Chesapeake Regional Information System for Our Patients (CRISP)

Policies and Procedures

Version: 10
Date: March 2022

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 the 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.

Participant acknowledges that Participant is responsible for reviewing the Policies and Procedures on the 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 with the applicable Section of the Participation Agreement. Unless otherwise noted, capitalized terms contained herein have the meaning given to them in the Participation Agreement.

1. Participant Users

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 Participant.

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 this 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 Participant User as necessary.

1.1 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 a Participant, the Participant must inform CRISP of this termination within five (5) business days, and prior to actual termination if at all possible. CRISP will terminate the Participant User's account immediately upon notification of termination of employment from the respective Participating Organization. Participants accessing the CRISP Services through third party EHRs, via SSO/SAML, will be responsible for terminating access through this EHR for the terminated Participant User at the time of termination. However, Participating Organizations must still notify CRISP within five (5) business days so that CRISP can terminate access to other CRISP tools and services that are not accessed via SSO/SAML, including but not limited to CRISP Direct, and DocHalo.

1.2 Training

CRISP will make training available through their website, in addition to other training materials as appropriate. Participating Organizations will be responsible for training individual users on data consumption, CRISP policies, and in accordance with the Participation Agreement and Business Associate agreement, including the creation and dissemination of any necessary training provided by CRISP (*See*

Section 8.3. Maintenance) and beyond. If additional training is necessary as a result of system updates, CRISP will provide training through the website and inform Participating Organizations of the changes, and each organization will then be responsible training all of its end users.

2. User Name and Passwords

CRISP will utilize security-industry best practices for authenticating user access to CRISP Services and tools. CRISP and Participants must ensure that each Participant User is assigned a unique username,password, and multi factor authentication (MFA) is enabled on each account to access services.

2.1 Password Convention

CRISP password requirements differ across the tools and services. CRISP will communicate requirements as needed for each tool. Participant User passwords will expire every 90 days, requiring that each Participant User selects a new password at that time. Password history settings will be enforced to ensure that a Participant User does not duplicate a password used previously.

2.2 Lock Outs and Password Resets

Participant Users will be able to reset their own password using answers to the challenge questions set during initial login for the Portal. 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 Participant User must call the CRISP support desk directly at 1-877-952-7477. Participant 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. Participant Users not using single sign on must be verified every 90 days by the authorized administrator of the Participant.

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 Participant Users access to clinical data on behalf of the Participant, as a covered entity, and its clinicians. This authorized 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

Participant Users agree to view, 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. It is the Participant's obligation to ensure the appropriate use of CRISP Services by Participant and Participant Users

3.2 Data Misuse

Health information available through CRISP is to be accessed, viewed, and used only by CRISP Participants and Participant Users who have been authorized to do so, and only for permitted purposes. CRISP uses a privacy tool for additional monitoring of all user activities around protected health information access to ensure all provisioned accounts are being used appropriately and to protect personal health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of CRISP Services by

Participant and Participant Users. Any misuse of protected health information in connection with CRISP services must 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 protected health information has occurred. As 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 use for a Participant or Participant User(s).

3.3 Participant Procedures for Non-Compliance

In accordance with the participation agreement, each Participant should implement procedures to mitigate and deter misuse and issue appropriate consequences to hold Participant Users responsible for misuse of data obtained when accessing protected health information through the CRISP Services. As 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 information twice per year free of charge. CRISP requires the patient request 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

Unless otherwise required by Applicable Law, CRISP's 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. It is the Participant's responsibility, 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 after CRISP's receipt 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 Access to Health Information

Available Information and Methods for Access

As discussed below, patient access it a Permitted Purpose and is required, in most cases, under Appliable Law. Patients can find a list of the types of information CRISP stores as part of its routine operations on the CRISP website. The list indicates which information is available for patient access and which information is unavailable. CRISP will facilitate multiple methods for patient information access, including through third party applications and accessing information directly from CRISP.

Access to Information for Minors

State or Federal law my prohibit health care providers from disclosing certain health related information about a minor patient to anyone, including parents, without the express consent of the minor. It is technically infeasible for CRISP to segment or remove data from encounters or clinical documents in order to avoid disclosing specific types of information that Applicable Law prohibits being disclosed. At this time, CRISP is not able to make available any information for individuals aged 12-17. Parents or legal guardians who are able to demonstrate their custodial relationship may have access to information for their children aged 0-11.

Support and Education

CRISP will make available on the CRISP website educational materials about best practices and methods for patients accessing their information, including privacy and security risks associated with certain methods or vendors. In addition, the materials will remind patients that their healthcare providers will likely have more robust information and are the appropriate contact if they have questions or concerns with the information shared. The CRISP support team will answer patient questions about how to access their CRISP information, but patients who have questions about their information will be directed to the health care provider who shared the information.

5. Permitted Purposes

Participants and Participant Users may access and use data through CRISP Services for only Permitted Purposes. Permitted Purposes for data use are listed below:

1. For treatment of an individual
2. For a Public Purpose as permitted or required by Applicable Law and consistent with the mission of the HIE to advance the health and wellness of patients in the CRISP service area (
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 the Participation Agreement
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.
5. Individual access and patient authorized access.
6. All other allowed purposes as determined by CRISP to be required under the Applicable Law.

Permitted Purposes may be further specified through use cases, which can be found on the CRISP Website at www.crisphealth.org. The use cases are approved and amended by the applicable Committee before their incorporation into a Permitted Purpose.

With the approval of the applicable Committee, 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 may add Permitted Purposes according to the Participation Agreement.

6. Participating Data Providers

Participants must complete testing and other onboarding activities prior to going live with connectivity to CRISP. These testing and onboarding activities are tailored to the type of data being provided and accessed and typically include a patient panel. CRISP communicates these requirements during the onboarding process. 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. 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 confirm that they are ready to go live.

6.1 Data Contributors

Participants will make data available that are necessary to engage CRISP Services. For each Participant, information made available to the CRISP Services will be subject to appropriateness and technical readiness. For a Participant to be connected to and remain connected to CRISP Services, it 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, including but not be limited to - substance use disorder treatment and self-pay information that may be restricted by Applicable Law, unless a separate written agreement has been executed with CRISP to share sensitive data protected by Applicable Law. Participants are responsible for complying with Applicable Laws and for filtering any information that should not be disclosed to through CRISP.

7. Data Retention and Reuse

CRISP will retain disclosure data for a minimum period of seven (7) years, as required by Applicable 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 to the Permitted Purposes.

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 terminates access to the CRISP Services in accordance with the Participation Agreement, CRISP will disable that Participant's data feeds and terminate the Participant's ability to access the CRISP Services in accordance with the Participation Agreement. 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, 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. CRISP makes data available through five core service areas:

1. Point of Care: Clinical Information
2. Care Coordination: Encounter Notifications
3. Population Health: CRISP Reporting Services (CRS)
4. Public Health Support: Public Health Alerting and Reporting
5. Program Administration: Supporting HSCRC Care Redesign Programs

8.2 Availability and Network Monitoring

CRISP services are monitored continuously by CRISP and/or third parties. CRISP and our partners and vendors maintain agreements that provide for at least 99.7% uptime per calendar month, not including scheduled downtime. CRISP commits to 99.9% of messages being delivered within 24 hours of receipt of admission, discharge, or transfer message from supplying Participant. 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 or CRISP web page.

In the event of unexpected downtime, CRISP will provide notifications to Participants via e-mail or other electronic method such as the CRISP or CRISP web page. 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 until notification of resolution.

8.3 Maintenance

Participants 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 at least one, but preferably two points of contact, HIE administrators for CRISP Services. This administrator will be responsible for the maintenance of user profiles, including providing all necessary information to CRISP for adding users, deleting users, and assigning or changing user roles. The Administrator 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 HIE Admin Tool (recommended) or an email to support@crisphealth.org. The administrator will also be responsible for attesting to the user identity verification and 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.

8.4 Implementation Support

CRISP will make available the following implementation services (collectively, "Implementation Services") to the Participant:

- Establish environments (test and production) for secure transactions
- Configure environments based on CRISP Policies and Procedures regarding privacy, security, and consent;
- Conduct planning and decision sessions;
- Jointly document transaction types;
- Jointly document data conversion and mapping requirements;
- Establish real-time notifications, if applicable;
- Test and validate real-time notification, if applicable;
- Establish batch transaction, if applicable;
- Test and validate batch transactions, if applicable.

8.5 Operations Support

CRISP will make available the following operational support to the Participant:

- At least daily backups of the production environment;
- Transaction logs of all database updates that occur between daily backups;
- Periodic performance management;
- Disaster Recovery as required in the event of a catastrophic failure of the primary production site location using an alternate recovery site;
- Maintain Datasets (e.g., authorized users) with data supplied by CRISP or Participant;
- Support Participant's periodic reconciliation of ENS notification and claims-based encounter information.

9. Support

CRISP offers participants technical support to respond to technical problems, including support for test and production environments. The technical support can be reached at support@crisphealth.org or 1-877-952-7477. CRISP support uses a trouble ticket logging system that documents the severity and enables triage of most severe problems. 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. 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 provides support 24 hours a day, seven days a week, including weekends and holidays. 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 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 Participating User to include and up to termination of CRISP Services access. CRISP uses a privacy tool for additional monitoring of all user activities around protected health information access to ensure all provisioned accounts are being used appropriately and to protect protected health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of CRISP Services by Participant and Participant Users.

11. Report of Breach

In the event that a Participant determines that the data transmitted through 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 must notify 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 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. In the event of a Breach of protected health information in CRISP Services requiring notification to individuals under Applicable Law, CRISP, as required by the Participant, will make such notification electronically to individuals who have previously agreed to electronic notice.

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 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. 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 Services, 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, this 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 a 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 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 Participation Agreement.

15.1 Definition of Majority

Majority, as referenced in the Participation Agreement, 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.

16. Information Blocking Rule

The 21st Century Cures Act (CURES) and its implementing regulation (the Information Blocking Rule (IBR)) prohibits "information blocking," which is a practice engaged in by an Actor that interferes with the access, use or exchange of Electronic Health Information. The IBR requires Actors, like Health Information Networks, to fulfill requests for Electronic Health Information (EHI). This requirement is entirely consistent with CRISP's goals. The IBR also expressly recognizes that Actors, like Health Information Networks, must impose restrictions on those who seek to access, exchange or use EHI because those restrictions promote a larger public purpose such as making certain that the privacy and security of EHI is protected and that only those who are authorized can actually access, exchange or use EHI. The IBR

includes several specific Exceptions which an Actor can use to decline to fulfill a request for EHI in certain situations. The Content and Manner Exception specifically allows an Actor and a data requestor to mutually agree on the terms under which the requestor will access, exchange or use EHI.

The Participation Agreement and these Policies and Procedures are designed to comply with the Content and Manner Exception by specifying the mutually agreed upon terms and conditions that govern the access, exchange and use of information by Participants. Other IBR exceptions may also apply from time to time depending upon the unique facts and circumstances that are present when a request for EHI is presented to CRISP. CRISP will document its reasons for not fulfilling a request for EHI to the best of its ability so that a record exists in the event that an information blocking complaint is filed. CRISP will also review and update its Participation Agreement and the Policies and Procedures from time to time in an effort to assure that they remain in compliance with the IBR and any other Applicable Law.

17. External HIE Participation

17.1 CRISP Shared Service Affiliates

As an affiliate of CRISP Shared Services (CSS), CRISP is able to take advantage of many economies of scale provided to affiliates, including data storage and maintenance costs. CRISP's relationship with CSS requires CSS to ensure that CRISP participant data is handled securely and shared only in accordance with the Permitted Purposes outline in CRISP Policies and Procedures. CRISP participant data may be shared with other CSS affiliate HIEs in accordance with Applicable Law and CRISP Permitted Purposes. For example, patients who may receive treatment in both MD and WV, may have data viewed by Participants on their care team as well as WV Health Information Network (WVHIN) participants on their care team for purposes of treatment and care coordination.

17.2 Current Participation

From time-to-time, CRISP will enter into agreements to participate with External HIEs as defined by the CRISP Participation Agreement. These External HIEs include but may not be limited to National Networks or other state or local HIEs. At this time, CRISP shares information with External HIEs only for the purpose of treatment. Any additional purpose for sharing would be approved by the appropriate CRISP Advisory Committee and in accordance with the CRISP Participation Agreement and these Policies and Procedures.

17.3 New Participation Procedures

In collaboration with the CRISP Advisory Committee(s), CRISP may determine it is beneficial to CRISP and CRISP Participants to participate with additional External HIEs. CRISP Advisory Committee(s) will assist CRISP to perform privacy and security reviews of the External HIEs. Additionally, CRISP will ensure that any External HIE agreements are substantially equal to the CRISP Participation Agreement and the CRISP Policies and Procedures relative to privacy and security; data storage and transmission, insurance and liability provisions, and permitted purposes for data disclosure and redisclosure.

17.4 Education and Notice

CRISP will publish all External HIE agreements, including terms and conditions and policies and procedures to the CRISP website for Participant review. If in collaboration with the CRISP Advisory Committee, CRISP MD enters into an agreement with an External HIE, CRISP will provide notice to CRISP participants with 30 days. CRISP will provide information for patients on CRISP website regarding CRISP participation with External HIEs and whether and how a patient can opt-out of the External HIE. CRISP will not share any information with an External HIE for any patient who has opted out of CRISP MD.

18. HIE Fees

As of 2021, CRISP charges participation fees to hospital providers and payer participants. At this time, other participants are able to access CRISP Services free of charge. This policy and the corresponding fee assessment procedures are approved by the CRISP Board of Directors as overall projection of future costs and may be changed from time-to-time by the CRISP Board of Directors.

18.1 Hospital Fees

Maryland hospital fees are calculated based on the number of admissions and total revenue for each hospital relative to other Participant hospitals.

18.2 Payer Fees

Maryland payer fees are calculated on a Per Member Per Month basis, with is multiplied by the annual membership count of the Participant.

Appendix A - Sample Authorized User Agreement

AUTHORIZED USER AGREEMENT

CRISP currently has a Participation agreement with each data-contributing hospital ("Participants") and with all other provider and payer organizations that access data. The Participation Agreement includes specific provisions governing the use of data and includes a business associate agreement. These agreements and CRISP's Policies and Procedures can be found at www.crisphealth.org. Any capitalized terms in this Authorized User Agreement, unless otherwise defined, have the meaning given to them in the Participation Agreement.

I, the undersigned individual below, as a condition of being granted access to CRISP Services as an Authorized User, hereby acknowledge, represent, and agree to the following Terms and Conditions:

1. I acknowledge and understand that CRISP makes patient information ("Data") available to only authorized individuals and organizations for treatment, care coordination, quality improvement, and other permitted purposes, as identified in the Participation Agreement ("Permitted Purposes"). I understand that I am a designated Authorized User of Data of on behalf of my participating organization ("Participant");

2. By signing below, I agree to comply with all terms and conditions of access to Data under this Authorized User Agreement, the Participation Agreement, and CRISP Policies and Procedures, and applicable state and federal laws and regulations (collectively, the "Terms and Conditions");

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

4. I understand that I may access the Data only for Permitted Purposes specific to my role and responsibilities in Participant;

5. This Authorized User Agreement grants to me a nonexclusive, nontransferable right to access the Data 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 CRISP's Services, nor connect or install unauthorized or uncertified equipment, hardware or software or improperly use the hardware or software relating to use of CRISP Services;

6. 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;

7. I understand that I have an obligation to maintain the confidentiality, privacy, and security of the Data, 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 the Terms and Conditions;

8. 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 Data;

9. I will not make any unauthorized copies of Data, and will not save any Data outside of CRISP Services;

10. I will not email any Data to another email account, except as expressly provided for in the secure network messaging environment provided by CRISP Services or the approved secure and encrypted email solution provide by the Participant;

11. 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 CRISP SERVICES 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;

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

13. I agree to notify CRISP and Participant immediately if I become aware or suspect that another person has access to my authentication code or device or password or if I have reason to believe that the confidentiality of my password is broken or believe that there has been a misuse of Data;

14. I agree to log out of CRISP Services before leaving my workstation to prevent others from accessing the Data;

15. 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 it is necessary to provide services to a patient with whom I or the physician(s) with whom I work has a direct treatment relationship;

16. I understand that CRISP uses a privacy tool for additional monitoring of all users' activity around PHI access to ensure all provisioned accounts are being used appropriately and to protect personal health information.

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

18. I acknowledge and agree that CRISP 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 HIE and compliance with the terms of this Authorized User Agreement, the Participation Agreement, the Policies and Procedures, and Applicable Law, including any hardware or software located at my office, home, or any other site from which I access CRISP Services;

19. By signing below, I acknowledge and agree that I have completed all required training for CRISP Services, including on the permissible and prohibited practices relating to the access and use of CRISP Services, and agree to abide by all information covered during such training;

20. If I unlawfully access or misappropriate Data, including patient information, I agree to indemnify and hold harmless CRISP Services and Participant, their subsidiaries, affiliates, and their 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;

21. I certify that the documents and information I provide to CRISP Services 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

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

By signing below, I have read and agree to abide by all Terms and Conditions of access and use to the CRISP Services as set forth in this Authorized User Agreement.

Please Print Clearly – ALL FIELDS ARE REQUIRED

Full Name (First, Middle, Last):

Signature:

Professional Title:

Cell Phone:

Primary E-mail: