SOUTH DAKOTA

HealthLink

Exchanging information. Changing lives.

Policy and System Operation Manual

January 2023

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

Revision Log

Date	Revision Type	Summary	Lead Author
October 24, 2022	Annual review & revision	21st Century Cures Act & associated updates	Lisa Moon
January 9, 2023	Revision	Appendix D Update	Lance Jahnig

Table of Contents

1. Introduction

The South Dakota Health Link Policy and System Operation Manual contain policies and practices for the South Dakota Health Link Information Exchange To become a South Dakota Health Link Participant, an organization must agree to adopt the Manual in its current form and fully execute the South Dakota Health Link Participation Agreement.

The Policy and System Operation Manual contents are updated regularly in compliance with applicable Federal and State statutes, rules, laws, and policies related to the operation, technical standards, and exchange of electronic health information (EHI). This includes alignment with emerging legal and policy standards. The Policy and System Operation Manual is meant to be a guide but does not replace legal advice. An electronic version can be found at South Dakota Health Link (sdhealthlink.org)

1.1. Overview

In 2006 the South Dakota Departments of Health, Human Services and Social Services funded the South Dakota Electronic Health Record Assessment (SDEHRA) project to investigate two key topics:

- The usage of electronic health records in the state
- The perceptions of providers and consumers in relation to electronic health records and health information exchange

In 2008 the South Dakota eHealth Collaborative was established by the Governor's Health Care Commission to develop a long-range plan to facilitate implementing interoperable information technology to improve the quality, safety, and efficiency of healthcare in South Dakota.

The Collaborative was formed to address both the barriers found in the SDEHRA phase and the suggestions from the Zaniyah Taskforce, which involved health information technology.

- People will continue to seek and receive healthcare
- Documentation of that healthcare will continue to be needed
- Health Information Exchange will continue to be needed
- Electronic health records and electronic data exchange are happening and evolving
- Single data entry is ideal

The results of these efforts include the formation and implementation of the South Dakota Health Link Information Exchange.

1.2. Mission Statement

Foster the sharing of information through a secure platform to improve the quality, safety and efficiency of care provided to all citizens.

1.3. Vision & Goals

- To improve care by reducing medical errors associated with inaccurate and incomplete information to healthcare providers.
- To reduce the cost of exchanging information among healthcare providers by increasing the use of electronic methods of sharing.
- To improve communication among healthcare providers and patients in order to provide the right care at the right time based on the best available information.
- To reduce the number of duplicate tests to give specialists a more comprehensive view of the patient upon referral, and to expedite the reporting of opinions between specialist and referring physicians.
- To improve efficiency and value of electronic health records and to assist those physicians without an EHR to better organize and retrieve test results.

South Dakota Health Link is a member driven organization operated by the South Dakota Department of Health. Launched in 2009 in response to the American Recovery and Reinvestment Act (ARRA, 2009) and the Health Information Technology for Economic and Clinical Health Act (HITECH, 2009) to promote the adoption and meaningful use of health information technology in health and care. South Dakota Health Link continues to meaningfully support the advancement of information exchange across an expanded community of participants and users as described in the 21st Century Cures Act. (Cures Act, 2020).

Connecting hospitals, Federally Qualified Health Centers, primary care providers, specialists, labs, pharmacies, and public health agencies – South Dakota Health Link allows participating providers to share a limited set of electronic patient medical record information safely and securely. The network enables faster, more accurate diagnosis and treatment of patients and reduces physician burden when searching for and locating critically important health information. The network ensures critical, life-saving information is available to providers at the point-of-care when and where it is needed for regular and emergency care. The goal is to help providers save time, reduce costs, and improve quality, safety, and efficiency of care for South Dakota residents.

South Dakota Health Link is continually growing and provides services to participant organizations serving South Dakota, and neighboring states of Iowa, Minnesota, Nebraska, North Dakota, and Wyoming. South Dakota Health Link is also a member of the eHealth exchange. South Dakota Health Link core service offerings enable health information to be available at the point-of-care for more than 2 million + individuals that live, work, and recreate in South Dakota and adjacent states. South Dakota Health Link's critical infrastructure is financially supported through member fees and grant funding.

1.4. Governance

SDHL is a public-private partnership between the South Dakota Department of Health (SDDOH) and participating member organizations. The South Dakota Department of Health performs the business, operation, fiduciary, and oversight functions of the Statewide information exchange network. Its members are participant organizations that are responsible for the treatment, payment, and health care operations of patients across the Midwest and Central Plains. Figure 1 shows the South Dakota Health Link governance structure.

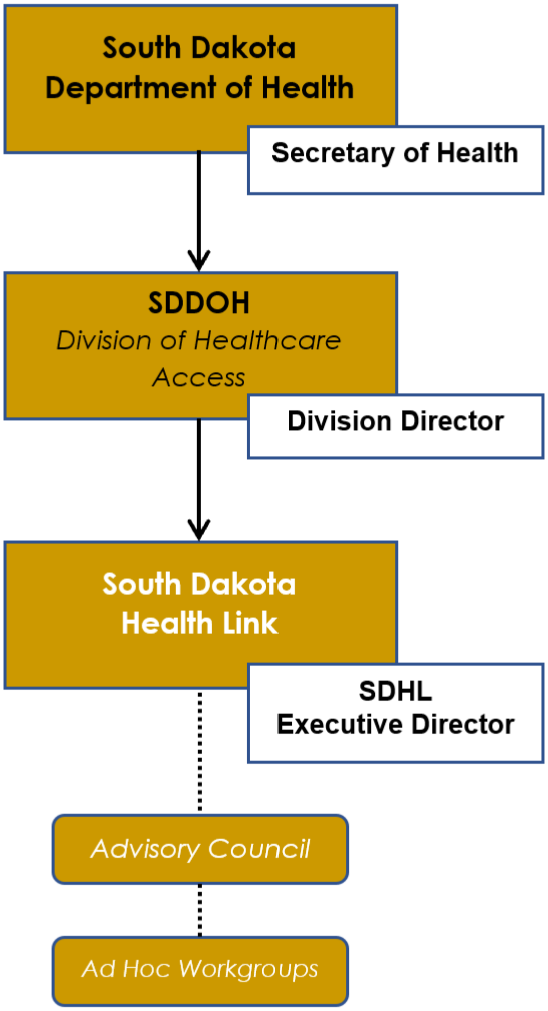

Figure 1: South Dakota Health Link Governance Structure (2022)

The South Dakota Department of Health (SDDOH) secretary of health provides oversight to South Dakota Health Link including the review and approval of recommendations from the Advisory Council related to South Dakota Health Link business operation and services. The Division of Healthcare Access under SDDOH is the primary contact for South Dakota Health Link acting as a champion and sponsor for the greater healthcare community and South Dakota Health Link members.

South Dakota Health Link is led by an executive director employed by the South Dakota State Department of Health. The executive director serves several roles. They function as the main point of strategic and operational integration between the State DOH, the Department of Human Services, South Dakota Health Link member organizations and contracted technology vendors. The Executive Director has responsibility for day-to-day operation. The Executive Director also ensures strategic, operation and financial alignment with Federal, State, and regional activities as they relate to the management and exchange of electronic health information (EHI). In addition, the Executive Director serves a dual role as a member of the South Dakota Health Link Advisory Council.

The South Dakota Health Link Advisory Council is made up of members representing the State of South Dakota (DOH, Medicaid, Department of Social Service), Medical Centers and Hospitals, Physicians, Pharmacists, System Users and Technology Vendors, etc. The list of Advisory Council members can be found here Advisory Council - Health Link (sdhealthlink.org). The South Dakota Health Link Advisory Council makes recommendations to the SDDOH on behalf of the member participants. SDDOH then reviews and may approve Advisory Council recommendations based on merit, demand, emerging need, funding, and feasibility.

South Dakota Health Link may also recruit members, coordinate and hold workgroups at any time to advance business, operation, technical, policy or financial sustainability issues that arise. Workgroups allow member participants to bring their firsthand experience to a community conversation with the purpose of solving for new or emerging issues and use cases.

1.5. South Dakota Health Link Network

South Dakota Health Link uses a federated approach acting as the convenor, integrator and network facilitator for information exchange. Member organizations sign a participation agreement and are onboarded to the network through a registration and technical process. Participating organizations may also include South Dakota Department of Public Health, Health and Human Services, Department of Corrections, and other State Agency programs.

South Dakota Health Link contracts with a technology vendor that is responsible for all technical aspects of the *Health Link* platform, services, implementation, exchange capabilities and security. The technical vendor is also responsible for controls related to privacy, security and technical compliance requirements for the collection, storage, and exchange of electronic health information. This includes emerging technical standards and requirements identified by the Office of the National Coordinator and Health and Human Services like those in the 21st Century Cures Act.

All South Dakota Health Link participants (hospitals, ambulatory care settings, etc.) must be legally connected to the network. Legal connection is accomplished through participation agreement which outlines the terms and conditions for sharing electronic health information. The participation agreement includes data sharing and business associated agreement (BAA) requirements consistent with State and Federal regulations. It also describes the permitted purposes for which electronic health information can be shared among participating organizations.

2. Participation Obligation

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

South Dakota Health Link makes every effort to ensure safe, secure, and reliable 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 by fully executing the South Dakota Health Link Participation Agreement that enables a trusted network of exchange to exist.

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

Any participant that joins South Dakota Health Link must confirm their commitment to compliance with Health Insurance Portability and Accountability Act (HIPAA) rules and regulations as set forth in 45 CFR 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) through their policies and practices. South Dakota Health Link participants must also consider their obligations under the 21st Century Cures Act, Trusted Exchange Framework and Common Agreement (TEFCA) and 42 CFR Part 2 protection of sensitive data. Any organization found to not to be compliant will be subject to enforcement as described in the applicable statute, public health code, rules, or policy.

2.1. Provider Participation

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 Manual may be revised and updated annually. Each Participating Organization is responsible for ensuring it has in its possession and follows the most recent version of the South Dakota Health Link Manual which can be found at Policy & System Operation Manual - Health Link (sdhealthlink.org).

Each Participating Organization is responsible for having 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 Participating Organization shall comply with the policy that is more protective of individual privacy and security. Participating Organizations 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 Participating Organization shall have policies and procedures to promote the integrity of the PHI maintained and made 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.") Participating organizations will not send sensitive data to South Dakota Health Link.

2.2. Health Plan Participation

A Health Plan may qualify as a participating organization in the South Dakota Health Link network when they sign the Participation Agreement (PA) and Business Associate Agreement (BAA). A health plan is a HIPAA covered entity. Clinical data access would be for permitted purposes related to payment and health care operations. Health Plans shall use the minimum amount of data necessary. Health Plans would only have access to clinical data for those members that they serve through medical benefit contracts. Health plans would need to make a special request to South Dakota Health Link in which they identify a specific use case, the permitted purpose, and the patients of interest using a roster to ensure that only individuals for which a health plan has a contractual obligation are included in the identified use case. Examples may include, but not be limited to conditions of participation like admission, discharge and transfer alerts required by CMS, care coordination, quality assessment, improvement activities, and other purposes specifically listed in 45 CFR 164.501. The Health Plan is not permitted to use data to deny insurance coverage or benefits to any individual.

2.3. Patient Participation

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 chooses to Opt-Out of South Dakota Health Link.

If a Patient does not Opt-Out of South Dakota Health Link, their PHI will generally be disclosed in response to a specific request, query, or inquiry, made by a Participating Organization for a permissible purpose as defined by HIPAA. 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 hospital visits. Patients may not Opt-Out of Clinical Event Notifications. CMS Conditions of Participation (CoP) require hospitals, including psychiatric hospitals and critical access hospitals to send electronic patient event notifications for Admission, Discharge and Transfer (ADT) Alerts for all transitions of care (TOC) (42 CFR 482.24(d), 482.61(f), and 485.638(d)).

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 Resources for Patients | South Dakota Health Link (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://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. Minor child in South Dakota is an individual under the age of 18 years (South Dakota § 26-1-1).

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.

Patients 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://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 submitted 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 and any data prior to the date the Patient opted back in will be available in the Point of Care.

2.4. Information Blocking

South Dakota Health Link encourages safe, secure, and electronic health information exchange to improve patient safety, care, and coordination in compliance with state and federal laws, including the 21st Century Cures Act Information Blocking Rules.

The 21st Century Cures Act prohibits specific actors; healthcare providers, HIT developers, Health Information Networks (HINs) and Health Information Exchanges (HIEs), from the impermissible interference with the access, exchange, or use of electronic health information (EHI) unless the practice is required by law, or a regulatory exception applies (45 CFR 171.103). EHI is defined as electronic protected health information (PHI) included in the designated record set as defined in the HIPAA Privacy rule. Information blocking claims are primarily investigated and enforced through the Health and Human Services Office of Civil Rights Information Blocking FAQs (healthit.gov).

There are eight exceptions that the Office of Civil Rights considers prior to making an enforcement decision.

1. Exceptions that involve procedures not fulfilling requests to access, exchange, or use of EHI:

    - Preventing Harm Exception

  - It will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.
- Privacy Exception
  - It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.
- Security Exception
  - It will not be information blocking for an actor to interfere with the access, exchange, or use EHI in order to protect the security of EHI, provided certain conditions are met.
- Infeasibility Exception
  - It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.
- Health IT Performance Exception
  - It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

2. Exceptions that involve procedures for fulfilling requests to access, exchange, or use of EHI:

- Content and Manner Exception
  - It will not be information blocking for an actor to limit the content or its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met.
- Fees Exception
  - It will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.
- Licensing Exception
  - It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.

Participating organizations shall notify South Dakota Health Link of suspected information blocking incidents. South Dakota Health Link may investigate claims of information blocking using their audit and compliance procedures. Participating organizations may be required to submit claims to the Health and Human Services Office of Civil Rights using the Information Blocking | Health IT Feedback and Inquiry Portal.

3. Membership Fees

South Dakota Health Link is a member funded enterprise. Membership fees are outlined in the participation agreement. Fees may be subject to change over time.

3.1. 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.

3.2. Past Due Accounts

Participant's 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.

3.3. Interface Modifications

Major changes to the interfaces or any Direct member who wishes to change their domain address may be subject to change fees or other costs associated with the change.

4. South Dakota Health Link Service Offerings

South Dakota Health Link is able to combine data from systems like electronic health records, enterprise resource planning systems, enterprise data warehouses and across health information exchanges to provide actionable insights, with the consent of members. This enables seamless, standard, systematic and high-availability sharing of electronic health information in compliance with national health IT standards outlined in Section 3.5 of the Certified Health IT - Health IT Playbook.

Access to South Dakota Health Link is a one-click, on-demand transaction to access continuity of care documents even from networks with differing data protocols and electronic health record variations, eliminating barriers to information sharing.

South Dakota Health Link ***Core Services*** include:

4.1 ***Point of Care Exchange*** connects participating providers through an electronic interface to real-time information necessary for treatment and care coordination. South Dakota Health Link facilitates the transfer of critical information to support clinical decision-making at the point-of-care through a single sign on feature that integrates the information exchange with electronic health records. Available information includes clinical, encounters, laboratory, radiology, pathology, and information available in an HL7 Continuity of Care Document (C-CDA/CCD). Point of Care Exchange may include the following services:

4.1.1 ***Clinical Event Notifications*** (Notify) is a flexible user configured admission, discharge, and transfer (ADT) notification service. Notify delivers real-time notifications to clinicians and care managers to assist with the monitoring of care events that impact patient treatment and care coordination.

4.1.2 ***Prescription Drug Monitoring Program*** South Dakota Health Link's Point of Care Exchange Allows access to the state's PDMP within the portal for users credentialed by the SD Board of Pharmacy**.** The Prescription Monitoring Program tab displays filled Schedule II, III, IV, and V prescriptions as reported by dispensers.

4.1.3 ***eHealth Exchange*** is a connection to the broader national health information network. South Dakota Health Link is 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.

4.2 ***Health Insights*** is a population health analytics service that used by South Dakota Health Link participant organizations to define population and run analysis to manage risk, outcomes, and measure quality. Health Insights brings cost effective and easy to use analytic tools to the South Dakota Health Link participants.

4.3 ***Direct Secure Messaging*** is a standards-based electronic communication tool made for healthcare. Using email-like features a participating organization can seamlessly communicate through a health information service provider that is nationally accredited. Endorsed by the Office of the National Coordinator and designed for HIPAA compliant healthcare communications, Direct Secure Messaging has become a foundational tool for modernizing electronic communication in health and care.

4.4 ***Community Referrals*** are enabled through the connection between SDHL and the Community Information Exchange. SDHL participants with social determinants of health needs can be connected to human service resources in their communities.

South Dakota Health Link service catalog that fully describes these services can be found in Appendix A.

5. Electronic Health Information Confidentiality, Privacy, and Security

5.1. Confidentiality

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 Organization level, or an implied consent received through relationships indicated in HL7 transactions.

- Active care relationships link patient to their providers through ADT or CCD data (HL7). This linkage through treatment relationship can function as an implied consent, and that relationship allows the doctor to access unrestricted portions of a patient’s health record based on role.
- Patients that do not want to participate in information exchange may opt-out of South Dakota Health Link using the SDHL-NonParticipationForm.pdf (sdhealthlink.org)
- For the opt-out consent method, a patient has to opt-out before their data is excluded through signing the opt-out form, having their provider verify with signature or notary, and submitting that form to South Dakota Health Link.
- The default status is that all patients are opt-ed in, until they opt-out. This means that their patient data is included (made accessible) up and until the patient completes the opts-out process.
- Should the patient choose to participate at a later date then the patient can opt-back into South Dakota Health Link. At that time, all past, present, and future data will be included going forward in the Point-of-Care record.

Some limited options for sensitive data are available based on type of data and type of provider. Most providers do not send sensitive data to the HIE.

5.2. Information Privacy

The HIPAA Privacy Rule ensures that Protected Health Information (PHI) is shared with patient permission or for care coordination purposes between covered entities.

South Dakota Health Link relies on Participant members to apply strong privacy controls through well-established policies, procedures and practices used in their organizations. Privacy is also maintained through HIPAA compliant technology controls applied by South Dakota Health Links' vendor business and technical rules and policies.

The HIPAA privacy rule allows for the confidentiality of patient records, while also enabling the sharing of patient health information for treatment, payment, and operation by covered entities (health care providers, employer sponsored payers and healthcare clearinghouses) and their business associates (45 CFR 164.500 – 164.534). HIPAA minimum necessary rule ensures that only the patient information necessary to complete the stated purpose is accessed and available to end-users.

HIPAA privacy standards outline a set of permitted purposes and disclosures when protected health information is allowable and when it is necessary to obtain or have on file an authorization to release information from a patient. South Dakota Health Link relies on participating providers and organizations to obtain the appropriate authorizations to share protected health information.

5.3. Data Security

HIPAA Security Rule establishes national standards to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity (45 CFR 160 and Subparts A and C of Part 164).

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

South Dakota Health Link accomplishes 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. This includes the maturation of current data and security standards to include those identified in the 21st Century Cures Act.

Maintaining the security, confidentiality, integrity, and availability of health information is South Dakota Health Link's top priority. South Dakota Health Link technology vendor is NIST compliant and HITRUST certified. All requests for security risk assessment, penetration testing/results, disaster recovery plans, etc. will be directed to the technology vendor.

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.

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

5.3.1. Provisioning Credentials

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 usernames or users can self-assign usernames 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. Point of Care Exchange Release 75.7.0 allows an organization to set up two factor authentication utilizing Google Authenticator as an additional layer of security.

Through single-sign-on 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.

5.3.2. 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 authorization occurs at the application level. A system administrator can create various user roles as found in Appendix D, 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 based on data contributed by their organization. Access can be refined further on the individual user level, thus supporting personalization. Patients can receive a copy of their medical record through a request to their health care provider.

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.

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. Administrators may 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. See Appendix D for the role settings.

Other roles may 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.

5.3.3. 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 that is fully protected through security controls that meet or exceed industry standards. These are examples of physical security safeguards.

5.3.4. Encryption

South Dakota Health Link protects data while in-transit and while at-rest via multiple mechanisms. Technical security safeguards such as those used by the Direct Protocol, Secure Sockets Layer (SSL), Public Key Infrastructure (PKI), one-way hashing of certain data types such user passwords, and symmetric encryption of clinical data at-rest are integral to the platform.

South Dakota Health Link uses health care compliant national standards and methods to protect data during transmission:

- South Dakota Health Link encrypts data transmissions using 128bit Transport Layer Security (TLS) or SSL encryption.
- South Dakota Health Link secures connections to its servers for transmission and receipt of Health Level Seven (HL7) data with a LAN to- LAN (L2L) IPSec Virtual Private Network (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 Online Certificates Status Protocol (OCSP) /Certificate Revocation Lists (CRLs) for revocation.

5.3.5. 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. Non-repudiation refers to a service, which provides proof of the origin of data and the integrity of the data.

- 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 SDHL suite of services, 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. South Dakota Health Link also uses highly secured web services (signed with X.509 certificates) throughout our Service Oriented Architecture.

5.3.6. 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, and the 21st Century Cures Act 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.

SDHL personnel 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.

5.3.7. Network Monitoring and Breach Notification

South Dakota Health Link's vendor protects against external breaches by maintaining perimeter firewalls, Intrusion Detection System (IDS) 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. Report any incident to South Dakota Health and complete a full documentation cycle to ensure that the incident does not reoccur. If appropriate, incidents related to breach may be reportable to the Department of Health and Human Services Office of Civil Rights (OCR).

5.4. Unauthorized Access

Any individual may submit a complaint about a suspected or known unauthorized 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 Personnel.

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

When deemed necessary, South Dakota Health Link personnel 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.

5.4.1. Duty to Investigate

By signing the Participation Agreement each organization accepts responsibility for their end-users. This includes a duty to proactively monitor, investigate and report unauthorized access to protected health information (45 CFR 160 and 164.400-414).

Each Participant shall promptly investigate reported or suspected privacy breaches of Participant's System. 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.

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.

5.4.2. 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.

5.4.3. 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.

5.4.4. 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.

5.4.5. *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/their PHI.

5.4.6. *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.

5.4.7. *Notification to South Dakota Health Link*

A Participant primarily responsible is to 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.

5.4.8. *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 personnel 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.

5.4.9. 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 personnel 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.

5.5. 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 activity is within expected parameters. Any anomalous or suspicious finding should be reviewed by the South Dakota Health Link personnel. South Dakota Link personnel 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 personnel 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 personnel or their designee when needed.

5.5.1. Audit Trails/Logs

The proposed solution supports full HIE audit logging capabilities, 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 service comes back online. 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 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 personnel 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 South Dakota

Health Link personnel or their designee 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 South Dakota Health Link personnel and/or 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 South Dakota Health Link personnel or their designee 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.

5.5.2. Accounting of Disclosures

Patients 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 personnel. Efforts will be made to respond to such request in thirty (30) days, however, in the event more time is needed the patient will be notified.

Accounting of disclosures will include a 3 – 6-month lookback of clinical data available in the system. This may not include queries through eHealth exchange as this data does not persist in the database. This is an administrative procedure only. It is not a comprehensive record review by a licensed professional.

South Dakota Health Link will provide an accounting of disclosures to consumers at no cost once in a twelve (12) month period. If a consumer requests a subsequent accounting within the twelve (12) month period, they will be notified of the fees that may be charged to generate the report. Such fees shall only include actual and reasonable costs for staff time and copying.

6. System Support and Service Levels

6.1. User System Support

Please contact SD Health Link if you have issues with logging in with your account. We are available 8 am to 5 pm, Monday through Friday. Some organizations manage the user accounts and can assist you with account issues. Please send all PHI securely and do NOT submit any PHI through the contact page or email.

- Via Phone @ (605) 800-1678
- Contact Us – SD Health Link – choose the product under the request type.
- poc-help@sdhealthlink.org – this will send an email to South Dakota Health Link staff and is not part of a ticketing support system

6.2. How to Contact Support

Support Services are available 24×7 every day of the year to handle your support issues. Please send all PHI securely and do NOT submit any PHI through email.

- Via Phone @ (888) 830-1022 – Follow the tree to appropriate number for your issue.
- support@healthcatalyst.atlassian.net This email address auto generates a ticket number via our ticketing system. This allows for a quick ticket # assignment, however, the ticket will still require review by a resource to insure it is prioritized and all required information is provided to allow for processing of the ticket.
- Your organization may be provided with access to the ticketing system. Please contact South Dakota Health Link for more information.

6.3. Ticketing Guidelines for Ticket Submission

1. South Dakota Health Link member name
2. URL
   - https://member.sdhealthlink.org/ProAccess/Login
   - https://notify.medicity.com/notify/user/login
3. Client name, phone number, location city and email address
4. Practice name, (if needed)
5. Product Name:
   - Community Health Record (Point of Care) or
   - Notify
6. Current impact to your organization – Critical, Medium, or Low
7. Description, as detailed as possible, regarding the issue
   - Is this a brand-new issue or have you had this issue before
   - Have there been any changes to your environment, including but not limited to network changes, application updates, updates to your PC, location of your PC
8. What are the best contact hours for us to reach you?

A South Dakota Health Link Severity 1 issue is one that largely impacts patient care and has no available workaround. Issues that largely impact patient care, but do have workarounds, are generally deemed Severity 2 issues. A Severity 1 can present itself in many ways in a production environment. The declaration of a Severity 1 will require one primary contact (from SD South Dakota Health Link and client) and detailed information including, but not limited to, the production environment impact, steps to reproduce, patient demographics, Nexus Engines and Instances, endpoints, IP addresses, usernames, HL7 messages, error messages, and Community Hub requests and responses.

The Table 1 below defines ticket severity and South Dakota Health Link technology vendor response times for each. Potential Severity 1 incidents are treated as Severity 1 incidents until they are deemed otherwise. There are also times that both parties may agree to change the ticket severity. It is anticipated that during a Severity 1 event that both parties be engaged until it is resolved, or the severity is changed. This is especially important for after hours, weekends, and holidays. If South Dakota Health Link technology vendor cannot reach the client within 1 hour, the Severity 1 will be downgraded until the next business day.

SEVERITY DESCRIPTION

SEVERITY	DESCRIPTION
1	Loss of service, or serious impairment of service, which cannot be circumvented. Examples of this type of problem are: • Web server not accepting connections due to functionality or performance issues • Persistent inability to access clinical information due to functionality or performance issues • Critical product feature does not work (identifiable part of functionality), no workaround exists, or workarounds are impractical • User data is corrupted • Reproducible, unavoidable crash or deadlock • Legally incorrect text or graphics
2	A problem exists which can be reasonably circumvented or does not materially affect normal operations. Examples of this type of problem are: • A non-functioning product feature which is not critical to a User (identifiable part of functionality) • Part of a product feature is affected, a viable workaround exists • Performance is less than optimum • Highly visible usability problem that doesn't affect functionality
3	Failure of a system which does not have any effect on normal operations

Table 1 Severity Levels 1 - 3

7. Medical Record Request

Healthcare providers connected to South Dakota Health Link can assist patients in obtaining a copy of their record by running a report of available records in Point-of-Care. Any records available in Point-of-Care can be printed by the patient's healthcare provider at the time of the visit. Healthcare providers needing assistance with the record search and printing function can reach out to South Dakota Health Link for support.

Please note that records queried for and found through the eHealth Exchange are not persistent, meaning they are only available for the period of time that a provider at the Point of Care is reviewing them for treatment and care coordination activities. End-users are able to print and download documents that are returned in a query request. The only item that is not printable is the Prescription Drug Monitoring Program (PDMP) data in the Point of Care.

Patients wanting to connect and retrieve records through application programming interfaces (API) to a third-party data aggregator will want to reach out directly to the health care provider or health system that is the primary source of their records. South Dakota Health Link patient API will be available through their technology vendor.

Patients experiencing difficulty when requesting medical record access may report the issue to their healthcare provider or health system, and to South Dakota Health Link. The issue may result in a claim submission to the Information Blocking | Health IT Feedback and Inquiry Portal for further investigation.

8. Training and Education

South Dakota Health Link periodically offers training and education on topics related to use cases, onboarding, and implementation. Webinars and special trainings are posted online at Webinars – Health Link (sdhealthlink.org) Informational links can be found at Health Links – Health Link (sdhealthlink.org). If you don't see information that you are looking for on the South Dakota Health Link website, please reach out at 605-800-1678.

Training associated with becoming a new South Dakota Health Link Participating Organization:

- After the participation agreement is signed then onboarding activities begin.
- Onboarding activities are accomplished through scheduled and personalized training with a South Dakota Health Link Personnel. These sessions ensure that your Participating Organization can successfully join and implement the South Dakota Health Link tools.
- Technical interfaces are completed during technical onboarding. South Dakota Health Link works with your organizations Health IT department. Mutually agreed upon meetings are scheduled to review technical requirements, configuration, and testing.
- Ongoing support is available for all Participating Organizations as part of member benefits.
- Technical service issues should follow instructions found in Section 6.

APPENDIX A

South Dakota Health Link Service Catalog

South Dakota Health Link uses national standards to provide state of the art health information exchange services that deliver safe, secure, and fully accessible clinical information to its authorized users. Those services include the following:

South Dakota Health Link Core Services include:

1. Point of Care

Point of Care allows providers to access critical clinical information and receive clinical event notifications into their workflow. This reduces administrative burden on providers who are often left to search and find necessary information in the vast amount of available data.

Secure Point of Care allows:

- Access to patient health records across the network of community providers is based on role, provisioned credentials and aligns with HIPAA
  - Permitted Purpose
  - Minimum Necessary rules
- The sharing of critical health information across a diverse and interprofessional care team that spans organizations and regions.
- Timely access to critical, life-saving information that is important to managing a medical emergency treatment.
- Access to a patient's care summary, lab results, and transcribed radiology reports.
- Access to pharmacy fill data
- Prescription Drug Monitoring Program
- Referrals
- Direct Secure Messaging
- eHealth Exchange

Point of Care features enhance provider experience and streamline clinical process through:

- 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.

South Dakota Health Link supports safety, the reduction of medical errors and the improved quality of care and health outcomes through its Point of Care service. Bringing data together to form information and provide insights is key to the success of South Dakota Health Link. Point of Care is the tool that enables a better experience for providers and patients.

1.1. Clinical Event Notifications (Notify)

Clinical event notification is a primary use case for health information exchange. Built on national standards for exchange of information "Notify" assist providers and their staff to monitor and intervene in transition of care (ToC) and care coordination services.

Notify is a flexible, user-configured solution that puts the power of real-time notifications in the hands of those who need them in clinical service delivery. South Dakota Health Link providers subscribe to receive notifications when a patient is admitted, discharged, or transferred from a hospital, emergency, or other health care setting to ensure the right health care decisions are made efficiently and effectively.

South Dakota Health Link providers customize their Notify subscription to ensure that they receive the information they want, how they want it, and when they want it. The subscription allows a provider, to determine what cohorts of patients with certain conditions in the larger population they want to be notified about for activities like post-acute care follow-up, care coordination and disease management. South Dakota Health Link providers are able to configure their alerts for those patients, identify how they want to be notified, and identify if they want to receive real-time notifications or as a summarized report.

The Clinical Event Notification service supports the Center for Medicare and Medicaid Interoperability and Patient Access Rule Condition of Participation requirements (CMS-9115-F) which requires hospitals to send ADTs to notify relevant members of a patients care when they participate in the network. Clinical event notifications enable care coordination and help to initiate timely interventions necessary to improve health as individuals move across the care continuum.

South Dakota Health Link participates in local, regional, and interstate clinical event notification in compliance with the 21st Century Cures Act and Information Blocking final rule. Organizations interested in Notify participation should contact South Dakota Health Link to join its comprehensive community of partners (providers, community-based organizations, behavioral health, nursing homes, payers, etc.).

1.2. Prescription Drug Monitoring Program

South Dakota Health Link is connected through an electronic gateway to the State Prescription Drug Monitoring Program (PDMP). The PDMP is a statewide electronic database developed to track distribution and use of controlled substances.

The PDMP was authorized through South Dakota legislature in 2017 (34-20E-2). The PDMP has been established to improve patient care by providing prescribers and pharmacists with a comprehensive controlled substance history for their patients and to help identify potential abuse or misuse of controlled substances.

South Dakota Health Link's Point of Care Exchange allows providers to access the state's PDMP within the portal. This Prescription Monitoring Program tab displays filled Schedule II, III, IV, and V prescriptions as reported by dispensers.

For providers to use this feature through SD Health Link, they must complete the following steps:

- If you currently have an account with SD's PMP AWARxE, log in and update your account to include your DEA number or Professional License Number.
- If you do not have a SD PMP AWARxE account, go through the program's website at http://southdakota.pmpaware.net and click "Create an Account."
- Contact the SD PDMP with questions by emailing sdpdmp@state.sd.us
- Once your SD PMP AWARxE account is update or approved, reach out to South Dakota Health Link to create your end user account.

South Dakota Health Link’s access to PDMP is state of the art and designed to decrease provider burden while enabling seamless experience in their daily workflow. The gateway features deliver timely, accurate and available information on controlled substances. Providers can enjoy a comprehensive record of Schedule II, III, IV and V medications from any system where South Dakota Health Link is enabled.

1.3. eHealth Exchange National Network

South Dakota Health Link is a member of the eHealth Exchange. The eHealth Exchange is a national Network of Networks connecting 50 states, federal agencies, and non-federal health care organizations. Using national standards for exchange of electronic health information and a policy and legal framework that is nationally accepted, the eHealth Exchange is the largest network of organizations in the United States.

South Dakota Health Link Participating Organizations have the ability to access patient electronic health information across an expanded network using the eHealth Exchange. This capability enables more robust set of patient data to be available in the Point of Care platform.

Providers make a request through Point of Care, and that request yields available information through the continuity of care document (CCD). The information is available for that one instance, does not persist and goes away after the provider and patient encounter. The next time the provider needs to access the expanded record, they request another query be run and the updated CCD is presented. Any information that is new or newly available will be included in that request.

Note that all HIE-to-HIE (or Federal Agency) connections will be made in accordance with the eHealth Exchange policies and procedures available in Appendix C. All eHealth Exchange HIEs (or Federal Agencies) connecting with South Dakota Health Link must be a validated member of the eHealth Exchange. A list of organizations that participate in the eHealth Exchange national Network of Networks can be found at Participants - eHealth Exchange.

2. Health Insights Analytic Service

Health analytic services are essential to the advancement of health care initiatives like accountable care organizations, new models of care and payment, care management and population health. Analytics are used for operational reports and to understand the health of populations.

Population health is the management of cohorts within a defined population using evidence-based interventions to improve health outcomes and well-being. Population health may include case and chronic disease management (e.g., diabetes, asthma, cardiac disease) or may be linked to quality metrics necessary to participate in value-based care and payment.

Providers, Accountable Care Organizations, and others that participate in population health typically benefit from data analytics tools used to understand the prevalence of disease, utilization of healthcare resources, outcomes, and total cost of care. Insights derived from data analysis is used to better understand and manage individuals, cohorts, and populations of interest. Data analytic tools can be costly, difficult to use and their efficacy dependent on the ability of the analyst to master data.

South Dakota Health Link is committed to support the growing number of population health initiatives in South Dakota by providing a limited starting set of data analytic capabilities through its Health Insights service. Health Insights is a visually oriented analytics tool that allows South Dakota Health Link to define populations quickly, without using sophisticated or customized SQL coding to reduce analyst workload and increase analytics productivity.

Health Insights Benefits

- Improve stakeholder buy-in and trust throughout the analytics process.
- Speed up analysis and accuracy by having access national quality improvement and regulatory code sets.
- Maintain and govern organization-wide population definitions for key populations.
- Reduce costs by growing analytic capabilities without increasing headcount.
- Improve data governance and consistency by leveraging Health Insights reusable value sets and populations.

Data used for health insights is deidentified. Types of data available include clinical and claims. Data types will expand as new data and sources become available.

Health Insights use cases are driven by member demand and public health activities as defined by HIPAA (45 CFR 164.512(b) or 45 CFR 164.514(e)). South Dakota Health Link member participants can submit proposed population health use cases to South Dakota Health Link through a website submission. All request for operational or population level reports are reviewed and approved based on feasibility measures like cost, resources, and community impact.

3. Direct Secure Messaging

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 Direct Implementation Guide is available at https://sdhealthlink.org/healthlink-resources/policy-system-operation-manual/.

Direct does not require providers to implement software. Instead, the process for sending information is similar to sending e-mail today only HIPAA compliant and encrypted.

- 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.
- Then the provider would be identity validated using their professional demographics, office location, national provider ID, and other available documents to establish ID.
- Then 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.

South Dakota Health Link is a member of DirectTrust**.** 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.

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.

The 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.

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 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.

South Dakota Health Link will consider connections with HISPs outside our network who are also DirectTrust members. All HISP-to-HISP connections will be made in accordance with DirectTrust policies and procedures available at Direct Secure Messaging » DirectTrust. All HISP's connecting to South Dakota Health must be a DirectTrust member.

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.

4. Community Referrals

Community referrals are enabled through the connection between SDHL and the Community Information Exchange. SDHL participants with social determinants of health needs can be connected to human service resources in their communities.

Individuals with social care needs can be assessed, linked with the appropriate resource and feedback made available to both the referring organization and the referral target (e.g., food pantry, transportation, etc.). This seamless electronic communication enables partners in the community to better coordinate care and close the loop on critical information needed to ensure the individual is connected to and benefits from the referral made to the community resource.

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 submits the Opt-Out form suppressing their data from 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 may 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 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 SDHL-NonParticipationForm.pdf (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 sdhealthlink.org. The Patient may Opt-Out by completing the Opt-Out form found online at sdhealthlink.org.

4. A Patient may Opt-Out of the Health Information Exchange by having a conversation with their physician and obtaining a physician signature.

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. 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.

7. 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 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 and prior data will be available.

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 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, Payment, Health Care Operations, and Authorization based disclosures as defined by HIPAA;

   2.2. Transaction of Message Content related to value-based payment models, alternative payment arrangements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements. This could include, but is not limited to, participation in Medicare bundled payments, the Medicare Shared Savings Program, other Medicare Alternate Payment programs, Medicaid Managed Care programs or commercial value-based payment programs.

   2.3. Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agency's statutory obligations for programs the agency administers including, but not limited to: (i) activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; (ii) for the purpose of the Department of Veterans Affairs determining the individual's eligibility or entitlement to benefits under the VA upon separation or discharge of the individual from military service; (iii) to determine eligibility for or entitlement to or provision of other government benefits; (iv) for activities related to eligibility for or enrollment in a health plan that is a government program; (v) for administering a government program providing public benefits, to coordinate covered functions; or, (vi) to improve administration and management relating to the covered functions of such government programs;

   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. Transaction of Message Content in support of an individual's: (i) right to access their health information or (ii) right to direct with whom their information can be shared or where their information should be sent. For the avoidance of doubt, a Participant may be prevented from disclosing information due to Applicable Law even though the individual asserts this Permitted Purpose;

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 2. 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. Evaluating requests for and approving new Use Cases;
5.4. Developing and amending Operating Policies and Procedures;
5.5. Receiving reports of Breaches and acting upon such reports in accordance with Section IV.3 of Appendix C (Breach Notification).
5.6. Suspending or terminating Participants.
5.7. Resolving Disputes between Participants.
5.8. Managing the amendment of this South Dakota Health Link Policy and System Operation Manual.
5.9. Approving the adoption of Network Utilities;

5.10. Maintaining a process for managing versions of the Performance and Service Specifications, including migration planning;

5.11. 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 activities;

5.12. Entering into agreements to broaden access to data to enhance connectivity across platforms and networks as provided in accordance with Operating Policies and Procedures which shall include an express opt-out right for every Participant; and

5.13. 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.

eHealth Exchange exists to promote the seamless exchange of health information across a variety of technical platforms and Health Information Networks. A core principle of eHealth Exchange is that Participants make commitments to the minimum level of data sharing that they will support so that all other Participants can know, and rely on, each Participant's commitment. All Participants that choose to participate in a specific Use Case must comply with all of the Performance and Service Specifications for a Use Case and must take measures to require that its Participant Users comply with all of the Performance and Service Specifications for a Use Case.

1.1. 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. 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 Technology Partners.** Each Participant shall require that all of its Participant Users and Technology Partners 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 Technology Partners, 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. Provide evidence that the Submitter has obtained an Authorization or other evidence of an individual directed transaction, 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. 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. Business Associate Agreement. Some Use Cases will involve the Transaction of Message Content among Participants, or their Participant Users, that result in a Participant, or Participant User, being considered a Business Associate under the HIPAA Regulations. While this will not be the general rule, when it does occur, the Participants agree that they will enter into a Business Associate Agreement.

3. 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.

4. Breach Notification.

4.1. As soon as reasonably practicable, but no later than five (5) business days after determining that a Breach Event (or "Event") has occurred and is likely to have an adverse impact on the Network or another Participant, Participant shall provide a notification to South Dakota Health Link and all Participants that are likely impacted by the Event. Participant shall supplement the information contained in the notification as it becomes available and cooperate with other Participants. Notwithstanding the foregoing, Participant agrees that (a) within one (1) hour of learning that a Breach Event occurred and that such Event may involve a Federal Participant, it shall alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant, and (b) that within twenty-four (24) hours after determining that a Breach Event has occurred and is likely to have an adverse impact on a Federal Participant(s),

Participant shall provide a notification to all such Participants that are likely impacted by the Event, and South Dakota Health Link, in accordance with the procedures and contacts provided by such Federal Participant. The Notification should include sufficient information for South Dakota Health Link to understand the nature of the Breach Event. 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 any unauthorized access to, use or disclosure of PHI as a result of 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.

4.2. 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.

4.3. 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.

4.3.1. 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)
  - Zero (0) Non-Alpha Numeric Character required (default is 0)
- Password validity may not exceed 180 days
  - Default is 180 days
- Password uniqueness must be a minimum of 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 provider type and location.

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

User Access Levels

Role	Access	Access Additional Records	Restricted to
ED Provider	All Data	No	ED providers only - Doctors, NPs, PAs, CNPs (have NPI, DEA or prescription license) including specialists such as Optometry, Dentist, Chiropractic, EMT/Paramedics, etc.
ED Staff	All Data except Confidential	Yes - Confidential Patients	Licensed Professionals - RNs, LPNs, Pharmacists, PT, OT, Dietitians, etc.
Community Provider	Own Patients except Confidential	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).
Administrative Staff	All Patients except Confidential	No	Receptionists, Admissions, Nurse Assistants, Billing Staff, etc.
Compliance Staff	None	No	HIPAA Compliance Officer, Audit Personnel, etc.
HIM/IT	Own Patients except Confidential	No	IT Staff, HIM Staff
Payer	Own Patients	No	Payer

Data Access

Role	Data	
ED Provider, **ED Staff,** **Community Provider,** **HIM/IT,** **Payer**	Cardiology Catheter GI Immunization Laboratory Medication Orders Other	Pathology Radiology Transcription Medical Transcriptions Ambulatory Medications Community Documents Facesheets Patient Demographics
Administrative Staff	Patient Demographics	
Compliance Staff	Community Documents	

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 username and password to anyone.
2. I will not allow anyone to access the system using my username and password.
3. I will not attempt to learn or use another's username and password.
4. I will not access the System using a username and password other than my own.
5. I am responsible and accountable for all data retrieved and all entries made using my username and password.
6. If I believe the confidentiality of my username 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.