Version: 2.2

Copyright Notice
Copyright © 2017, eHealth Ontario

All rights reserved
No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks
Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
# 1 Table of Contents

## 2 General Information

2.1 Purpose and Scope .............................................................. 4
2.2 Audience ........................................................................... 4
2.3 Related Documents ............................................................. 4

## 3 Service Description

3.1 Overview ........................................................................... 5
3.2 Benefits ............................................................................ 5
  3.2.1 Benefits to You .............................................................. 5
  3.2.2 Benefit to Your Patients ............................................... 5
3.3 Responsibilities ................................................................. 5
  3.3.1 Identity Provider Responsibilities .................................. 5
  3.3.2 Responsibilities of those Who View CDR Data .................. 6

## 4 Privacy and Security Considerations

4.1 Patient Consent ................................................................. 7
  4.1.1 Consent Management ................................................... 7
  4.1.2 Applying Consent Directives ........................................ 7
  4.1.3 Overriding a Consent Directive ..................................... 8
4.2 Access Requests by Patients ............................................... 8
  4.2.1 Access to Data Requests .............................................. 8
  4.2.2 Requests for Audit Logs ............................................... 9
4.3 Correction Requests .......................................................... 9
4.4 Privacy Complaints and Inquiries ....................................... 10
4.5 Retention ........................................................................... 10
4.6 Privacy and Security Training ............................................. 11
4.7 Privacy-Related Questions from Health Care Provider Sites .. 11
4.8 Privacy Breach Management .............................................. 12
4.9 Security Incident and Breach Management ......................... 12
  4.9.1 Instructions for Health Care Providers .......................... 12
  4.9.2 Instructions for Designated Privacy Contact .................. 13

## 5 Summary of Security Safeguards in Place at eHealth Ontario

5.1 Administrative Safeguards .................................................. 14
5.2 Technical Safeguards .......................................................... 14
5.3 Physical Safeguards ............................................................ 14

Glossary .................................................................................. 15
2 General Information

2.1 Purpose and Scope

This guide describes the functions and associated benefits provided by the Clinical Data Repository (CDR) and the related privacy and security considerations, which health care providers and organizations using the CDR must adhere to.

2.2 Audience

This document is intended for health care providers across Ontario's health care sector that may be an organization or a person, who has signed or will sign the appropriate eHealth Ontario access agreement(s) and use the CDR to access the clinical data information related to their patients.

2.3 Related Documents

The Guide should be read in conjunction with the following information found at eHealthOntario.on.ca:

- eHealth Ontario Personal Health Information Privacy Policy
- EHR Access and Correction Policy
- EHR Assurance Policy
- EHR Consent Management Policy
- EHR Inquiries and Complaints Policy
- EHR Logging and Auditing Policy
- EHR Privacy and Security Training Policy
- EHR Privacy Breach Management Policy
- EHR Retention Policy
- eHealth Ontario Federation Identity Provider Policy and Standard
- EHR Security Policies
  - Acceptable Use of Information and Information Technology Policy
  - Access Control and Identity Management Policy for System Level Access
  - Business Continuity Policy
  - Cryptography Policy
  - Electronic Service Provider Policy
  - eHealth Ontario Federation Identity Provider Standard
  - Information Security Incident Management Policy
  - Information and Asset Management Policy
  - Information Security Policy
  - Local Registration Authority Practices Policy
  - Security Logging and Monitoring Policy
  - Network and Operations Policy
  - Physical Security Policy
  - System Development Lifecycle Policy
  - Threat Risk Management Policy
3 Service Description

3.1 Overview

The CDR is an eHealth Ontario data repository that allows authorized health care providers to view clinical information. This clinical information originates from acute-care and primary-care settings that are contributing to the repository. CDR information can include clinical reports such as CCAC reports, discharge summaries, emergency department reports, visits, encounters, as well data within an Electronic Medical Record (EMR). The CDR gives authorized providers important information to make better decisions about treating their patients. With the support of information technology, the CDR identifies, collects and stores priority data from existing databases and registries [i.e. Hospital Information Systems (HISs) and Electronic Medical Records (EMRs)].

3.2 Benefits

3.2.1 Benefits to You

1. Enhanced care and experience
   - Reduce redundancy and frustration
   - Help improve interactions with timely point-of-care access to patient information
   - Improve transition between health care providers
   - A more comprehensive patient record and improved data quality of that record

2. Improved productivity and satisfaction
   - Improve efficiency of decision-making and the ability to monitor health outcomes
   - Provide electronic access to integrated health care information
   - Help improve inter-professional care and coordination of services

3. Improved organizational and system coordination and capacity
   - Accelerate the development and delivery of electronic health records
   - Provide significant cost-savings, enabling an integrated and sustainable approach to better manage, coordinate and plan care
   - Build foundational information technology (IT) elements that can be leveraged for other organizational, regional and provincial health initiatives

3.2.2 Benefit to Your Patients

- Patients receive better, more timely and more coordinated care

3.3 Responsibilities

3.3.1 Identity Provider Responsibilities

Health care organizations who provide the identity management service shall comply with the following obligations:
- Follow the requirements of the eHealth Ontario Identity Provider Policy and Standard
Follow the supporting EHR security policies when providing an identity management service. See Related Documents for a complete listing of policies.

3.3.2 Responsibilities of those Who View CDR Data

Health care providers who view the CDR data must comply with the obligations set out in the EHR Access Services Schedule or EHR Practice Agreement signed with eHealth Ontario by their organization or by themselves and:

- Agree to follow the EHR Security Policies available at http://www.ehealthontario.on.ca/docs
- Review the reference information listed in Related Documents and learn how to protect privacy and security when using eHealth Ontario products
- Use the CDR only for approved clinical purposes
- Always indicate the person or the organization that the user represents when accessing patients’ health information within the CDR
- Obtain the patient’s or the Substitute Decision Maker (SDM) consent prior to requesting temporary reinstatement of consent to access health information restricted by consent directives
- Implement and assist users to follow EHR privacy and security policies, where applicable
4 Privacy and Security Considerations

Quick Tip
The CDR gives patients or their SDM the option to allow or restrict access to patient data within the solution. Restriction of access is known as a ‘consent directive’. Should a patient choose to place a consent directive in CDR, he/she must fill out the EHR Consent Directive form, found at http://www.ehealthontario.on.ca/docs, and send it to eHealth Ontario. Providers may help a patient fill out the form and forward it to eHealth Ontario on the patient’s behalf.

4.1 Patient Consent

4.1.1 Consent Management

The CDR gives patients or their SDM the option to allow or restrict access to their patient data when viewed. If a patient restricts access to his/her data, by applying a ‘consent directive’, providers querying the solution will be unable to access the information to which a consent directive has been applied.

Consent directives can be made, modified or removed to restrict access the following ‘levels’ of patient information in the CDR:

- **Global**: All Health Care Providers (HCPs) would be restricted from accessing any of the patient’s Personal Health Information (PHI) contained in the CDR. Please note that this excludes demographic data available in the Client Registry and the Consent Registry
- **Domain**: Block all providers from accessing patient records in CDR domain
- **HIC-Agents**: Specific HCPs (Dr. Smith) from a specific HIC (i.e. Hospital A) would be restricted from accessing any PHI from that patient in the CDR.
- **Agent**: Specific HCPs (Dr. Smith) would be restricted from accessing any PHI from that patient in the CDR.

4.1.2 Applying Consent Directives

If a patient contacts a Health Information Custodian (HIC) and wishes to either place a restriction on access to his / her information, or wishes to reinstate access (remove the restriction), the HIC should:

1. Capture the consent directive information on the EHR Consent Form at http://www.ehealthontario.on.ca/docs,
   and
2. Submit the consent directive information to eHealth Ontario by faxing it to 416-586-4397 or 1-866-831-0107.

eHealth Ontario will send the HIC a confirmation that the request has been fulfilled. The HIC should then provide notice to the patient that the consent directive has been successfully applied.

In instances where a patient requests to place a consent directive on or reinstate access to records contributed by more than one HIC, the patient should complete the EHR Consent Form at http://www.ehealthontario.on.ca/docs or contact eHealth Ontario directly at 416-946-4767.

In all instances, eHealth Ontario will apply the consent directives within 7 days of verifying the identity of the patient making the request. The health care provider or organization who received the consent directive request from the patient then notifies the patient that his / her request has been fulfilled. If you cannot notify the patient, the HIC will let eHealth Ontario know so that eHealth Ontario can notify him / her on your behalf.
Note that consent directive requests sent to eHealth Ontario on behalf of patients should come from the Designated Privacy Contact at your organization. A Designated Privacy Contact is either the Privacy Officer or someone designated as a delegate according to your agreements with eHealth Ontario.

### 4.1.3 Overriding a Consent Directive

**For Organization’s using the ConnectingOntario Clinical Viewer**

ConnectingOntario permits a health care provider in special cases to temporarily override a patient’s consent directive. Providers can temporarily override a consent directive under the following circumstances:

- With the express consent from the patient or the patient’s SDM
- Believes on reasonable grounds that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the patient to whom the personal health information (PHI) relates and where it is not reasonably possible to obtain the consent of the patient in a timely manner —or;
- Believes, on reasonable grounds, that the override is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons

A temporary consent override will be logged in the ConnectingOntario interface, along with the identity of the overriding health care provider. The override will be in effect for no more than 24-hours for ConnectingOntario. eHealth Ontario will notify the HIC’s privacy office if one of the HIC’s agents overrides a consent directive. Once contacted by eHealth Ontario, it is the responsibility of the HIC’s privacy office to:

1. Investigate the override to ensure it was for one of the reasons stated above, and
2. Notify the patient of the override at the first opportunity.¹

If a consent directive override is applied for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the patient to whom the PHI relates or to a group of persons, the HIC should provide a written notice to the Information and Privacy Commissioner of Ontario (IPC) as soon as possible indicating that this type of override has occurred. For more information on what to include in this notice to the IPC, please see the EHR Consent Management Policy.

For OLIS, a consent directive override may only occur at the express consent of the patient or SDM. Refer to the OLIS Health Care Provider Guide for more details.

**For Organization’s Using the Clinical Connect Clinical Viewer**

An override may not be performed at this time in the Clinical Connect clinical viewer on CDR data.

### 4.2 Access Requests by Patients

#### 4.2.1 Access to Data Requests

Under *Personal Health Information Protection Act* (PHIPA), patients or their SDM have a right to access data held by a HIC about them. When a HCP receives a request for records collected, created and/or contributed by the provider to
the CDR, the provider must follow Part V of PHIPA as well as all any related internal policies, procedures and practices to respond directly to the patient.

In instances where requests for access involves information contributed by another HIC or by multiple HICs, the provider is required to:

- Notify the patient that the request for access involves PHI not within the custody or control of the HIC that received the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

As per the *EHR Access and Correction Policy*, eHealth Ontario may seek assistance from the HIC when responding directly to a request for access by a patient. The HIC should provide eHealth Ontario a contact person at the organization that can assist with this work.

### 4.2.2 Requests for Audit Logs

Audit logs are reports that show details relating to who has viewed your clinical information (i.e. when they viewed this information, from what location, etc.)

When a provider receives a request from a patient to view the audit logs for associated with their records stored in the CDR, the HIC is required to:

- Notify the patient that the HIC is unable to process the request for access, and
- Direct the patient to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

**Note:** Access requests and audit log requests should come from the Designated Privacy Contact at your organization.

### 4.3 Correction Requests

When a HIC receives a request for correction directly from a patient related to health records that were created and contributed to the CDR solely by that HIC, the HIC is required to follow Part V of PHIPA and its internal policies, procedures and practices to respond directly to the patient in respect of the request for correction.

- At the request of the patient, when a correction request is fulfilled, the HIC must notify eHealth Ontario of the correction and request an audit report of who has accessed the patient’s record, in the event that the patient would like to inform other HICs who may have accessed their record. The HIC must then notify relevant sites that have viewed the patient’s record of the correction.

Where a HIC receives a request for correction directly from a patient related to records that were created and contributed to the CDR by another HIC or more than one HIC, the HIC must respond to the patient no later than two days after receiving the request for correction by:

1. Notifying the patient that the request for correction involves PHI not within their custody or control, and
2. Directing the patient to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

eHealth Ontario will coordinate the response to this request, and may seek assistance from the HIC(s) when responding to the patient. The HIC should provide eHealth Ontario a contact person at the organization that can assist with this work.

**Note:** Correction requests should come from the Designated Privacy Contact at your organization.
4.4 Privacy Complaints and Inquiries

Quick Tip
When a person submits an inquiry or complaint related to the CDR, direct him / her to contact eHealth Ontario with their inquiry or complaint.

When a HIC directly receives an inquiry/complaint related solely to that HIC’s records in the CDR, or related to the HIC and its agents and service providers, the HIC is required to follow its own internal policies, procedures, and practices to address the inquiry.

When a HIC directly receives an inquiry/complaint related solely to the CDR or to eHealth Ontario’s agents or electronic service providers that it is unable to address, the HIC must:

1. Notify the person that the HIC is unable to respond to the inquiry/complaint, and
2. Direct the patient to contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

eHealth Ontario may seek assistance from the HIC(s) when responding directly to inquiries or complaints received by eHealth Ontario.

4.5 Retention

Quick Tip
HICs must retain records containing PHI for specified periods of time. Any information collected to respond to access and correction requests, inquiries, complaints, and information pertaining to consent directives must be retained for two years after the request was made.

PHIPA requires HICs to ensure that its records are retained for a specified period, and transferred and disposed of in a secure manner. HICs must ensure records are protected and disposed of in accordance with the Information Security Policy.

HICs will retain records containing the following information for the corresponding retention period:

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit logs and audit reports that contain PHI created and maintained for compliance purposes</td>
<td>The longer of 30 years or when PHI is removed from the EHR.</td>
</tr>
<tr>
<td>Information collected to respond to patients related to their:</td>
<td>Two years after the request was made.</td>
</tr>
<tr>
<td>o Request for Access or Request for Correction under PHIPA;</td>
<td>For complaints, retain for two years after the complaint has been closed by the HIC, eHealth Ontario, or the IPC, whichever is longer.</td>
</tr>
<tr>
<td>o Request to make, modify, or withdraw a Consent Directive under PHIPA; or</td>
<td></td>
</tr>
<tr>
<td>o Inquiries or Complaints under PHIPA.</td>
<td></td>
</tr>
<tr>
<td>Information created about a patient as part of an investigation of Privacy Breaches and/or Security Incidents.</td>
<td>Two years after the Privacy Breach has been closed by the HIC, eHealth Ontario or the Information and Privacy Commissioner of Ontario, whichever is longer.</td>
</tr>
<tr>
<td>Information used for identity provider registration that</td>
<td>Seven years after last use</td>
</tr>
</tbody>
</table>
contains PI

| End User Credential Information where HIC is an Identity Provider | Permanent |
| System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI | For a minimum of two years |
| Authentication Events where HIC is an Identity Provider | 60 days online, 24 months total in archive |
| Templates or resources developed by eHealth Ontario in respect of the EHR; | For a minimum of two years |
| Assurance-related documents | 10 years |

The specific types of PHI that are included in each of the information types can be found in the *EHR Retention Policy*.

### 4.6 Privacy and Security Training

HICs are required to provide privacy and security training to their agents and electronic service providers prior to their access to the CDR. The training should ensure that agents and electronic service providers are aware of their duties under applicable privacy legislative, such as PHIPA, as well as relevant privacy and security policies and procedures in respect of the CDR. Training should be completed:

1. Prior to end users being provisioned an account for accessing the CDR
2. Prior to end users accessing the CDR
3. On an annual basis to all end users

This training is initiated as part of your site's CDR on-boarding process.

HICs are required to track which of their agents, electronic service providers, and any end users have received privacy and security training as part of the onboarding process and annually thereafter.

eHealth Ontario has developed role-based training materials to facilitate this training requirement. For more information on what to include in privacy and security training, please see the *EHR Privacy and Security Training Policy* and the *Privacy Toolkit*.

### 4.7 Privacy-Related Questions from Health Care Provider Sites

If a health care provider has any questions regarding the privacy-related processes described above, including how to respond to patient access requests, consent obligations or incident/breach management processes, contact eHealth Ontario at 1-866-250-1554 or info@ehealthontario.on.ca

Please ensure that you do not include any personal information or personal health information in any emails to eHealth Ontario.
4.8 Privacy Breach Management

**Quick Tip**
A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible.

The EHR Privacy Breach Management Policy describes detailed steps to be taken in the event of an actual or suspected privacy breach/incident.

A HIC shall report an actual or suspected privacy breach to eHealth Ontario by calling the 24/7 service desk at 1-866-250-1554 as soon as possible, but in any event no later than the end of the next business day. According to the EHR Privacy Breach Management Policy, reporting a breach / incident to eHealth Ontario is required when a HIC becomes aware of an actual or suspected privacy breach caused or contributed by:

- Another HIC or the agents or electronic service providers of another HIC,
- More than one HIC or the agents or electronic service providers of more than one HIC,
- eHealth Ontario or its agents or electronic service providers, or
- Any other unauthorized persons who are not agents or electronic service providers of eHealth Ontario or any other HIC.

In instances where a breach is caused by a HIC who solely created and contributed the data to the CDR, the HIC shall follow its internal policies, procedures, and practices to notify the patient(s) to whom the PHI relates at the first reasonable opportunity in accordance with PHIPA and to contain, investigate and remediate the privacy breach.

In instances where a breach was solely caused by a HIC that did not solely create and contribute the PHI to the CDR, the HIC, in consultation with other HICs (who contributed data) and eHealth Ontario, shall identify the individual to investigate the breach. The specific roles for each party involved in the privacy breach are noted in the EHR Privacy Breach Management Policy.

4.9 Security Incident and Breach Management

This section includes instructions for HICs to report to eHealth Ontario any security incidents or breaches (defined below) related to the CDR.

A security incident is an unwanted or unexpected situation that results in:

- Failure to comply with the organization’s security policies, procedures, practices or requirements
- Unauthorized access, use or probing of information resources
- Unauthorized disclosure, destruction, modification or withholding of information
- A contravention of agreements with eHealth Ontario by your organization, users at your organization, or employees, agents or service providers of your organization
- An attempted, suspected or actual security compromise
- Waste, fraud, abuse, theft, loss of or damage to resources.

The security incident and breach management process does not apply to the handling of internal HIC incidents or to any HIC, their agents or their electronic service providers who do not view or contribute PHI to the CDR.

4.9.1 Instructions for Health Care Providers

If you become aware of, or suspect, a security incident or breach of the CDR or data by you or any of your employees, agents, or service providers, you must immediately report the incident or breach to your Designated Privacy Contact. If you are unable to reach your Designated Privacy Contact or support team to report a breach, please contact the eHealth Ontario service desk at 1-866-250-1554 and advise the service desk that you would like to open a security incident ticket.
You are expected to cooperate in any incident or breach containment activities or with any investigation undertaken by eHealth Ontario. During the investigation by eHealth Ontario, you may be required to provide additional information which may include personal health information or personal information, in order to contain or resolve the incident or breach.

**Important:** It is extremely important that you do not disclose any patient personal health information and/or personal information to the service desk when initially reporting a security incident or breach.

### 4.9.2 Instructions for Designated Privacy Contact

Depending on the type and size of your site, you may or may not have a Privacy Office/Officer. If you do not have Privacy Office/Officer, one was designated as a delegate in your agreements with eHealth Ontario.

If you become aware of, or suspect, an incident or breach related to the CDR or data by any of your organization’s staff members, including employees, agents or service providers, you must immediately report the incident or breach to the eHealth Ontario service desk 1-866-250-1554 and advise the service desk that you would like to open a security incident ticket.

**Important:** It is extremely important that you do not disclose any patient personal health information and/or personal information to the service desk when initially reporting a security incident or breach. It is expected that you will cooperate with any investigations conducted by eHealth Ontario in respect of any security incidents or breaches related to data.

When reporting a confirmed or suspected security incident, please have the following information ready:

1. The time and date of the reported incident
2. The name and contact information of the agent or electronic service provider that reported the incident
3. Details about the reported incident, (e.g., type and how it was detected)
4. Any impacts of the reported incident, and
5. Any actions undertaken to contain the incident either by the agent or electronic service provider that reported the incident or the point of contact.

Once a call has been logged with the service desk, the incident response lead or team will be engaged to deal with the situation. A remediation plan will be developed in consult with the requestor.
5 Summary of Security Safeguards in Place at eHealth Ontario

5.1 Administrative Safeguards

- eHealth Ontario has a Chief Privacy Officer and a Chief Information Security Officer; these patients are accountable for health information privacy and security
- The privacy and security committee (made up of the health care organizations participating in the CDR) oversees the privacy and security programs
- Health care organizations must ensure that their health care providers are informed of their duties
- Agreements, policies and procedures define each organization’s role in protecting PI/PHI. They also define the roles of any people working for the organization or service providers who provide the health care organizations with services. Staff members and contractors are required to read the relevant policies and sign an attestation that they have read, understood and are committed to complying with them
- Privacy and security assessments are conducted to identify new risks to privacy and security when the privacy and security committee feels that there is a significant enough change to the CDR or information system
- eHealth Ontario notifies health care organizations of any unauthorized access to PI/PHI that the healthcare organization contributed to the CDR
- CDR staff, consultants, suppliers and users must promptly report any privacy and security breaches for investigation. A security and privacy incident management program is in place to ensure management of incidents and regular training and awareness for staff members involved in incident management

5.2 Technical Safeguards

- Only approved health care providers and staff that support them can view the information in the CDR
- Users are authenticated each time they access the system
- The actions of everyone who views the personal information and personal health information are recorded electronically
- The PI/PHI is always encrypted when it is transmitted to and from participating sites
- Networks are protected by devices (firewalls and routers) that limit access to and from systems
- All actions in the information system are logged so that the privacy officers of the health care organizations are able to monitor and audit their health care providers and staff who view PI/PHI in the information system
- Security agents are installed on each system to protect the CDR from malware and detect intrusions
- Vulnerability assessments of technical configurations and operational security practices are conducted periodically

5.3 Physical Safeguards

- The PI/PHI is stored in a data centre with cameras, restricted access, alarms, and 24/7 security
- When servers are no longer needed, the hard disks storing the PI/PHI are physically destroyed or permanently erased
- Information is not physically removed from the data centre
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCAC</td>
<td>Community Care Access Centre</td>
</tr>
<tr>
<td>CDR</td>
<td>Clinical Data Repository</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>ESP</td>
<td>Electronic Service Provider</td>
</tr>
<tr>
<td>HIAL</td>
<td>Health Integration Access Layer</td>
</tr>
<tr>
<td>HCP</td>
<td>Health Care Providers</td>
</tr>
<tr>
<td>HIC</td>
<td>Health Information Custodian</td>
</tr>
<tr>
<td>HIS</td>
<td>Hospital Information System</td>
</tr>
<tr>
<td>IPC</td>
<td>Information and Privacy Commissioner</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PHIPA</td>
<td><em>Personal Health Information Protection Act, 2004</em></td>
</tr>
<tr>
<td>PI</td>
<td>Personal Information</td>
</tr>
<tr>
<td>SDM</td>
<td>Substitute Decision Maker</td>
</tr>
</tbody>
</table>