

A Participant primarily responsible to mitigate shall notify South Dakota Health Link of all events related to the System requiring mitigation and of all actions taken to mitigate. In the event the mitigation results in termination of an employee, the Participant has the responsibility to notify South Dakota Health Link of the name of the individual whose employment was terminated.

South Dakota Health Link may facilitate the mitigation process if asked. South Dakota Health Link may use examples of breaches for education and for policy and other safeguard development; however, South Dakota Health Link will not disclose the names of individuals or organizations involved in the breach.

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 and as required by law through the terms of their business associate agreements.

If the South Dakota Health Link Privacy Officer determines that PHI that was wrongfully accessed, used, or disclosed is created or maintained by a subcontractor of South Dakota Health Link, the HIPAA Privacy Officer will notify the subcontractor of the results of the investigation and any required action on the part of the subcontractor. If the results of the investigation are that the South Dakota Health Link subcontractor inappropriately accessed, used, or disclosed an individual's PHI, the South Dakota Health Link Privacy Officer will prepare a recommendation for the Secretary of South Dakota Department of Health as to whether the relationship between the subcontractor and South Dakota Health Link should continue.

Mitigation by South Dakota Health Link

If an investigation of a privacy breach indicates that PHI was misused or improperly disclosed, the South Dakota Health Link Privacy Officer shall determine:

- What, if any, privacy practices at South Dakota Health Link require modification.

- Whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised.
- Whether additional training is required to avoid a repeat violation.
- What corrective actions, if any, will be imposed against the individual who committed the violation.

Auditing and Access Monitoring

A secure audit log shall be created for each instance where PHI is accessed, created, updated, or archived via South Dakota Health Link.

Audit logs shall be maintained for all transactions to and from South Dakota Health Link. The following information shall be captured by such audits:

- sender/recipient identifier
- date and time of event
- system component where event occurred
- type of event or transaction
- outcome (success/failure)

Audit logs shall be maintained for all instances of user access, as well as granting or revoking user access rights to the system. The following information shall be captured by such audits:

- user identifier
- date and time of event
- system component where event occurred
- type of event
- outcome of event (success/failure)

South Dakota Health Link shall randomly review audit logs to ensure that all activity is within expected parameters. Any anomalous or suspicious finding should be reviewed by the South Dakota Health Link Information Security Officer and other necessary personnel as the Security Officer deems necessary. The Information Security Officer shall be responsible for ensuring South Dakota Health Link policies are followed including that each anomaly or suspicious activity is properly reported, remediated and documented, consistent with South Dakota Health Link policies.

Participants in states with consent models other than opt-out shall be subject to periodic random audits to ensure appropriate consents or documents are on file.

The Information Security Officer at South Dakota Health Link might from time-to-time communicate with Participants to verify audit results are consistent between South Dakota Health Link and the submitting or receiving provider entity. All Participants will be

expected to engage in audit review, communicating with the South Dakota Health Link Information Security Officer or his designee when needed.

Audit Trails/Logs

The proposed solution supports full HIE logging, as specified by the eHealth Exchange 2011 Specifications. Logged events include all outbound messages sent from a gateway, all inbound messages received by a gateway, and all significant user activity (log in, time out, patient record access, query, etc.).

The logging service is a robust, secure, high performance web service designed for the internal logging of all events in a unified location. Its robust features include the ability to continue logging if the central service is temporarily unavailable (such as for scheduled maintenance). This is accomplished via a local persistent cache that automatically inserts into the main logging service once the logging servicecomes back on line. This logging service is in turn mined by our optional analytics data mart collectors to enable logged activity to be reported on and viewable interactively via ad hoc reports.

Every time a user accesses or modifies a patient record or piece of clinical information a record of that event goes into a common event log. In addition to these patient specific log entries, the system creates other non-patient specific entries for events such as user logon/logoff. These log entries include information such as:

1. User ID/context
2. Event date/time
3. Event type
4. Patient ID/ context
5. Encounter context
6. Software module
7. Data type
8. Data descriptor/index
9. Event-specific information

The Information Security Officer at South Dakota Health Link can access this log online or through reports designed to meet specific reporting and discovery requirements. For example, to report or investigate unauthorized record access. The first report enables the Information Security Officer to create a report of all users that have accessed a patient's record over a declared time frame. The second report focuses in on the activities of a specific user. This allows the Information Security Officer/Administrator to identify a specific user that may have accessed a record inappropriately and then look for additional unauthorized accesses by that individual.

The system logs the patient consent process just like other events. Each consent log entry forms the basis of a special report that the Information Security Officer can generate for

regular review and forward to peer review or regulatory organizations for appropriate action.

Participant may request an audit trail or log regarding the use, access and/or disclosure of information by its own Authorized User.

Consumer Requested Report

Consumers may request an audit trail or log regarding the use, access, and/or disclosure of their PHI. Such request should be submitted in writing to the South Dakota Health Link Privacy Officer. Efforts will be made to respond to such request in thirty days, however, in the event more time is needed the consumer will be notified.

South Dakota Health Link will provide an accounting to consumers at no cost once in a twelve month period. If a consumer requests a subsequent accounting within the twelve month period, they will be notified of the fees that may be charged to generate the accounting. Such fee shall only include actual and reasonable costs for staff time and copying.

eHealth Exchange

South Dakota Health Link shall be a member of the eHealth Exchange. The eHealth Exchange is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through secure, trusted, and interoperable health information exchange. More information about the eHealth Exchange can be found in Appendix C of this document.

HIE-to-HIE Exchange

All HIE-to-HIE (or Federal Agency) connections will be made in accordance with the eHealth Exchange policies and procedures available at ehealthexchange.org. All HIEs (or Federal Agencies) connecting with South Dakota Health Link must be a validated member of the eHealth Exchange.

Membership Fee

Refunds

Participant agrees that, once paid, all Membership Fees are nonrefundable for any reason, including termination of participation in South Dakota Health Link services by either party.

Past Due Accounts

Participants membership year begins October 1 and ends September 30. All membership payments are due no later than November 1st of the billing year, and will be considered past due after this date. Past due accounts will be charged compounded interest of 1% per month, added to the initial invoice. Any account which is more than 120 days old will be due immediately plus accrued interest or account access shall be suspended.

If no payment arrangement has been made 14 days after account suspension, the account will be assigned to the State of South Dakota contracted collection agency. An administrative charge of 35% will be assessed on all accounts turned over to the contracted collection agency.

Section 2: Direct Messaging Services*

***Section 2 Applies only to those using South Dakota Health Link Direct Messaging Services.**

Overview

South Dakota Health Link has incorporated a set of rules to which a Health Information Service Provider (HISP) member would agree in order to be trusted by another HISP member within a privacy policy framework set by ONC. Note that a HISP member must agree to South Dakota Health Link policies and agreements in order to be part of the HISP. Connectivity to other HISPs will only be done with other accredited DirectTrust members.

Definition

A Health Information Service Provider (HISP) is a role in a Direct message exchange that provides edge protocols, message formatting, security, and routing according to the Direct project specification. A HISP also provides trust-store management tools and services for members. The HISP member may be providers, payers, EHR vendors, PHR vendors, health information exchanges, and third-party entities.

Role

The Health Information Service Provider (HISP) shall provide services to a variety of organizations including providers, payers, EHR vendors, PHR vendors, health information exchanges, and other HISPs. The Direct Project developed a set of specifications to enable a secure, scalable, standards-based mechanism for universal transport and addressing that every HISP must follow. The consensus obtained during this process is expressed in the Applicability Statement for Secure Health Transport and includes (but is not limited to) use of X.509 certificates, S/MIME, MDNs, RFC5322 payload formatting, email-like endpoint addresses, and an SMTP backbone protocol. Consensus was also achieved within the XDR and XDM for Direct Messaging specification for use of XD metadata with XDR and XDM as well as conversion mechanisms for data traversing both XDR and SMTP.

Goal

The goal of Direct is to achieve universal information exchange and interoperability between HISPs within the confines of a trust model. As real-world pilot implementations of direct exchange have taken hold, a desire has been expressed for additional clarity and agreement in areas that go beyond the specifications listed above, in order to ensure that HISPs will be able to assess the trust-worthiness of other HISPs. Trust between

HISPs is essential if direct addresses are to have confidence that their messages will be received consistently and reliably. Specifically, these areas include:

1. Security profile of HISP edge protocols.
    - Authentication and privacy mechanisms utilized up to the S/MIME.
    - Privacy (encryption) of data at rest.
2. Certificate discovery/directory mechanisms.
    - The Applicability Statement recommends Domain Name System (DNS) as one option for certificate discovery.
    - Specific qualifiers that either contribute to, or detract from, trust-worthiness of a HISP that uses DNS
3. Judging the trustworthiness of a Certificate Authority and Registration Authority associated with a HISP.
    - Certificate Policy and Certificate Practices Statements (including identity verification practices) – RFC 3647
    - WebTrust seal, ETSI certification, or FBCA cross-certification
    - HIT Policy Committee recommendations
    - Evaluation Criteria for Trust Anchors and Certification Authorities
4. Identity verification of patients versus providers.
5. Transparency and public disclosure requirements for HISPs.

HISP Policy

HISPs Serving Healthcare Organizations

It is the responsibility of the HISP member to provide intuitive tools and knowledge within a healthcare organization/individual that allows it to implement a trust policy consistent with security policies and within the capabilities of the Direct Project PKI architecture. To reap the benefits of secure but ubiquitous communication, healthcare organizations/individuals should codify trust by, possibly, adding trusted root certificates to its users' Direct Project trust stores. Healthcare organizations should not use the Direct Project PKI trust store to enforce business policies above and beyond those dealing with privacy and authentication of Direct Project messages.

A healthcare organization/individual that is a HIPAA covered entity will either provide HISP services within its network or execute a HIPAA Business Associate Agreement (BAA) with a third-party HISP. Either way, all PHI retention, use, disclosure, security, and access will follow HIPAA guidelines for a covered entity.

A healthcare organization/individual that is not a HIPAA covered entity will either provide HISP services within its network or execute a BAA with a third-party HISP that is materially equivalent to a HIPAA BAA. Either way all PHI retention, use, disclosure, security, and access will follow guidelines equivalent to those required of a HIPAA covered entity.

A Direct address contains a domain component that may be rooted at the HISP (e.g., OrganizationName@OrganizationName.sdhealthlink.net) or may be independent of the HISP (e.g., Provider@OrganizationName.sdhealthlink.net). Should the user decide to switch to a different HISP, choosing the latter option allows them to do so without changing his Direct domain/address. HISPs should allow a provider to use their own domain (and certificate) if desired.

When a healthcare organization is issued an organizational Direct certificate, then HIPAA best practices should be followed by the healthcare organization in determining the appropriateness of assigning Direct addresses to its members (all of which will use the same Direct organizational certificate for S/MIME signature verification and encryption).

A HISP member should not use an organizational certificate to represent more than one distinct organization. A HISP member should not use an individual certificate to represent more than one distinct healthcare individual. For example, if a third-party HISP provides service to 20 distinct hospitals (legal entities), each hospital should be associated with a different organizational certificate.

Any HISP member who wishes to change their domain address may be subject to change fees or other costs associated with the change.

HIPAA and Legal Agreements

Because the HISP is a separate business organization from the sending and receiving organization, there are some functions that should be enforced through contract law, in addition to those enforced by Federal, State and local laws and regulations.

In many cases, HISPs may be required to have Business Associate Agreements (BAAs) with HIPAA Covered Entities. In cases where BAAs are not strictly required (for example, because the sender or receiver is not a Covered Entity), coverage under similar agreements is essential to provide the equivalent safeguards and protections provided under contractual law to those provided by BAAs for Business Associates of Covered Entities.

HIPAA provides legal safeguards and clear requirements for Individuals (patients/consumers) and Covered Entities, as defined in HIPAA. There are some participants that will desire to participate in directed exchange but will not meet the legal triggers for Covered Entity status. Including such participants in directed exchange without ensuring the same legal safeguards provided under HIPAA is problematic. HIPAA extends privacy safeguards and protections to apply to Business Associates of Covered Entities. Directed exchange of Personally Identifiable Information (PII) that involves intermediaries or third parties that are not Business Associates or covered by equivalent protections is likewise problematic, unless separate mutual contracts are in place to protect privacy, security and transparency. Because a model that requires mutual

contracting is not operationally scalable, it is desirable to limit exchange to entities that have clear recognized responsibilities under HIPAA.

Exchange of data protected by strong encryption over the open Internet using pure routing functions (e.g., TCP/IP switching, SMTP servers handling encrypted data) generally does not need these levels of protection so long as the routing organizations do not have access to the decryption keys.

Directed exchange where participants have access to unencrypted data or could have access to unencrypted data (because they hold decryption keys for encrypted data) must involve Individuals, Covered Entities and Business Associates (using those terms as defined by HIPAA) OR organizations that have strong legally enforceable contractual obligations that provide equivalent protection for individuals to those provided by HIPAA.

By noting "equivalent protection," we recognize that the investigational powers and remedies available in contractual law do not equal those available to the Federal Government under HIPAA.

Information Security

The ability to protect PHI through strong information security is critical to establishing trust in directed messaging. There are well-established best practices in information security across multiple industry contexts that are available for HISPs to follow.

The HIPAA Security Rule establishes uniform national standards for information security. The security rule applies to Covered Entities, and, by extension to Business Associates; Meaningful Use also requires compliance to the HIPAA Security Rule. At a more detailed level, information security guidelines have been developed to protect cardholder data for financial transactions, in the PCI Data Security Standards (PCI-DSS); many of the detailed requirements for that purpose have broad applicability to health care as well.

Regardless of legal requirements, all HISPs will hold themselves to the provision of the HIPAA Security Rule, and, to the extent that it is relevant and consistent with the Security Rule, will follow the guidelines of PCI-DSS.

Some HISPs might maintain private keys as well as public certificates, and will use those private keys to manage trust on behalf of providers, provider organizations, or other participants in health information exchange. This implies a high degree of trust that must be protected with a high degree of security.

HISPs that manage private keys must perform specific risk assessment and risk mitigation to ensure that the private keys have a strong protection from unauthorized use. That risk assessment must address the risk of internal personnel or external attackers gaining unauthorized access either to the keys or to the health information functions for which

the keys enforce trust. Some HISPs will manage trust anchors on behalf of their customers. This is a critical aspect of trust, and must be managed well to avoid compromise on strong assurance of identity.

HISPs that manage trust anchors on behalf of their customers must be an accredited DirectTrust member.

Transparency of Healthcare Information

Any HISP that manages, transforms or performs value-added services PHI has an obligation to make the extent of data use and other activities clear and transparent. Transparency initiatives should focus on both quality and cost. Empowering consumers to make health care decisions based on quality information should be a critical part of the discussion on health care transparency.

Health information transparency enhances the appropriate use and quality of healthcare, and it helps in cost management by enabling informed decision-making. HIT based on broadly accepted standards, allows patients, healthcare providers and health plans to share information securely, driving down costs by avoiding duplicate procedures and manual transactions.

HISP Direct Email Services

Using Direct will not require that providers implement software. Instead, the process for sending information is similar to sending e-mail today.

First a physician would contract with a HISP, such as South Dakota Health Link that has decided to offer Direct as one of its exchange services. South Dakota Health Link HISP would assign the physician a Direct e-mail address.

To use Direct, the physician would log into his or her HISP Direct gateway via the Internet and use his or her Direct e-mail address to send information to another provider who also has a Direct e-mail address. Information can only be sent to other providers using the Direct service.

Deployment Models

The deployment models associated with use of Direct Project specifications allow, under control of the sender and receiver, for the locus of encryption/decryption activities to take place either at the sender or receiver or with a separate party under an appropriate contractual relationship with the sender or receiver.

Preconditions

The sender and receiver have ensured that agents of the sender and receiver (for example, HIO, HISP, intermediary) are authorized to act as such and are authorized to handle protected health information according to law and policy.

Direct Messaging

Direct messaging is secured with appropriate level of encryption; HISP members must be approved to join the HISP and have a valid digital certificate in order to exchange messages within the HISP network.

DirectTrust

South Dakota Health Link is a member of DirecTrust. DirectTrust is a vibrant and collaborative non-profit alliance of health IT and health care provider organizations who have joined forces to support secure, interoperable health information exchange via the Direct Message Protocols. South Dakota Health Link will consider connections with HISPs outside our network who are also DirectTrust members.

HISP-to-HISP

All HISP-to-HISP connections will be made in accordance with DirectTrust policies and procedures available at www.directtrust.org. All HISP's connecting to South Dakota Health must be a DirectTrust member.

Membership Fee

Refunds

Participant agrees that, once paid, all Membership Fees are nonrefundable for any reason, including termination of participation in South Dakota Health Link services by either party.

Past Due Accounts

Participants membership year begins October 1 and ends September 30. All membership payments are due no later than November 1st of the billing year, and will be considered past due after this date. Past due accounts will be charged compounded interest of 1% per month, added to the initial invoice. Any account which is more than 120 days old will be due immediately plus accrued interest or account access shall be suspended.

If no payment arrangement has been made 14 days after account suspension, the account will be assigned to the State of South Dakota contracted collection agency. An

administrative charge of 35% will be assessed on all accounts turned over to the contracted collection agency.

Appendix A

Certification Authority

South Dakota Health Link uses Health Catalyst's HISP services. Digicert is Health Catalyst's Certificate Authority. The Cetificate Policy and Certificate Practice Statement are available on Digicert's site at https://www.digicert.com/legal-repository/. The DirectTrust Community X.509 Certificate Policy version 1.4 can be found on Digicert's site at http://www.directtrust.org/about-policies/. DirectTrust maintains a list of all the accredited HISP's and their Certificate Authority Certificate Policy at the following site https://services.directtrust.org/about_accredited_bundle/.

Registration Authority

Registration Authority Overview

Registration Authority (RA) is defined as an entity that is responsible for identification and authentication of certificate subjects. The RA function for their participants shall be conducted by South Dakota Health Link HISP.

South Dakota Health Link RA is responsible for ensuring the eligibility of a member with the accuracy and integrity of required information presented by the member.

The guidance contained in this document takes into consideration that joining members have met the common minimum requirements for RA services.

Registration Authority Requirements

South Dakota Health Link Health HISP serves as a RA for their participants. RA is the entity that enters into an agreement with a Certification Authority (CA) to collect and verify each participant's identity and information to be entered into the public key certificate. The HISP RA performs its function in accordance with South Dakota Health Link CA Policy and the Certificate Practice Statement (CPS), and any other relevant agreements or policy documents. Minimum activities that shall be conducted by the RA include:

1. In-person proofing
2. Verification and validation of identity documents
3. Enrollment and registration
4. Credential issuance
5. Credential usage
6. Credential revocation
7. Post issuance updates and additions
8. Credential re-issuance

The RA is responsible for the standards, training, oversight and audit of the RA entities operating at the direction of South Dakota Health Link HISP. As such, the RA ensures that the approved Participant is in material compliance with South Dakota Health Link policies and agreements at all times. The RA shall ensure that timely corrective action is taken to address any RA entities deficiency, including the termination or suspension of specific RA entity duties, when warranted.

Registration Authority Roles and Responsibilities

South Dakota Health Link HISP serves as an RA for all HISPs joining the HISP community in order to allow simple, secure movement of health information between HISP participants.

Appendix B

Opt-Out Process

1. No action is needed by a Patient if he or she wishes to participate in South Dakota Health Link's Point of Care Exchange. A Patient shall be deemed to have given his or her Consent to participate until and unless the Patient affirmatively Opts-Out of South Dakota Health Link's Point of Care Exchange. These alternatives shall be collectively referred to herein as the Patient's Consent decision.

2. Every Patient should receive educational information about South Dakota Health Link's Point of Care Exchange from his or her Participating Organization during his or her first encounter with that Participating Organization after it enrolls in South Dakota Health Link. This educational information will be available at www.sdhealthlink.org and should be provided in writing, or any other format (on-line presentation, oral presentation, foreign language presentation, etc.) designed to ensure that its contents are communicated to and understood by the Patient. This educational information must explain:

    a. The function of South Dakota Health Link's Point of Care Exchange.
    b. The Permissible Purposes for which a Patient's Protected Health Information may be disclosed to other Participating Organizations through South Dakota Health Link.
    c. The types of Protected Health Information which may be disclosed to other Participating Organizations.
    d. The fact that a Patient's Personal Demographic Information will be included in a Master Patient Index maintained by South Dakota Health Link to permanently record his or her Consent decision.
    e. The fact that a Patient's participation in the Health Information Exchange is voluntary and subject to a Patient's right to Opt-Out.
    f. The fact that a Patient may Opt-back-In at any time.
    g. Educational information about South Dakota Health Link's Point of Care Exchange will be available to Patients on-line at www.sdhealthlink.org.

3. A Patient may Opt-Out of participation in South Dakota Health Link's Point of Care Exchange by following the instructions provided online at www.sdhealthlink.org. The Patient may Opt-Out by completing the Opt-Out form found online at www.sdhealthlink.org.

4. A Patient may Opt-Out of the Health Information Exchange during a visit or encounter with his or her Participating Organization.

5. After a Patient's identity has been verified either by a provider signing the Opt-Out form or a notary public, patient should communicate the Opt-Out form to South Dakota Health Link to ensure compliance with each Patient's decision to Opt-Out. It is necessary for the Opt-Out form itself to be sent to South Dakota Health Link.

6. South Dakota Health Link's electronic on-line process includes the same educational information that is made available to Patients by their Participating Organizations. Prior to Opting-Out on-line, a Patient must acknowledge electronically that he or she has been presented with and understands the educational material available at www.sdhealthlink.org.

7. A Patient may choose to Opt-Out at any time, even after having already been enrolled in South Dakota Health Link's Point of Care Exchange. However, any exchange of Protected Health Information that may have occurred prior to a Patient's decision to Opt-Out will not be reversed.

8. A Patient may revoke his or her decision to Opt-Out (Opt-In) of South Dakota Health Link's Point of Care Exchange by completing the Opt-In form available at www.sdhealthlink.org. This form must be signed by the Patient and signed by his or her provider or notary public.

Once the Opt-In form has been executed by the Patient and communicated to South Dakota Health Link, he or she will be enrolled in the Health Information Exchange from that date forward.

Appendix C

eHealth Exchange

I. Use of Message Content

1. **Permitted Purpose.** Participants shall only Transact Message Content for a Permitted Purpose as defined in the following Section I.2 of Appendix C.

2. **Permitted Purpose** shall mean one of the following reasons for which Participants or Participant Users may legitimately Transact Message Content:

    2.1. Treatment of the individual who is the subject of the Message;
    2.2. Payment activities of the Health Care Provider for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan.
    2.3. Health Care Operations of either
        2.3.1. The Submitter if the Submitter is a Covered Entity;
        2.3.2. A Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or
        2.3.3. The Recipient if (i) the Recipient is a Health Care Provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such Health Care Provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such Health Care Provider;
    2.4. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e);
    2.5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content, provided that the purpose is not otherwise described in section I.2.1-I.2.4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and

2.6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.

3. **Permitted Future Uses.** Recipients may retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient's record retention policies and procedures. If the Recipient is a Participant that is a Business Associate of its Participant Users, such Participant may retain, use and re-disclose Message Content in accordance with Applicable Law and the agreements between the Participant and its Participant Users.

4. **Management Uses.** South Dakota Health Link may request information from Participants, and Participants shall provide requested information, for the purposes listed in the next section Section I.5 of Appendix C. Notwithstanding the preceding sentence, in no case shall a Participant be required to disclose PHI to South Dakota Health Link in violation of Applicable Law. Any information, other than Message Content, provided by a Participant to South Dakota Health Link shall be labeled as Confidential Participant Information and shall be treated as such in accordance with Section V of Appendix C.

5. **Grant of Authority.** The Participants hereby grant to South Dakota Health Link the right to provide oversight, facilitation and support for the Participants who Transact Message Content with other Participants by conducting activities including, but not limited to, the following:

5.1. Determining whether to admit a New Participant;
5.2. Maintaining a definitive list of all Transaction Patterns supported by each of the Participants;
5.3. Developing and amending Operating Policies and Procedures;
5.4. Receiving reports of Breaches and acting upon such reports in accordance with Section IV.3 of Appendix C (Breach Notification).
5.5. Suspending or terminating Participants.
5.6. Resolving Disputes between Participants.
5.7. Managing the amendment of this South Dakota Health Link Policy and System Operation Manual.
5.8. Maintaining a process for managing versions of the Performance and Service Specifications, including migration planning;
5.9. Evaluating requests for the introduction of Emergent Specifications into the production environment used by the Participants to Transact Message Content;

5.10. Coordinating with ONC to help ensure the interoperability of the Performance and Service Specifications with other health information exchange initiatives including, but not limited to, providing input into the broader ONC specifications activities and ONC Standards and Interoperability Framework initiatives; and

5.11. Fulfilling all other responsibilities delegated by the Participants to South Dakota Health Link as set forth in South Dakota Health Link Policy and System Operation Manual.

II. Expectation of Participants

1. Minimum Requirement for Participants that request Message Content for Treatment.

1.1. All Participants that request, or allow their respective Participant Users to request, Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A Participant shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. All responses to Messages shall comply with any agreements between Participants and their Participant Users, and Applicable Law. Participants may, but are not required to, Transact Message Content for a Permitted Purpose other than Treatment. Nothing in this Section II.1.1 of Appendix C shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.

1.2. Each Participant that requests, or allows its respective Participant Users to request, Message Content for Treatment shall Transact Message Content with all other Participants for Treatment, in accordance with Section II.1.1 and Section IV of Appendix C. If a Participant desires to stop Transacting Message Content with another Participant based on the other Participant's acts or omissions in connection with South Dakota Health Link, the Participant may temporarily stop Transacting Message Content with such Participant either through modification of its Participant Access Policies or through some other mechanism, to the extent necessary to address the Participant's concerns. If any such cessation occurs, the Participant shall provide a Notification to South Dakota Health Link of such cessation and the reasons supporting the cessation. If the cessation is a result of a Breach that was reported to, and deemed resolved by, South Dakota Health Link pursuant to Section IV.3 of Appendix C the Participants involved in the Breach and the cessation shall engage in the Dispute Resolution Process in an effort to attempt to reestablish trust and resolve any security concerns arising from the Breach.

2. **Participant Users and Health Service Providers (HSPs).** Each Participant shall require that all of its Participant Users and HSPs Transact Message Content only in accordance with South Dakota Health Link Policy and System Operation Manual, including without limitation those governing the use, confidentiality, privacy, and security of Message Content. Each Participant shall discipline appropriately any of its employee Participant Users, or take appropriate contractual action with respect to contractor Participant Users or HSPs, who fail to act in accordance with the terms and conditions of South Dakota Health Link Policy and System Operation Manual relating to the privacy and security of Message Content, in accordance with Participant's employee disciplinary policies and procedures and its contractor and vendor policies and contracts, respectively.

III. Specific Duties of a Participant When Submitting a Message

Whenever a Participant or Participant User acts as a Submitter by submitting a Message to another Participant or Participant User, the Submitter shall be responsible for:

1. Submitting each Message in compliance with Applicable Law, and Procedures including, but not limited to, representing that the Message is:

    1.1. For a Permitted Purpose;
    1.2. Submitted by a Submitter who has the requisite authority to make such a submission;
    1.3. Supported by appropriate legal authority for Transacting the Message Content including, but not limited to, any consent or Authorization, if required by Applicable Law; and
    1.4. Submitted to the intended Recipient.

2. Representing that assertions or statements related to the submitted Message are true and accurate, if such assertions or statements are required by policies and procedures;

3. Submitting a copy of the Authorization, if the Submitter is requesting Message Content from another Participant or Participant User based on the Permitted Purpose described in Section I of Appendix C. Nothing in this Section shall be interpreted as requiring a Submitter who is requesting Message Content to obtain or transmit an Authorization for a request based on a Permitted Purpose other than the one described in Section I of Appendix C, even though certain other Participants or Participant Users require such Authorization to comply with Applicable Law.

4. For Federal Participants only, in addition to complying with South Dakota Health Link Policy and System Operation Manual, ensuring that Messages submitted by such Federal Participant adhere to interoperability standards adopted by the Secretary of

Health and Human Services, and the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS), as applicable.

IV. Privacy and Security.

1. Applicability of HIPAA Regulations. Message Content may contain PHI. Furthermore, some, but not all, Participants are either a Covered Entity or a Business Associate. Because the Participants are limited to Transacting Message Content for only a Permitted Purpose, the Participants do not intend to become each other's Business Associate by virtue of signing the South Dakota Health Link Participation Agreement or Transacting Message Content. To support the privacy, confidentiality, and security of the Message Content, each Participant agrees as follows:

    1.1. If the Participant is a Covered Entity, the Participant does, and at all times shall, comply with the HIPAA Regulations to the extent applicable.
    1.2. If the Participant is a Business Associate of a Covered Entity, the Participant does, and shall at all times, comply with the provisions of its Business Associate Agreements (or for governmental entities relying upon 45 C.F.R. §164.504(e)(3)(i)(A), its Memoranda of Understanding) and Applicable Law.
    1.3. If the Participant is a Governmental Participant, the Participant does, and at all times shall, comply with the applicable privacy and security laws and regulations.
    1.4. If the Participant is neither a Covered Entity, a Business Associate nor a Governmental Participant, the Participant shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations as if it were acting in the capacity of a Covered Entity or such other standards as decided by South Dakota Health Link.

2. Safeguards. Participant agrees to use reasonable and appropriate administrative, physical, and technical safeguards and any Policies and Procedures to protect Message Content and to prevent use or disclosure of Message Content other than as permitted by Section I of Appendix C.

3. Breach Notification.

    3.1. Each Participant agrees that within one (1) hour of discovering information that leads the Participant to reasonably believe that a Breach may have occurred, it shall alert other Participants whose Message Content may have been Breached and South Dakota Health Link to such information. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, the Participant shall provide a Notification to all Participants likely impacted by the Breach and South Dakota

Health Link of such Breach. The Notification should include sufficient information for South Dakota Health Link to understand the nature of the Breach. For instance, such Notification could include, to the extent available at the time of the Notification, the following information:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content Breached
- Participants likely impacted by the Breach
- Number of individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by the Participant to mitigate the Breach
- Current Status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and South Dakota Health Link in accordance with South Dakota Health Link Policy and System Operation Manual. The Notification required by this Section IV.3 of Appendix C shall not include any PHI. If, on the basis of the Notification, a Participant desires to stop Transacting Message Content with the Participant that reported a Breach, it shall stop Transacting Message Content in accordance with Section II.1.2 of Appendix C. If, on the basis of the notification, South Dakota Health Link determines that (i) the other Participants that have not been notified of the Breach would benefit from a summary of the Notification or (ii) a summary of the Notification to the other Participants would enhance the security of the Performance and Service Specifications, it may provide, in a timely manner, a summary to such Participants that does not identify any of the Participants or individuals involved in the Breach.

3.2. Information provided by a Participant in accordance with this Section IV.3 of Appendix C, except Message Content, may be "Confidential Participant Information." Such "Confidential Participant Information" shall be treated in accordance with Section V of Appendix C.

3.3. Section IV.3 of Appendix C shall not be deemed to supersede a Participant's obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law.

3.3.1. Compliance with Section IV.3 of Appendix C shall not relieve Participants of any other security incident or breach reporting requirements under Applicable Law including, but not limited to, those related to consumers.

V. Confidential Participant Information.

1. Each Receiving Party shall hold all Confidential Participant Information in confidence and agrees that it shall not, during the term or after the termination of South Dakota Health Link Participation Agreement, re-disclose to any person or entity, nor use for its own business or benefit, any information obtained by it in connection with South Dakota Health Link, unless such use or re-disclosure is permitted by the terms of the South Dakota Health Link Participation Agreement.

2. Confidential Participant Information may be re-disclosed as required by operation of law, provided that the Receiving Party immediately notifies the discloser of the existence, terms and circumstances surrounding such operation of law to allow the discloser its rights to object to such disclosure. If after discloser's objection, the Receiving Party is still required by operation of law to re-disclose discloser's Confidential Participant Information, it shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

Appendix D

Organizational Default Settings

South Dakota Health Link sets the following minimum and maximum required settings for organizational access and individual user access (User Access Role).

- Hospital session timeout may not exceed 30 minutes
    - Default is 30 Minutes
- Clinic session timeout may not exceed 45 minutes
    - Default is 45 Minutes
- Password strength (all organization types)
    - Eight (8) Character minimum (default is 8)
    - One (1) Alpha Character required (default is 1)
    - One (1) Numeric Character required (default is 1)
- Password validity may not exceed 180 days
    - Default is 180 days
- Password uniqueness must be a minimum of three (3)
    - Default is 3
- Dictionary checking may be either Lax or Strict
    - Default is Lax
- Password reset may be Denied, Allowed, or Per User
    - Default is Allowed

If individual organizations wish to request an amendment to the minimum or maximum requirements please contact South Dakota Health Link.

User Access Roles

- User Access Roles
    - Provided on the following pages and based on organization type, provider type, and location.

User Access Roles are assigned by each organization based on the access required by each user.

Hospital User Access Levels

	Role	Access Additional Records	Restricted to
Emergency Department Provider	ED Provider	No	ED providers only • (Doctors, NPs, PAs, CNPs (have NPI, DEA or prescription license) including specialists such as Optometry, Dentist, Chiropractic, EMT/Paramedics, etc.)
Emergency Department Staff with Patient Query	ED Staff w Query	Yes • Confidential Patients	ED Licensed Professionals • (RNs, LPNs, Pharmacists, PT, OT, Dietitians, etc.)
Community Provider	Community Provider	Yes • New Patients • Confidential Patients	Non ED provider or Non ED Licensed Professional • (Doctors, NPs, PAs, CNPs (have NPI, DEA or prescription license) including specialists such as Optometry, Dentist, Chiropractic, EMT/Paramedics, etc. RNs, LPNs, Pharmacists, Medical Coder, PT, OT, Dietitians, and other Ancillary Staff (not licensed to write prescriptions)).
Community Staff with Patient Query	Community Staff w Query	Cannot Access Additional Records (Break Glass)	Receptionists, Admissions, HIMs, Nurse Assistants, Billing Staff, etc.
Community Staff without Patient Query	Community Staff w/o Query	Cannot Access Additional Records (Break Glass)	IT Staff, HIPAA Compliance Officer, Audit Personnel, etc.

Clinic User Access Levels

	Role	Access Additional Records	Restricted to
Community Provider	Community Provider	Yes • New Patients • Confidential Patients	Non ED provider or Non ED Licensed Professional • (Doctors, NPs, PAs, CNPs (have NPI, DEA or prescription license) including specialists such as Optometry, Dentist, Chiropractic, EMT/Paramedics, etc. RNs, LPNs, Pharmacists, Medical Coder, PT, OT, Dietitians, and other Ancillary Staff (not licensed to write prescriptions)).
Community Staff with Patient Query	Community Staff w Query	Cannot Access Additional Records (Break Glass)	Receptionists, Admissions, HIMs, Nurse Assistants, Billing Staff, etc.
Community Staff without Patient Query	Community Staff w/o Query	Cannot Access Additional Records (Break Glass)	IT Staff, HIPAA Compliance Officer, Audit Personnel, etc.

Appendix E

End-User License Agreement

As a condition to being allowed access to the South Dakota Health Link "Point of Care" Health Information Exchange ("the System"), I agree to abide by the following terms and conditions:

1. I will not disclose my user name and password to anyone.
2. I will not allow anyone to access the system using my user name and password.
3. I will not attempt to learn or use another's user name and password.
4. I will not access the System using a user name and password other than my own.
5. I am responsible and accountable for all data retrieved and all entries made using my user name and password.
6. If I believe the confidentiality of my user name and password has been compromised, I will immediately notify the help desk at 888-830-1022 so that my password can be changed.
7. I will not leave my computer unsecured while logged into the System.
8. I will treat data available to me through the System confidentially, as defined by HIPAA. I will not disclose any confidential information unless required to do so within the official capacity of my job responsibilities, and then limited to parties with a legitimate need to know.
9. I will not access, view, or request information regarding anyone with whom I do not have a clinical relationship or a need to know in order to perform my job responsibilities.
10. I acknowledge that my use of the System will be routinely monitored to ensure compliance with this agreement.

By continuing, I further acknowledge that if I violate any of the terms as stated above, I am subject to loss of System privileges, legal action, and/or any other action available to South Dakota Health Link.