IHDE Program Manual

1) Relationship to Terms and Conditions

(a) IHDE Program Manual Incorporation by Reference into Terms and Conditions

This IHDE Program Manual is incorporated by reference into the IHDE Terms and Conditions for Participation Agreement.

(b) Promulgation of and Amendments to Program Manual.

1. Development and Dissemination of Amendments

IHDE is solely responsible for the development of the Program Manual. IHDE may amend, or repeal, or replace the Program Manual at any time. IHDE Management is representative of the Board of Directors, and is charged with developing policies and procedures of the IHDE which may change the Program Manual. IHDE generally will notify all Data Source/Users of any changes to the Program Manual at least thirty (30) days before implementation of the change. However, if the change is required for IHDE and/or Data Source/Users to comply with applicable laws or regulations, IHDE may implement the change within a shorter period of time as appropriate under the circumstances but in any event will notify the Data Source/User of the change at least ten (10) days prior to implementation of the change.

2. Changes to Program Manual

Changes to the Program Manual will automatically be incorporated by reference into each Participation Agreement. The changes will be legally binding upon IHDE and the Data Source/User, as of the effective date of the change. If a change to the Program Manual affects a right or obligation of the Data Source/User under their Participation Agreement, and they object to that change, the Data Source/User may terminate their Participation Agreement as set forth in the Terms and Conditions. The Data Source/User must give IHDE written notice of termination within thirty (30) days following IHDE's notice of the change. The termination of the Data Source/User's Participation Agreement shall be effective as of the effective date of the change to which they object. However, any change to these Terms and Conditions or the Program Manual or to a Participation Agreement that IHDE determines is required to comply with any federal, state, or local law or regulation shall take effect as of the effective date IHDE determines is required. In this case the termination of the Participation Agreement based on the Data Source/User's objection to the change shall be effective as of IHDE's receipt of the Data Source/User's notice of termination.

3. Program Manual Review and Updates

IHDE Management will review and update the IHDE Program Manual at least annually. IHDE will update the Program Manual to comply with changes in the law, including the relevant standards and implementation requirements of HIPAA and the State of Idaho. Changes to this Manual will be distributed to all Security Administrators.

2) Authorized Users

Data Source/Users are responsible for designating the "Authorized Users" within their organizations who will use the IHDE Program. Each Data Source/User must designate at least one Security Administrator (SA). The SA is responsible for identifying users, assigning the appropriate

security level for each user and obtaining organizational approval of proposed users. The IHDE will accept requests for user IDs and passwords only from an organization's designated SA.

(a) Required Information for Authorized Users
Use of, and access to, the Program shall be based on the functional needs and job roles of each Authorized User. Only the minimal access privileges necessary to perform a given job function should be requested by the Data Source/User, or will be granted, by IHDE.

The information required for each user access request includes:

- First Name
- Last Name
- Title
- Password
- Company Name
- Job Category
- Work Group
- Office phone
- Office Fax
- Office address

The following is only applicable to provider user requests.

- Cell phone
- Pager
- NPI (National Provider Identifier)
- Specialty
- Prescription License Number
- DEA Number

(b) Authorized User Types
An Authorized User of the Program will be assigned a **unique** User ID, password and/or other security measure associated with a Clinical Portal License Type and based on the specific user role, and job category. Data Provider/User agrees to abide by IHDE Privacy and Security Safeguards Policies that organization's users will not share usernames or passwords with anyone inside or outside of their organization at any time.

Clinical Portal License Types:

There are two types of licensed users of the Orion Health system:

- *Uni-directional and/or Bi-directional EMR Connection including Clinical Portal Access:* This user type is licensed to receive results delivered through the IHDE to the Data Source/User's EMR, and access the patient-centric Clinical Portal.

- *Clinical Portal View Only Access:* This type of user is licensed to access and use the Clinical Portal.

Job Category:

IHDE-Authorized Users are granted access to the Idaho Health Data Exchange (IHDE) functions based on their job category.

- *Providers, Residents, Nurse Practitioners, Registered Nurses, Physician Assistants, Medical Assistants*: Access and view clinical data and images

- *Staff 1*: Medical support or clinical staff members including registration staff, unit clerks, billing and coding personnel, lab and radiology staff, Insurance/Payer Case and HEDIS Reporting personnel who need to access patient clinical data.

3) Authorized User Account Creation and Management

(a) User Account Policies

These policies govern user account creation and management. These policies represent the minimum set of policies for the creation and management of user accounts. Data Source/Users must incorporate these policies into their existing policies and procedures for granting system access.

1. Each Data Provider/User must assign a Security Administrator (SA). The IHDE will provide training to the SA before any User IDs are granted to Authorized Users of that Data Source/User.

2. The IHDE will accept requests for new User IDs only from the SA.

3. Each user for whom access is requested must complete training as specified in the Terms and Conditions.

4. Each user for whom access is requested must sign an acknowledgement stating that he or she understands the requirements and obligations, under HIPAA and State regulations, governing confidential health information. This acknowledgement must be kept on file by the Data Source/User.

5. Each Data Source/User must have and maintain policies and programs for educating Authorized Users about patient privacy and the confidentiality of patient health information.

6. All requests for User IDs will be evaluated according to the user types, roles and categories defined in section *2.b, (Authorized User Types)* providing the minimum access level necessary for each user to perform their job duties. The SA must verify the identity of the requested user and must ensure the requested access is appropriate and necessary for the user's job roles and duties.

7. Requests for deletions of users or modifications of Authorized User access must be submitted by the SA to the IHDE.

(b) User Account Procedures

1. User access requests approved by the Data Source/User must be submitted to the IHDE by the SA.

2. The SA must submit new user account requests using the format specified by the IHDE.

3. An account request must be submitted for each user. Users in an organization cannot share a single user ID and password. A unique user ID will be established by IHDE for each user.

4. Users are assigned a temporary password upon creation of a new user ID. Upon initial login to the system with the temporary password, the user must change their password, using the Change Password function. User-created passwords must be minimum of eight characters in length including upper and lower-case letters, at least one number (e.g. 1, 2, 3) and a special character (e.g.!, @, #, $, etc. - periods are not accepted).

5. The IHDE will notify the new Authorized User directly, informing them of their login ID. The IHDE will notify the SA the new Authorized User account has been established.

(c) Resetting Passwords

1. Authorized Users can perform routine password changes through the system using the "Change Password" function and as specified in the Security Safeguards policy.

2. Authorized Users must contact their SA to request a password reset. During normal support hours (8 a.m. to 5 p.m. Mountain Time, weekdays) if an SA is unavailable, an Authorized User can contact IHDE for a password reset.

(d) Terminating or Changing User Accounts

1. When an Authorized User's employment is terminated, his/her supervisor must as soon as practical notify the SA and request deactivation of the employee's IHDE account.

2. When an Authorized User's job duties change and this would impact IHDE access, his/her supervisor must notify the SA as soon as practical and request modification of the user's access.

3. The SA shall immediately contact the IHDE and request deletion or modification of the user account as appropriate.

4. The SA and IHDEmust maintain permanent documentation of this action.

4) Privacy & Patient Consent

(a) Privacy

The IHDE Security and Privacy Policies are issued to each Data Source/User as part of the Participation Agreement. Each SA must read and comply with the Security and Privacy Policies. Each Data Source/User must comply with the Privacy PoliciesPolicies.

(b) Audits and Reports
It is the responsibility of the IHDE Authorized User access only the minimum necessary information required for the treatment and healthcare operations related to patients of record, and to comply with the IHDE Privacy Policies. The IHDE Program has sophisticated access logging facilities that monitor and record each request for a specific patient's health information, capturing data relating to time, date, location and name of each user and the data accessed. These access logs form the basis for auditing compliance with health privacy regulations and the IHDE Security and Privacy policies.

In the event of a suspected breach, the IHDE will provide audit services and reporting to the Data Source/User, at their request, for the purpose of analyzing access to specific patient health data.

If an audit report results in a concern of inappropriate usage of the Program, the following procedure will be followed:

- A one page summary of the potential inappropriate use will be submitted, with a copy of the Audit Report, to the IHDE Executive Director.
- The IHDE Executive Director will contact the Authorized User identified as having inappropriately accessed the Program to request clarification regarding the use in question.
- Subsequent to those findings, a notice will be provided to the requesting party detailing the findings and resultant actions taken or to be taken.
- Any Authorized User found engaging in inappropriate use will have their user ID revoked.
- The Data Source/User will fully investigate and prosecute the incident according to their organization's rules, as well as according to HIPAA and the laws of Idaho.

5) Use of Data

(a) Permitted Uses of Data
The IHDE Terms and Conditions permit specific uses of data for Authorized Users under *Section 2, Authorized Users*. IHDE data may only be used for treatment, payment and healthcare operations which promote efficiency of communication in care, patient safety and enhanced patient health.

(b) Non-Permitted Uses of Data
Each Data Source/User must have and maintain specific policies and procedures for identifying and responding to suspected or known security incidents. Each Data Source/User must have and maintain specific policies and procedures for mitigating, to the extent practicable, harmful effects of such security incidents. The Data Source/User must retain documentation relating to the security incident, and their subsequent actions, for a minimum of seven (7) years.

Use of the IHDE system or services is prohibited for any purpose other than as specified in *5a, Permitted Uses of Data* including:

No Services to Third Parties: The Data Source/User will access their registered Program only for their own account, on behalf of the User and its Affiliated Entities. The Data Source/User must not use any part of the Program to provide separate services or sublicenses to any third party, other than its Affiliated Entities. See *Section 5c, Affiliated Entities* for a list of affiliated entities.

No Services Prohibited by Local Laws: The Data Source/User will not employ the Program for any purpose or in any manner prohibited by Federal laws or the laws of the State of Idaho.

No Use for Comparative Studies: The Data Source/User will not employ the Program to aggregate data to compare the performance of other Data Source/Users and/or Authorized Users, without the express written consent of the IHDE Board, and each of the Data Source/Users and Authorized Users being compared. This is specifically defined to forbid use of the Program for credentialing or de-credentialing providers.

No Use for Underwriting: Authorized Users shall not use the Program for the purpose of underwriting.

No Use for Marketing: Authorized Users shall not use the Program for marketing purposes, as defined by HIPAA (45 CFR 164.501).

(c) Affiliated Entities

The following is a list of the approved Affiliated Entities that may have access to IHDE systems and services as part of an Authorized User account access. Modifications will not be made to this list without express written consent of the IHDE Board.

- Pharmacy Benefit Managers (PBMs)
- National Account Partners
- Contracted Business Associates
- Legal, audit, third party billing, RHIT consultants, clinical consultants, etc.

6) Provision of Data

Data is provided to IHDE by community Data Sources to create a patient-centric view of clinical results. Data Sources make available a subset of their clinical information which they feel appropriate to provide to other healthcare providers.

Data is pushed to a connected Data Source's respective EMR, updating the Enterprise Master Patient Index EMPI and will be sent as a message to update a patient's health record.

Data Sources must establish a secure Virtual Private Network (VPN) connection as detailed by the IHDE and Orion Health implementation team. Data provided to IHDE from community Data Sources may consist of demographic data to build the community EMPI, including ADT information, lab results, radiology and transcription reports.

(a) Master Patient Index (EMPI)

The EMPI is the directory of the patients in the State of Idaho medical service area. Each record contains the patient's demographic data and can be used to identify matching clinical information for that patient in each participant's EMR system. The accuracy of the patient index is largely dependent on the data provided to it. Specific health care institutions in Idaho provide data to build the IDHE EMPI.

(b) Required data for physician directories to support clinical messaging

In order to route clinical reports and results correctly via the IHDE clinical messaging backbone, Data Sources will also provide Local Identifier as specified by the IHDE and Orion Health implementation team, in a mutually acceptable format.

(c) Required data for lab results

In order to provide trended lab results across institutions, providers of lab data will work with Orion Health and IHDE to map their lab results into standardized Logical Observation Identifiers Names and Codes (LOINC) encoded results. These national lab data standards will allow clinicians to better interpret trended results from institutions that may have different ranges and coding schemes.

(d) Required data for radiology reports

In order to provide radiology results and reports through the clinical message routing, Data Sources will work with Orion Health and IHDE to map the data elements necessary to provide Observation Result Unit (ORU) for structured patient-oriented clinical data. This will allow for the exchange of radiology reports and images between the radiology facility and the healthcare provider via the IHDE.

(e) Required data for medication history
At this time, medication history may only be provided by textual reports.

(f) Required data for Admission, Discharge, Transfer (ADT) results
Admission, Discharge, and Transfer (ADT) results from Hospital Systems providing Master Patient Index (EMPI) feeds will be utilized to keep the EMPI updated with the most current patient information.

7) Data Monitoring & Management

Each Data Source will use reasonable and appropriate efforts to assure that all data it provides to the IHDE is accurate, reasonably complete, and provided in a timely manner. Even with the best efforts of Data Sources, data entry personnel and software systems, there will be requirements to monitor, manage and correct the exchange of information as it moves from Data Sources to the IHDE.

(a) Monitoring & Management of the Enterprise Master Patient Index (EMPI)
The EMPI is populated by Admissions-Discharge-Transfers (ADT) feeds from IHDE participants who can provide this data. If patient records are merged in the source systems, the ADT feed should be set up to send that merger information to the IHDE. In either event, a minimum amount of data is required to add a new EMPI record:

1. Adding a New Record
A Minimum Data Set (MDS) of information is required before new patient records can be added to the EMPI. This MDS consists of:

UNIQUE Patient's Medical Record Number (MRN)
Patient Last Name
Patient First Name
Patient Gender
Patient Date of Birth

For manual addition of new patient index records, the user will be presented with a list of preexisting entries in the EMPI to help assist in reducing the creation of duplicate entries.

2. Building Incrementally

- Clinical Result transactions processed through IHDE will be added to the patient's community-wide record.
- New or revised patient data keyed by staff directly into patient index records will update the EMPI.

All IHDE components or interfaces, designed to add patient records automatically to the patient index, use algorithms to prevent duplicate entries from being created. Manual additions by users also follow an algorithm designed to minimize duplicates.

When multiple automated and manual sources are capable of changing existing patient information, an additional level of data management is required. For this reason, the algorithms that enable changes to a patient's record are configured depending on the Data Source/User. The audit trail function in Orion Health tracks the user making the changes, the date and time of the change, and the information being changed.

3. Merging EMPI entries

In order to display health record for a single patient across multiple data sources, it is critical that each clinical record be accurately related to a single patient index record.
Patients are identified and distinguished in the IHDE by the demographic data elements entered by the Data Sources. At times the patient-identifying data submitted to the IHDE is insufficient to distinctly and uniquely identify patients, and duplicate entries in the EMPI may be created. The IHDE addresses this problem with the administrative function of merging patient records. Merging creates associations among multiple patient records that actually represent the same individual.

Programs that process and load patient demographic data into the EMPI use rules to compare incoming patient data to patient data that already resides in the EMPI. These program rules attempt to determine whether an incoming patient record matches an existing entry in the EMPI. If a match can be established with sufficient confidence, the system creates an association (or link) of the incoming record to the existing entry. If the system cannot establish with sufficient confidence that the incoming patient record matches an existing EMPI entry, the incoming patient record is loaded into the EMPI as a new and unique EMPI patient entry.

4. System Level EMPI Clean Up

In addition to checking EMPI information as data is loaded, the EMPI tool also includes a utility to periodically check and correct EMPI information. This program will be run on a regular basis to assist in keeping EMPI information as clean as possible

5. User-Generated Requests for Merges

Users accessing the Clinical Portal for patient demographic information may discover multiple entries for what may be the same patient. Errors of this nature may occur for a variety of reasons, but typically happen because insufficient information was available to the EMPI for display in the Clinical Portal.

In response to such situations, users shall submit a request to IHDE to investigate and consider a merge of these records. IHDE will usually be able to confirm with the Data User

patient-specific demographic and treatment details, to facilitate accurate merging of the records using the EMPI Editor. If there are two or more patient demographic records in the Clinical Portal that the Data User suspects are one patient, but the Clinical Portal displays as different patients, then the user can request a merge (link) of these records.

(b) Managing & Monitoring Lab Results

Organizations providing lab results to the IHDE will consult with appropriate IHDE and Orion Health staff, and configure the appropriate method of data transfer to the IHDE. Before connecting live lab feeds to the IHDE, the Data Source will review the accuracy of the data as submitted and transmitted to a test environment. Once test results have been approved, and lab feeds have been moved into a production environment, the IHDE and Orion Health staff will monitor the work queues for any undeliverable results and seek to correct or route the results. The Data Source will appoint an internal resource within their organization to assist the IHDE staff or Orion Health staff in resolving data quality or data routing issues.

(c) Managing & Monitoring Radiology Reports

Organizations providing radiology results to the IHDE will consult with appropriate IHDE and Orion Health staff, and configure the appropriate method of data transfer to the IHDE. Technical Orion Health staff will work with radiology vendors to assist in defining and implementing the appropriate data transfer approach to the IHDE. Before connecting live radiology report feeds to the IHDE, the Data Source will review the accuracy of the data as submitted and transmitted to a test environment. Once report results have been approved, and radiology feeds have been moved into a production environment, the IHDE staff will monitor the work queues for any undeliverable results and seek to correct or route the results. The data providing organization will appoint a resource to assist the IHDE or Orion Health staff in resolving data quality or data routing issues.

(d) Managing & Monitoring Medication History

At this time, medication history may only be provided by textual reports.

(e) Managing & Monitoring Admission, Discharge, Transfer (ADT) Results

Hospitals providing ADT (Admission, Discharge, Transfer) feeds to the IHDE will consult with appropriate IHDE and Orion Health staff, and configure the appropriate method of data transfer to the IHDE. Before connecting live ADT feeds to the IHDE, the data providing organization will review the accuracy of the data as submitted and transmitted to a test environment. Once test results have been approved, and ADT feeds have been moved into a production environment, the IHDE staff will monitor the work queues for any undeliverable results and seek to correct or route the results. The data providing organization will appoint an internal resource within their organization to assist the IHDE or Orion Health staff in resolving data quality issues.

(f) Use and return of data in the event of termination

Institutional Data Sources, such as hospitals, labs, radiology practices and health insurance companies who have provided data to the IHDE and subsequently elect to terminate their relationship with the IHDE may request to have their data remove and destroyed from IHDE systems and repositories. The institutional medical record numbers or policy member numbers provided by the Data Source may be removed from the IHDE's Master Patient Index. The names of

non-participating physicians provided to the IHDE as part of the Data Source's physician address book may be deleted from the IHDE physician address book.

Messages and reports that have been messaged or routed throughout the exchange and may be resident in practice specific EMR systems, or in a printed form as part of a medical chart will not be returned.

8) System and Services

(a) Schedule of Associated Software and Hardware
IHDE has purchased software and system components from the Orion Health to support its IHDE offerings. IHDE also contracts with Orion Health to establish and maintain the IHDE Program. The software developed is built on the Orion Health platform. Data Source/Users may elect to use one of several software applications or services as detailed in the each Participation Agreement. Software purchased by IHDE and provided to support the Health Information Exchange is detailed below:

(b) Description of Associated Software Services

1. The Clinical Portal is a web-based, viewable collection of patient historical community-wide medical transactions (lab results, radiology and transcriptions reports). Authorized users can search for their patient via the Clinical Portal.

3. Results Delivery is the service for enrolled participants with either a uni-directional or bi-directional interface that facilitates the routing of results (e.g. labs, radiology and transcriptions reports) including the attending, ordering, referring and copy-to physicians listed on the respective result(s).

(c) Technology License Terms

Software is provided according to the license terms as included in the Participation Agreement.

(d) Data Source/User's Required Hardware and Software

1. Clinical Portal Access
Any computer with a web browser and internet access can access the Clinical Portal. The Clinical Portal application supports desktop personal computers (pc's), laptops, MAC, and select tablets and smart phones, and will configure its display based on the device accessing the system.

2. Connectivity:
Internet Connection: A high speed internet connection such as a cable modem, DSL line or T1 is recommended.

Internet Connection Minimum Requirements *

- ✓ Terrestrial persistent connection (i.e. always on and not via satellite)
- ✓ Upload speed of 256 Kbits per second
- ✓ Minimum download speed of 5 Mbit per second

Dedicated Personal Computer Minimum Requirements

- ✓ Minimum 2 GHz Pentium class processor
- ✓ Minimum 1 GB of RAM
- ✓ Minimum 50 GB hard disk drive
- ✓ 256 color screen with resolution of 1024 x 768 pixels
- ✓ Windows operating system 7, 8, 8.1, 10; or MAC OS X
- ✓ Internet Explorer versions 8 -11 (note: pop-ups may be required for other Orion Health features and must not be blocked)
- ✓ Windows or MAC-supported printer (color ink/toner is highly recommended)

Additional Browsers Supported by Orion Health

3rd Party browsers including Mozilla Firefox, Apple Safari and Google Chrome are supported by Orion Health. Mobile support on Android and iPad IOS is supported. IPhone is not currently supported.

(e) Hosting & Administration Services

IHDE contracts with Orion Health for Hosting and Maintenance of the Program. Their roles and responsibilities are detailed below:

1. **Provision and Access:** IHDE's vendor (Orion Health) will provide sufficiently powerful server hardware and software to process data transactions in a timely manner.

2. **Response Time:** IHDE's vendor (Orion Health) will ensure that for each non-holiday, non-weekend daily period between 8:00 am and 5:00 pm Mountain Standard Time (MST), the average transaction response time, defined as the time elapsed from the receipt of an online user request by the IHDE to the provision of a response to such user, will not exceed three (3) seconds.

3. **Service Availability:** With the exception of scheduled hardware, software or communications maintenance, IHDE will ensure the IHDE is available 97% uptime. For each calendar year, scheduled hardware, software and communications maintenance will not exceed an average of 8 hours in total per month under normal conditions. Normal conditions do not include emergency server or disaster recovery circumstances.

4. **Disaster Recovery:** Orion Health will maintain a secondary server with appropriate connectivity and disk access to permit recovery within 24 hours in the event of failure of the primary server. This secondary server will be maintained at a secure data center. IHDE will also maintain service contracts with appropriate hardware vendors for next day (or sooner) parts replacements. IHDE will maintain a recovery plan with the vendor (Orion Health) describing actions to be taken to restore service in the event of a disaster.

5. **Administration Services:** IHDE's vendor (Orion Health) will (i) perform nightly backups of the key databases; (ii) perform administrative services necessary for running and maintaining the server and IHDE; (iii) perform administrative services for troubleshooting routing issues and resending data as needed; (iv) monitor the systems so as to detect problem transactions in a timely manner and inform the client of any data structure or format problems that need addressing.

6. **Security and Privacy:** IHDE will maintain and follow policies and procedures that comply with generally accepted privacy and security policies and procedures and any and all applicable laws, rules, and regulations, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended and the regulations promulgated thereunder.

(f) Training

IHDE will provide training for system users:

1. **New User Training:** IHDE will provide training to familiarize each Authorized User with both the operation of the chosen software system and the privacy policies and conditions governing the use of the Clinical Portal. If several training options are made available by IHDE, Data Source/Users will have the option of selecting the training mechanism that works best for their organization.

2. **Security Administrator (SA):** Each Data User will have at least one user in the Security Administrator (SA) role. This individual will receive training specific to this role.

(g) Support

1. **On Line Information Regarding How to Use the Clinical Portal:** For online help when you are logged into the Clinical Portal, click on the Help link on your screen. This link is available from all screens in the Clinical Portal. This on-line help information will give you step-by-step information about how to use virtually all of the functions in the Clinical Portal. Using this feature in the Clinical Portal may answer your questions without the need to contact Technical Support.

2. **Technical Support:** IHDE Technical Support is available to all Authorized Users. Authorized users can request support, ask questions, or give feedback any time. All questions, problems, or issues should be communicated by:

Telephone: 208-332-7253
E-Mail: support@Idahohde.org

3. **Technical Support Policies**

- IHDE Support personnel will be available during normal operating hours, 8am to 5pm Mountain Standard Time (MST), Monday through Friday.

- Users can contact the IHDE by phone or via email directly from the IHDE Clinical Portal and/or the IHDE website.

- All problems escalated to the technology vendor (Orion Health) will be acknowledged and responded to as per vendor's customer service policy. User problems may only be escalated to the technology vendor by the IHDE Support personnel.

- The technology vendor will have and maintain procedures for staffing its own help desk, escalating problems internally, and maintaining contact information. The procedures

must be reviewed at least annually.

- A record of all support requests through the IHDE system, and support tickets with the vendor, will reflect all actions taken and will be permanently maintained by the IHDE Support personnel.

- Critical requests (severe impairment of vital functions of the IHDE supplied application such that users cannot access or use the application) for support will be responded to within one (1) hour during IHDE business hours, or if messages are received after business hours, the IHDE Support personnel response will be immediate.

- Non-critical requests for support will be responded to within the next business day.

- **DO NOT INCLUDE PATIENT HEALTH INFORMATION WHEN SENDING AN E-MAIL TO TECHNICAL SUPPORT. HIPAA DOES NOT PERMIT THE USE OF NON-SECURE COMMUNICATION USING E-MAIL SYSTEMS TO TRANSMIT PATIENT INFORMATION.**

9) Fees and Charges

(a) Fee Schedule
Program fees and charges for supplied software and services are detailed in the IHDE Participant Services and Pricing. The IHDE Participant Services and Pricing? will be provided to each Data Source/User with the Participation Agreement.

(b) Terms for Suspension and Resumption of Services

1. Suspension of Services: Data Source/Users may have their rights to access the IHDE suspended for the following reasons in addition to those identified in Section 12.7 (Suspension of Service) of the Terms and Conditions:

- Non-payment of fees and/or charges associated with use of the system.
- Non-payment of contracted service fees (services contracted directly between the Data Source/User and the IHDE).
- Non-payment of other applicable fees associated with products or services provided by the IHDE to the Data Source/User.

Suspension of services will remain in effect until all applicable fees and/or charges are paid in full, bringing the Data Source/User's account to a current status.

2. Reconnection fee: A reconnection fee will be assessed for all Data Source/Users who have been suspended and wish to have their access to IHDE reestablished. The reconnection fee will be the greater of 2.5% of the outstanding balance or a minimum of $50.

3. Resumption of Services: The IHDE will reconnect the Data Source/User's access to the system within one (1) business day of receipt of payment as described in section 1 and 2 above. Payments will be in the form of cash, check, cashiers check or money order made payable to Idaho Health Data Exchange, Inc.

10) Remedy for Failure to Achieve Service Availability

Should IHDE fail to achieve the Service Availability specified in 8(e)(3) Hosting & Administration Services for a month, IHDE will work with the Vendor to make necessary adjustments to infrastructure, configuration, platform, and other components so as to ensure the Service Availability commitments are achieved in subsequent months. Should IHDE fail to achieve the Service Availability commitments for two consecutive months, Data User/Provider shall become eligible to receive a rebate for each month the Service Availability commitments were achieved. The rebate for each such month shall not exceed 25% of the pro-rata fee for that month and will accrue at the rate of 5% of the fee for every 1% that the percent of availability is below the Service Availability commitment.

APPENDICES
IHDE Privacy and Security Safeguard Policies