Chesapeake Regional Information System for Our Patients (CRISP)

Policies and Procedures

Version: 9
Date: June 27, 2019

Contents

Background

These Policies and Procedures contain specific terms and conditions of operation and use of the CRISP Services, specific technical specifications information, and other terms or requirements relating to the CRISP Services as are specified in the Terms and Conditions of the Chesapeake Regional Information System for Our Patients (CRISP) Participation Agreement and are consistent with, or that supplement or implement the provisions of, the Terms and Conditions. In the event of a conflict between a provision of the Terms and Conditions and a provision of these Policies and Procedures, the provision of these Terms and Conditions will govern. The Policies and Procedures may be amended from time-to-time in accordance with Section of the Participation Agreement in the Terms and Conditions. These Policies and Procedures apply to participants using CRISP Maryland or CRISP DC services. Where necessary, differences in provisions or applications to CRISP Maryland or CRISP DC participants is outlined within. Participant acknowledges that Participant is responsible for reviewing the Policies and Procedures on CRISP Website and for monitoring the CRISP Website on a regular basis for, among other things, amendments to the Policies and Procedures or notices relating to such amendments made in accordance within the Section of the Participation Agreement.

1. Participant Users

1.1 Definition

Participant users include health care providers, employees, staff, and other workforce members of the participant organization who have been designated by the participant as needing access to the CRISP Services to perform their job function. Access to CRISP notification and reporting services is dependent on the role and position required to obtain access.

Participant users may have CRISP services access rights at multiple participant locations or organizations based on their employment. If a participant user chooses to access the CRISP services via the web-based portal application made available through CRISP, a single user name and password will be assigned to that user for each participating organization

1.2 Participant User Requirements

Participants must have enforceable agreements with each of their participant users; see Appendix A for example text. Agreements may take the form of written policies and procedures of the participant, as long as such policies and procedures constitute an enforceable agreement with users. Participants must require that all of their participant users comply with applicable laws; clauses in the Participation Agreement directly applicable to participant users; and the CRISP Policies and Procedures. If a participant user is in violation of any of these agreements, participant should immediately notify CRISP, and CRISP may suspend or terminate the user as necessary.

1.3 Change in Participant User's Job Status or Role

Participants are responsible for promptly informing CRISP when the job status or role of a participant user within their organization has changed and affects their access rights to the CRISP Services, or for changing the role of a participant user if access is obtained through a third-party electronic health record (EHR). If a participant user is being terminated from an organization, the organization must inform CRISP of this termination in a timely manner, and prior to actual termination if at all possible. CRISP will terminate the user's account immediately upon termination of employment. Participants accessing the CRISP Services through third party EHRs will be responsible for terminating access through this EHR for terminated employee at the time of termination.

1.4 Training

CRISP will make training available through their website, in addition to other training materials as appropriate. Participants will be responsible for training individual users on both data consumption and CRISP policies, including the creation and dissemination of any necessary training above and beyond that provided by CRISP (*See Maintenance*). If additional training is necessary as a result of system updates, CRISP will inform participating organizations of the changes, and each organization will then be responsible for passing the information along to end users.

2. User Name and Passwords

The CRISP services will utilize security-industry best practices for authenticating user access to the Query Portal. CRISP and Participants must ensure that each Participant User is assigned a at-least a unique username and password to access services but where possible multi-factor authentication will be utilized

2.1 Password Convention

Passwords must be at least eight (8) characters in length, including at least one number, one uppercase letter, and one lowercase letter. User passwords will expire every 90 days, requiring that each user selects a new password at that time. Password history settings will be enforced to ensure that a user does not duplicate a previous password used previously.

2.2 Lock Outs and Password Resets

Users will be able to reset their own password using answers to the challenge questions set during initial login for the Unified Landing Page. After five (5) consecutive failed log-in attempts, a user will be locked out of the system. In order to get his/her account unlocked, a user must call the CRISP support desk directly at 1-877-952-7477. Users whose accounts do not have any activity for a duration of ninety (90) days or longer will be automatically locked out of their account and must call CRISP to get their account unlocked. All users not using single sign on must be verified every 90 days by the participant point of contact.

3. User Access Policies

All participants are required to develop, or have in place, written requirements that govern participant's and participant users' access to information systems and use of protected health information. Such policies should be consistent with the permitted purposes in the Terms and Conditions and Policies and Procedures and should be made available to CRISP upon request. Participants must appoint an authorized individual to implement and ensure compliance with all policies related to CRISP participant users. The authorized individual will be responsible for implementing a policy that appropriately grants access to clinical data on behalf of the participant, as a covered entity, and its clinicians. This individual may also act as the designated point of contact for CRISP correspondence and user verification and updates as described in Section 8.

3.1 Minimum Necessary

Participants should only use and or disclose the minimum amount of information necessary for the purpose of such use. Participant users should only have access to the minimum amount of information required to perform their job function. Minimum necessary does not apply to use of data for treatment or other purposes required by law.

3.2 Data Misuse

Health information available through CRISP is to be accessed, viewed, and used only by CRISP participants and providers who have been authorized to do so, and only for permitted purposes. Any misuse of health information in connection with CRISP is to be reported to CRISP as soon as discovered. Health information misuse will be investigated and verified. CRISP will notify privacy and security officers of all impacted parties at the conclusion of such investigations, if it is determined that a misuse of health information has occurred. If appropriate, CRISP will also take actions necessary to remedy the misuse of data. These actions may include but are not limited to suspension and or termination of a participant or participant users.

3.3 Participant Procedures for Non-Compliance

Each Participant should implement procedures to issue appropriate consequences hold Participant Users responsible for misuse of data obtained through the CRISP Services. Applicable procedures in place for use of other health information systems may be leveraged for misuse of data.

4. Patient Access and Rights

4.1 Accounting of Disclosure Requests

Patients can request an accounting of disclosure of participating user access of the patient's medical records twice per year free of charge. CRISP requires the patient request to include first name, last name, date of birth, address, and a copy of a government-issued photo ID.

4.2 Opting Out of CRISP Services

The default patient consent policy is opt-out. This means that a patient must proactively, and explicitly, declare their desire to opt out of the exchange. Opting out means that a patient's health information can no longer be returned as the result of a query or sent as an encounter notification. Opting out does not cover point-to-point secure messaging (results and referrals). For example, if a primary care physician orders a lab from a national lab, the result for that order will still be electronically delivered to the ordering provider. The result will not be available to other physicians who query the exchange. It also does not apply to any state-mandated program that CRISP facilitates through our technology, such as the Prescription Drug Monitoring Program or public health reportable conditions.

The opting out of patients will be handled centrally by CRISP and will not occur at the participant level. It is the participant's responsibility, however, to adequately educate patients on the opt-out process and to ensure that Notice of Privacy Practices are updated accordingly. Patients can opt out by completing a paper form and mailing or faxing it to CRISP, calling a toll-free number (1-877-95-CRISP), or via online form submission. There may be a period of up to five (5) business days before the opt-out is recorded in the system, meaning that patient data may be available for query during this interim time after the opt-out has been submitted. Patients are allowed to opt back into the exchange at any time, but patient data may have been deleted during the time the opt-out was in effect.

4.3 Personal Health Records

CRISP is working to provide health information to patients' personal health records (PHRs) in the future but does not currently offer this capability. The CRISP architecture is standards-based and any future connection to PHRs will have a preference for infrastructure based on national standards. Any data that is delivered to a participant under an approved use case and/or permitted purpose that becomes a part of the patient's medical record may be shared through the participant's personal health record, should the

participant choose to do so. CRISP Policies and Procedures related to patients' personal health records may be updated or amended as industry standards change or regulatory requirements necessitate.

5. Permitted Purposes

Participants and participant users may access and use data through the CRISP for only for permitted purposes, as defined in the Terms and Conditions. Permitted purposes for data use are listed below:

1. For treatment of an individual
2. For a public purpose (see Participation Agreement for definition)
3. For quality assessment and improvement activities, including care coordination, defined in HIPAA as a subset of health care operations activities, when such uses are approved by the CRISP Clinical Advisory Board, and subject to the limitations stated in Section 3.02 b (i) of the Terms and Conditions (see Appendix B for a list of approved quality improvement and care coordination uses).
4. For research (approved 2016). Use cases are developed and recommended by the Research Subcommittee for approval by the CRISP Clinical Advisory Board. The Research Subcommittee then will review specific data requests of CRISP participants and evaluate their fit for approved use cases. Currently, only IRB-approved, patient-consented research is permitted, but this could alter based upon recommendations of the Research Subcommittee and decisions of the Clinical Advisory Board.

Approved uses under Permitted Purpose number three (3) or four (4) may be modified or added with the approval of the CRISP Clinical Advisory Board, and such modifications or additions will be treated as non-material amendments to the Policies and Procedures and posted on the CRISP website.

With the approval of the Clinical Advisory Board, specific use cases under Permitted Purpose number three (3) or four (4) may be extended to other entities, upon a finding that such an extension is in furtherance of the mission of CRISP, that entry into a full Participation Agreement is not possible or practical, and that the entity will be required to enter into a written agreement with CRISP that protects the interests of CRISP and its participants in the integrity of the CRISP Services and the appropriate use of the information to be provided to the entity.

CRISP reserves the right to add additional permitted purposes through an amendment to this Policies and Procedures document and will post on the CRISP website.

6. Participating Data Providers

Participants must complete testing prior to going live with connectivity to CRISP. In addition to initial testing, participants are responsible for validating data on a test platform provided by CRISP when changes or upgrades to their source systems are made. Participants should notify CRISP of any changes prior to system changes or upgrades being made. Data validation should be completed by comparing the data in CRISP's system to that in the participant's source system. The following should be taken into account while validating data:

- Values should be identical to those in the data provider source system
- Any supporting data, such as units, should be the same as in the source system
- Formatting should be similar to the source system

While it will not be necessary for participants to validate every data item in the system, it will be necessary to look at a large sample of data. In order to adequately validate the data, it will also be necessary to look at each type of report that is being sent from the source system. CRISP will provide

guidance on testing, but it is the Participant's responsibility to execute a complete test plan in accordance with their own testing policies and procedures. Following successful completion of participant testing, participants must complete and sign-off on a CRISP go-live checklist prior to going live with connectivity to CRISP.

6.1 Data Contributors

Data providers will make data available to the CRISP Services consistent with the services offered by CRISP. For example, CRISP is initially focused on receiving Admit Discharge Transfer (ADT), laboratory reports, radiology reports, and a subset of electronic documents including discharge summaries, consultations, history & physicals, operative notes, as well as other data types that may be deemed appropriate in the future. For each data provider, information made available to the CRISP Services will be subject to appropriateness and technical readiness. For a data provider to be connected to and remain connected to the CRISP Services, they must submit at least one defined data type. Contribution of data must occur over a secure connection configured by CRISP and the participant.

6.2 Sensitive Health Information

Data contributors of participating organizations must refrain from sending certain sensitive health information - substance use disorder treatment and self-pay information that may be restricted from disclosure by local, state, district, and federal law. Participants are responsible for complying with applicable laws and for filtering any information that should not be disclosed to the CRISP Services.

7. Data Retention and Reuse

CRISP will retain disclosure data for a minimum period of seven (7) years, as required by law, in order to maintain an auditable history of each transaction through the CRISP Services.

CRISP may allow access or otherwise release data from the CRISP Services for public health reporting or in other civil, criminal, or crisis-related matters where compelled to provide that data by a lawful order. Each request for data from outside participants will be independently vetted to ensure the request is legal and appropriate. CRISP will not release any personal health information to anyone for commercial, private, or other reasons that are not related treatment, payment, or health care operations.

7.1 Data Consumption

A participating organization can contribute and or consume data either via the CRISP Services or through a third party EHR. The hardware and software requirements for the CRISP Services depend on the means an organization is using to contribute/consume data.

7.2 Return of Data

If a participant wishes to terminate access to the CRISP Services, CRISP will disable that participant's data feeds and terminate the participant's ability to access the CRISP Services. All data that has been incorporated into a provider's EHR system prior to participant termination will continue to be the property of that provider. Additionally, a party CRISP or participant may retain one copy of the other's confidential information as defined in the Participation Agreement to the extent reasonably necessary to document matters relating to the Participation Agreement for legal or insurance reasons or for similar purposes, provided that the restrictions on Confidential Information in the Participation Agreement section continue to apply to the retained copy.

8. Systems Operations

8.1 Hardware and Software

CRISP services are made up of a combination of commercial off the shelf applications (COTS) and custom developed applications. The CRISP Services are hosted across data centers in Owings Mills, MD, Denver, CO, and cloud environments. CRISP makes data available through five core service areas:

- Point of Care: Clinical Query Portal and In-context Information
- Care Coordination: Encounter Notification Service
- Population Health: CRISP Reporting Services (CRS)
- Public Health Support: Public Health Alerting and Reporting
- Program Administration: Supporting HSCRC Care Redesign Programs

8.2 Availability and Network Monitoring

The CRISP Services are monitored continuously by the CRISP and/or third parties. CRISP and our partners maintain agreements that provide for at least 99.7% uptime per calendar month, not including scheduled downtime. For each calendar year, scheduled hardware, software, and communications maintenance shall not exceed an average of 8 hours in total per calendar month. All scheduled maintenance will be carried out on dates and at times authorized by CRISP with at least three (3) business days' notice provided by CRISP or vendor to all participants via e-mail or other electronic method such as the CRISP landing page https://ulp.crisphealth.org, or www.crisphealth.org.

In the event of unexpected downtime, CRISP will provide notifications to all participants via e-mail or other electronic method such as the CRISP landing page https://ulp.crisphealth.org, or www.crisphealth.org). Depending on the severity level of the problem. Initial notification to participants will occur between four (4) hours and three (3) business days after discovery of the problem.. Updates will occur, via the same methods, every eight (8) business hours to every three (3) business days, depending on the severity level.

8.3 Maintenance

Participants will be provided with a maintenance overview document and will be required to provide support contact information to CRISP. Participant support staff will be expected to assist with issues surrounding on-going training, master patient index (MPI) administration, data quality, system upgrades and downtime, and privacy and security issues.

Participants that are acting as consumers of data will be required to provide a single point of contact (POC) for CRISP Services. This contact will be responsible for the maintenance of user profiles. This includes providing all necessary information to CRISP for adding users, deleting users, and assigning or changing user roles. The POC should notify CRISP immediately if a user's employment at the organization has been terminated or if his or her functional role has changed. This notification can be done either using the self-service POC audit tool or an email to support@crisphealth.org. The POC will also be responsible for checking that users have completed all necessary policy training prior to obtaining access to the CRISP Services and for monitoring the general use and operations of the CRISP Services.

9. Support

CRISP offers participants a technical support to respond to technical problems. The technical support can be reached at support@crisphealth.org or 1-877-952-7477. Depending on the nature of the issue, technical problems may be dealt with directly by CRISP staff or in certain situations may be raised to the attention of the vendor. Examples of issues that will be resolved directly by CRISP staff include CRISP portal user support, password resets, new user setups, and MPI merge problems. The following types of issues will be escalated by CRISP to the vendor: system status, service problems, infrastructure problems, interface issues, connectivity problems, and other technical issues. For all reported problems, CRISP will work to find a resolution in a timely manner and update participants of actions taken as appropriate. The help desk operating hours are Monday through Friday 8:00 AM to 5:00 PM. An afterhours messaging service is also available Emergency support will only be accepted outside of normal operating hours. CRISP operations will be closed for the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Christmas Day

10. Audit

All participants are required to monitor and audit access to and use of their information technology systems in connection with the CRISP Services and in accordance with their usual practices based on accepted health care industry standards and applicable law. In the event CRISP wishes to exercise its right to audit the participant, participant will provide CRISP with monitoring and access records upon request. CRISP regularly reviews the usage of participating user's access of patient records and will enforce any misuse of a user to include and up to termination of CRISP Services access.

11. Report of Breach

In the event that a participant determines that the data transmitted through the CRISP Services has been requested, used or disclosed by the participant or a participant user in a manner that does not comply with applicable law and/or the provisions of the Participation Agreement, the participant is responsible for notifying CRISP of the event. Notification should include a detailed summary of the relevant facts, within two (2) business days of the determination. The participant will cooperate with CRISP as to further investigation or responsive action reasonably requested or taken by CRISP to respond to the event. The notification shall be treated by CRISP as confidential information, except as otherwise required pursuant to applicable law or as used or disclosed by CRISP in connection with exercise of CRISP's rights and/or obligations under the Participation Agreement, to defend its actions in any process or proceeding begun by or involving the participant or applicable law.

In the event that CRISP determines that participant data transmitted through the CRISP Services has been requested, used or disclosed by CRISP in a manner that does not comply with applicable law and/or the provisions of the Participation Agreement and that such event constitutes a breach, CRISP will comply with the provisions of the Business Associate Agreement.

12. CRISP Board of Advisors

CRISP has developed a governance model that includes a Board of Advisors to provide guidance and input to the CRISP Board of Directors on certain key decisions during the development and operations of the CRISP Services. The Board of Advisors is intended to be broad based to ensure that a breadth of interested organizations have the opportunity to participate and represent their constituencies. Distinct regions may develop their own committee structure. CRISP DC Board of Advisors consists of a Clinical Advisory Committee that has the authority to approve use cases. The CRISP Maryland Board of Advisors is organized into the five (5) committees below:

1. Technology Committee
2. Clinical Committee
3. Finance Committee
4. Privacy & Security Committee
5. Reporting & Analytics Committee

The general responsibilities of each committee are defined in the Board of Advisors Nomination and Selection Process available from CRISP. The CRISP Board of Directors will appoint individuals to the Board of Advisors Committees, selecting from among those who have been identified by or made known to CRISP who are deemed qualified for the particular Committee and are willing to serve, aiming for the most capable team possible, while also seeking to ensure geographic and organizational diversity, and after consultation with State and District officials. Decisions made by the CRISP Board of Directors will be final.

13. Provider Authorization

Participant Users, by electing to receive data through CRISP, authorize CRISP to transmit results reports and other patient information directly from Participant Users' ancillary providers, such as clinical laboratories and radiology centers. Participant Users further acknowledge the following:

1. All ancillary providers only represent that, at the time the data is transmitted by the ancillary provider, the data transmitted is an accurate representation of the data the is contained in, or available through, the ancillary provider's system;
2. Nothing in the Participation Agreement, Policies and Procedures document, or otherwise will impose responsibility or liability on ancillary providers related to the accuracy, content, or completeness of any data or information provided in connection with a message or otherwise;
3. As a data source, ancillary providers do not assume any control over or responsibility for the clinical decision making as to any patient of a Participant; and
4. If not approved by ancillary provider for delivery of Report of Record, access to such data through the CRISP Services is neither designed nor intended to replace ancillary provider's principal method of results delivery to Participant and does not constitute a "Report of Record." The official list of ancillary providers participating in CRISP can be found on the CRISP website at www.crisphealth.org.

14. Standards

CRISP aims to support the CRISP Services in a standards compliant manner and will use best practices and generally accepted standards when possible and appropriate that are recognized by State, Federal, or Industry authorities.

15. Policies and Procedures Amendment Process

CRISP reserves the right to make amendments to the Policies and Procedures and to the Participation Agreement. Notice of amendments may be provided by posting the amendment, along with its effective date, on the CRISP website www.crisphealth.org, as well as providing notice to participants. Amendments will be made pursuant to the Section of the Participation Agreement.

15.1 Definition of Majority

Majority will be determined in consultation with a special Amendment Review Committee that will be made up of a subset of members from each of the Committees on the CRISP Board of Advisors. The Amendment Review Committee will represent a broad range of HIE stakeholders, which can advise CRISP as to the extent of hardship that may be experienced due to a proposed amendment.

Appendix A - Sample Authorized User Agreement

AUTHORIZED USER AGREEMENT

I, the undersigned individual below, as a condition of being granted access to the Health System Health Information Exchange (Health System HIE) as an Authorized User, hereby acknowledge, represent, and agree to the following Terms and Conditions:

1. I acknowledge and understand that the Health System HIE facilitates making patient information (Data) available to authorized individuals and organizations for Treatment and other Permissible Purposes, such as care coordination and quality improvement, and that the Participant identified below has entered into a Participation Agreement with Health System HIE and has designated me as an Authorized User of Data of the Health System HIE on behalf of such Participant;

2. The Health System HIE will agree to provide me with access to Data through the Health System HIE only if I agree to the terms of this Authorized User Agreement;

3. By signing below, I agree to comply with all terms and conditions of access to Data under this Authorized User Agreement, the Participant's Participation Agreement, all Health System HIE Policies and Procedures, and applicable laws and regulations that may govern or affect my use of the Health System HIE (collectively, the "Terms and Conditions");

4. I understand that this is a BINDING agreement, and that my failure to comply with the Terms and Conditions of access and use of the Health System HIE may be grounds for discipline, including without limitation, denial of my privileges to access Data through the Health System HIE;

5. I understand that I may access the Health System HIE only to obtain Data allowable in the permitted purposes section of CRISP policies and procedures and in accordance with my role at my organization and may not use the Health System HIE for any purposes that are outside the scope of my responsibilities and duties with Participant;

6. This Authorized User Agreement grants to me a nonexclusive, nontransferable right to use the Health System HIE which is specific to Me, and I may not share, sell or sublicense this right with anyone else, nor change, reverse engineer, disassemble or otherwise try to learn the source code, structure or ideas underlying the Health System HIE's software or introduce a virus to the Health System HIE, nor connect or install unauthorized or uncertified equipment, hardware or software or improperly use the hardware or software relating to use of the Health System HIE;

7. As an Authorized User, I may have access to Data that includes protected health information (PHI) that is subject to confidentiality, privacy and security requirements under state, district, and federal law and regulations, and I hereby specifically and expressly agree that I will only access Data consistent with my access privileges, and pursuant to all requirements under the Terms and Conditions of the Health System HIE;

8. I understand that I have an obligation to maintain the confidentiality, privacy and security of the Data that I access through the Health System HIE, and that I will not disclose any Data except as required for the performance of my duties as an employee or agent of Participant and subject to all terms of this Agreement;

9. At any time after my employment/business relationship with the Participant has ended, I agree to keep confidential any and all information which I obtained as a result of my access to the Health System HIE;

10. I will not access or view any information other than what is required for the performance of my duties as an employee/agent of Participant, and will otherwise access or use the Health System HIE only for legitimate business purposes and not for conducting unlawful activities or any personal business;

11. I will not make any unauthorized copies of Data, and will not save any Confidential Information to portable media devices (Floppies, memory sticks, ZIP disks, CDs, PDAs, and other devices);

12. I will not email any Data to another email account, except as expressly provided for in the secure network messaging environment provided by the Health System HIE;

13. I ACKNOWLEDGE THAT MY AUTHENTICATION CODE AND PASSWORD IS THE LEGAL EQUIVALENT OF MY SIGNATURE, AND THAT I WILL NOT DIVULGE, RELEASE OR SHARE MY AUTHENTICATION CODE OR DEVICE OR PASSWORD WITH ANY OTHER PERSON, INCLUDING ANY EMPLOYEE OR PERSON ACTING ON MY BEHALF, AND SHALL NOT PERMIT OR AUTHORIZE ANYONE ELSE TO ACCESS THE HEALTH SYSTEM HIE UNDER MY AUTHENTICATION CODE OR DEVICE OR PASSWORD, AND FURTHER AGREE NOT TO USE OR RELEASE ANYONE ELSE'S AUTHENTICATION CODE OR DEVICE OR PASSWORD;

14. I acknowledge that I am responsible for all usage on my accounts, and that my account usage may be monitored at any time;

15. I agree to notify the Health System HIE and Participant immediately if I become aware or suspect that another person has access to my authentication code or device or password, and if I have reason to believe that the confidentiality of my password is broken or believe that there has been a misuse of Data, I will contact Health System Health Information Services (856-248-6333) immediately;

16. I agree to log out of the Health System HIE before leaving my workstation to prevent others from accessing the Health System HIE;

17. I agree never to access Data for "curiosity viewing," which includes accessing Data of my family members, friends, or coworkers, celebrities, public figures etc, unless access is necessary to provide services to a Patient with whom I or the physician(s) with whom I work has a direct treatment relationship with;

18. I will, to the best of my ability, ensure and protect that Data submitted or received through the Health System HIE is accurate and agree not to insert or enter any information into the Health System HIE, including through the Participant's electronic health record (EHR) that I know is not accurate;

19. I acknowledge and agree that the Health System HIE and Participant have the right at all times, including without my consent or notice to me, to monitor, access, review, audit and disclose my access to and use of the Health System HIE and compliance with the terms of this Authorized User Agreement, the Health System HIE Policies, and applicable law, including any hardware or software located at my office, home, or any other site from which you access the Health System HIE;

20. I fully understand that my failure to comply with any of the Terms and Conditions of this Authorized User Agreement or other terms of use of the Health System HIE may result in disciplinary action against me, which may include, but not be necessarily limited to, loss of access to the Health System HIE as an

Authorized User, voiding/termination of contracts; loss of medical staff privileges; and/or loss of licensure; penalties/and or fines imposed by state, district, or law, among other things;

21. By signing below, I acknowledge and agree that I have completed all required training regarding the Health System HIE, including on the permissible and prohibited practices relating to the access and use of the Health System HIE, and agree to abide by all information covered during such training;

22. If I unlawfully access or misappropriate Data, including patient information, I agree to indemnify and hold harmless Health System Health, its subsidiaries, affiliates, and its successors and assigns against and from any and all claims, demands, actions, suits, proceedings, costs, expenses, damages, and liabilities, including reasonable attorney's fees arising out of, connected with or resulting from such unlawful use;

23. I certify that the documents and information I provide to all Health System HIE in order to authenticate my identity and demonstrate my professional credentials is current, accurate and authentic, and I acknowledge and understand that if I present false documents for these purposes, this may subject me to criminal, civil and other repercussions; and

24. This Authorized User Agreement will be in effect from the time it is signed until Health System HIE or Participant terminates my status as an Authorized User or until I violate the terms of this Agreement, and any terms of this Agreement necessary to protect the Health System HIE and Data will survive the termination of this Agreement.

By signing below, you have read and agree to abide by all Terms and Conditions of access and use to the Health System HIE as set forth in this Authorized User Agreement. Please complete the entire form below, then fax to IS Security Administration at XXX-XXX-XXXX.

Please Print Clearly – ALL FIELDS ARE REQUIRED

Full Name (First, Middle, Last):

Signature:

Professional Title:

Cell Phone:

Primary E-mail:

Appendix B - Approved Quality Improvement and Care Coordination Uses

The following are approved uses of the health information exchange, under the category of quality assessment and improvement activities, including care coordination and are published on the CRISP website www.crisphealth.org. These uses may be among covered entities, such as payers and providers that have an interest in quality improvement and care coordinating for patients. Examples of these covered entities may also include patient centered medical home programs and accountable care organizations. Approved uses under permitted purpose number three (3) may be modified or added from time-to-time with the approval of the CRISP Clinical Advisory Board, and such additions will be treated as a non-material amendment to the Policies and Procedures. Additional criteria may be associated with approved uses, including requirements of Applicable Law, published by CRISP as a policy document for the specific use at the time of its approval by the Clinical Advisory Board.

1. **Reporting Services**: delivering summary reports to a provider with ADT information on medical services encounters their patients had with other HIE participants in the period prior to or the period after receiving treatment from the provider. For example, this use would include reports to a hospital on the number of readmissions their patients had to another hospital within 30 days of discharge. If such reports include identifying information, such as medical record numbers or small groupings, criteria must be followed to ensure information is related to encounters which happened within a short timeframe of the treatment event at the provider receiving the report and opt out capabilities must be maintained. (See CRISP Encounter Reporting policy document.)

2. **Notifications Service**: delivering ADT information about a patient's medical services encounter, for instance at the time of hospitalization, to a permitted recipient with an existing relationship with a patient, such as a primary care provider or payer. Criteria for validating the continued existence of the patient relationship must be followed, mechanisms for informing patients when appropriate must be in place, and opt out capabilities must be maintained. Organizations must provide justification criteria for subscribing to encounter alerts for the patient panel being submitted to CRISP (See CRISP Encounter Notification policy document.)

3. **Cancer Registrars**: allowing designated cancer registrars the use of the CRISP portal to collect relevant information on cancer patients to satisfy mandatory reporting to the state and national registries for accreditation purposes. At the state level, all newly diagnosed cancer patients are required to be reported to the registry. On a national level, the American College of Surgeons (ACoS) Commission on Cancer (CoC) accreditation program requires ongoing reporting of the diagnosis, treatment, and outcomes data over a patient's lifetime that contributes to organization-specific performance and quality benchmark reports. Criteria for validating the continued existence of the patient relationship must be followed, mechanisms for informing patients when appropriate must be in place, and opt out capabilities must be maintained, except for the case where reporting to the state is mandatory. (See CRISP Cancer Registry policy document.)

4. **Query Portal Access Outside CRISP Service Area:** expands access to CRISP Services which include the Query Portal and Notification Service for select out of CRISP Service Area providers who do not practice within the CRISP Service Area but provide care to patients who live within the CRISP Service Area. Currently CRISP Service Area operates in Maryland and the District of Columbia and expand outside this current Service Area. CRISP expanded access to CRISP Services so that more of the nurses and doctors who provide care for CRISP Service Area patients to improve and ease care for residents who seek out of CRISP Service Area care and promote care coordination within the CRISP

Service Area. CRISP will limit the eligible participants to ambulatory practices with a practice address within ten miles of the CRISP Service Area. For practices outside of this CRISP Service Area radius, or for any out of CRISP Service Area hospital, CRISP will consider portal access requests on a one by one basis.

5. **Access to Query Portal for Health Plans:** enables health plans to query for their members clinical information using CRISP services to improve care coordination for these individuals. An individual's information is available to the health plan while the members is active, including any historical information. Criteria for validating the continued existence of the patient relationship must be followed, mechanisms for informing patients when appropriate must be in place, and opt out capabilities must be maintained.

6. **Opioid Related Events:** leverages the clinical information received by hospital participants and potentially, other participant data sources to deliver opioid related event information to participants. Displaying this information in a clear manner will provide participants with an opportunity to integrate the information into clinical decision making and enable improved care coordination for individuals experiencing these events. Criteria for validating the continued existence of the patient relationship must be followed, mechanisms for informing patients when appropriate must be in place, and opt out capabilities must be maintained.

7. **Use of CRISP Services for Quality Improvement:** allows CRISP provider participants to access CRISP services for quality improvement purposes. HIPAA allows for quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities. Access to clinical data through CRISP services will serve as an additional vehicle for advancing quality improvement (QI) activities, including populating clinical and health registries. Criteria for validating the continued existence of the patient relationship must be followed, mechanisms for informing patients when appropriate must be in place and opt out capabilities must be maintained.