Chesapeake Regional Information System for Our Patients (CRISP)

Policies and Procedures

Version: 2.0
Date: September 2023

Table of Contents

Background

Overview of CRISP

Established in 2009, Chesapeake Regional Information System for our Patients ("CRISP"), a not-for-profit corporation, acts as the state-designated Health Information Exchange ("HIE") and Health Data Utility ("HDU") for the State of Maryland. CRISP's Services allow Participant Users across systems and platforms to share health information, as allowed by Applicable Law, to improve care for individuals and the state, as a whole. CRISP integrates Data from many different sources and provides governance to ensure that Data are protected and secure. Part of this governance includes common "rules of the road" for entities using CRISP services. Specifically, each Participant must enter into the CRISP Participation Agreement.

These Policies and Procedures contain specific terms and conditions for operation and use of the CRISP Services, specific technical specifications information, and other terms or requirements relating to the CRISP Services that are specified in the Terms and Conditions of the 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 governs. These Policies and Procedures may be amended from time-to-time in accordance with the Participation Agreement. Any capitalized terms in this document not otherwise defined have the definition given to them in the Participation Agreement.

Participating in CRISP

To be a Participant in CRISP, an organization must be a HIPAA-covered entity. These entities must work with the CRISP Outreach team to execute a Participation Agreement, including a Business Associate Agreement. In addition, every organization must attest whether it is covered by 42 CFR Part 2 ("Part 2"). If it is, the organization must either attest to not sending any data covered by Part 2 or must sign a Qualified Services Organization Agreement ("QSOA") addendum. After providing the appropriate documentation, Participants work with an onboarding team to technically integrate with the CRISP infrastructure and provide a list of patients with whom the organization has a relationship. The CRISP Onboarding team also works with the Participant to update its Notice of Privacy Practices and other documentation needed for consumer education. Limited CRISP Services may be provided to other entities that are not covered by HIPAA, as allowed by Applicable Law.

Participant Users

After onboarding, the Participant can credential users from its organization ("Participant Users") to directly access CRISP Services through the CRISP online portal or through an electronic health record ("EHR") system. 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 unique username and password will be assigned to that user for each Participant with which the user is associated.

Participants must have enforceable agreements with each of their Participant Users governing the appropriate use of the CRISP Services; 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 Participant Users. Participants must require that all of their Participant Users comply with applicable laws, clauses in the Participation Agreement, and these CRISP Policies and Procedures. If a Participant User is in violation of any of these terms, the Participant must immediately

notify CRISP, and CRISP may suspend or terminate the Participant User's access to the CRISP Services, as necessary.

Corporate Structure and Governance

Corporate Governance

A Board of Directors ("Board") oversees CRISP and provides guidance and input on certain key decisions during the development and operations of the CRISP Services. Decisions made by the Board of Directors are final. In addition to the Board, the following advisory committees provide specialized advice and guidance and report their recommendations and decisions to the Board:

1. Clinical Committee
2. Consumer Advisory Council
3. Finance Committee
4. Privacy and Security Committee
5. Reporting and Analytics Committee

The Board has the authority to form additional advisory committees at its discretion. The general responsibilities of each committee are defined by their respective Charters. Copies of these Charters will be made available to Participants upon request. The Board appoints individuals to each committee, 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. The Board aims for the most capable team possible, while also seeking to ensure geographic and organizational diversity, and after consultation with state officials.

Data Governance

Uses for the Data are governed by the Permitted Purposes in the Participation Agreement, which are further explained and authorized, as necessary, through use cases. The Clinical Committee is responsible for approving any new use cases, all of which are posted on the CRISP website. In addition, the Consumer Advisory Council may provide advice and guidance on uses of the Data that may raise specific privacy concerns. CRISP may not use or exchange any Data outside of the Participation Agreement or other agreements governing the Data.

CRISP Shared Services, Inc.

CRISP Shared Services, Inc. ("CSS") is an independent, managed services organization providing technology support and other resources and services to CRISP and other HIEs throughout the country ("Partner HIEs"). CSS is independently governed by its own Board, which consists of representatives from each of its member HIEs. CRISP provides input and guidance to CSS through its Board members.

Permitted Purposes for Data Use

Permitted Purposes

Participants and Participant Users may access and use Data through CRISP Services for Permitted Purposes. Permitted Purposes for Data use through CRISP Services are for:

1. Treatment of an individual;
2. 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. Quality assessment and improvement activities;
4. Research;
5. Individual access and patient-authorized access;
6. All other allowed purposes as determined by CRISP to be required under Applicable Law.

CRISP may add Permitted Purposes according to the process set forth in the Participation Agreement.

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 Clinical Committee before their incorporation into a Permitted Purpose.

With the approval of the applicable Committee, specific use cases 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 provided that the entity will be required to enter into a written agreement with CRISP that protects the interests of CRISP and its Participants, the integrity of the CRISP Services, and the appropriate use of the information to be provided to the entity.

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 non-Participants will be independently vetted to ensure the request is legal and appropriate. CRISP will not release any protected health information to anyone for commercial, private, or other reasons that are not related to the Permitted Purposes.

Use Cases

For all Permitted Purposes except the treatment of an individual, to access Data, the categories of Permitted Purposes must be further explained and specified through use cases before the Data may be accessed or used through the CRISP Services in that manner. The use cases are approved by the Clinical Committee, which may create specialized subcommittees to review certain use cases. All approved use cases are available on the CRISP website. If a Participant is interested in submitting a Use Case to the Clinical Committee, it should contact its applicable CRISP outreach resource.

Sensitive Data and Consent Management

If Applicable Law protects Data such that it cannot be released without the affirmative consent of the patient (e.g., Data covered by 42 CFR Part 2), the Data may not be used for any of the Permitted Purposes unless and until an authorized person enters the required consent of the patient. Data that do not require affirmative consent or authorization under Applicable Law may be accessed for any Permitted Purpose.

Data contributors of Participants must refrain from sending certain sensitive health information, including but not 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 in accordance with Applicable Law. Participants are responsible for ensuring that their disclosure of information to CRISP complies with all Applicable Law. If a Participant believes it holds information that is subject to special protection under Applicable Law, the Participant must work with CRISP to determine: (1) whether the appropriate legal framework is in place for the disclosure to CRISP; and (2) whether it is technologically feasible for CRISP to manage access to and further disclosure of such information through the CRISP Services in a manner compliant with Applicable Law. If either of the forgoing are not in place

and/or feasible, the Participant must not share such information with CRISP and/or through the CRISP Services.

Accessing CRISP

A Participant can contribute and/or consume Data either via the CRISP Services or through a third-party EHR. The hardware and software requirements for access/use of the CRISP Services depend on the means an organization is using to contribute/consume Data and are the responsibility of the Participant.

Portal

Participant Users can access the CRISP Services in two ways. First, Participant Users may access via the online portal.

Single Sign-on

Participant Users can also access the CRISP Services through their EHR. CRISP connects to and exchanges Data with many EHR vendors; users must single sign-on to their EHR service to also authenticate to CRISP and access Data through the CRISP Services. Unlike access through the Portal, Participants monitor the Participant Users' access and authentication without additional CRISP requirements. Single Sign-on access to CRISP Services leverages the industry standards Substitutable Medical Apps and Reusable Technology ("SMART") on Fast Healthcare Interoperability Resources ("FHIR") and Security Assertion Markup Language ("SAML") 2.0. All launches require information identifying the unique user and organization launching the service in addition to specific patient identifiers.

Participants' Responsibilities

Onboarding and Testing

Participants and/or their technical partners 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 submission of a patient panel. CRISP communicates these requirements during the onboarding process. 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 its own testing policies and procedures. Following successful completion of Participant testing, Participants must provide confirmation to CRISP that they are ready to go live. Participants should notify CRISP prior to any system changes or updates.

Compliance with Applicable Law

Federal, State, and Local Privacy Laws

All Participants must, and must require Participant Users to, comply with Applicable Law, which includes federal, state, and local privacy laws. As noted above, Participants are responsible for complying with Applicable Laws, gaining necessary consent or authorization, and filtering information, as necessary. If a Participant believes it holds information that the Participant is prohibited by Applicable Law from sharing, that information must not be shared with or through CRISP.

Federal Information Blocking Prohibition

The 21st Century Cures Act and its implementing regulations prohibit certain individuals and entities from engaging in "information blocking." Information blocking is any practice—an action or inaction—by an

"actor" that interferes with access, exchange, or use of electronic health information ("EHI") unless that practice is required by applicable law or satisfies a public policy-based exception set forth in the regulations. Actors, under the information blocking regulations, include:

1. Healthcare providers;
2. Health Information Networks / Health Information Exchanges (HINs/HIEs); and
3. Developers or offerors of Certified Health Information Technology.

Compliance with the prohibition against information blocking is consistent with CRISP's mission and purpose, as a Health Information Exchange.

Part of CRISP's compliance obligations, as an HIE, include requiring that Participants meeting the definition of an actor also agree to comply with the prohibition against information blocking in their use of CRISP. For actor-Participants, the information blocking regulations are Applicable Law, and failure to comply with those regulations would constitute a breach of the Participation Agreement. CRISP will investigate allegations of information blocking by a Participant that involve the Participant's use (or non-use) of the HIE and will take appropriate action. All Participants must reasonably cooperate with such investigations, even if the Participant intends to assert that it is not an actor under the information blocking regulations.

More information regarding the information blocking regulations is available in the *Information Blocking Frequently Asked Questions* that have been developed by the Office of the National Coordinator for Health Information Technology ("ONC"), available here.

Disputes

The Participants acknowledge that it may be in their best interest to resolve disputes through an alternative dispute resolution process rather than through civil litigation. The Participants have reached this conclusion based upon the fact that the legal and factual issues involved in the Participation Agreement are unique, novel, and complex and limited case law exists that addresses the legal issues that could arise from the Participation Agreement. Therefore, the Participants will resolve disputes using the following process.

Referral to CRISP Executive Director

If a dispute arises between any Participant(s) under the Participation Agreement, including these Policies and Procedures, the Participants will first refer the dispute to the CRISP Executive Director. Within five (5) business days of request by the Executive Director, the Participants involved must designate a senior representative who has authority to take actions to resolve the dispute. The Executive Director will designate a time for the senior representatives to meet in an effort to resolve the dispute. If these representatives can agree upon a resolution to the dispute within thirty (30) days of the initial Executive Director meeting, including a plan and timeframe for implementing the resolution, the resolution will be documented by the Executive Director and will be considered a final resolution.

Mediation

If the Participants cannot resolve the dispute within thirty (30) days after the initial meeting between the Participants and the Executive Director, the Parties will attempt to resolve the dispute through mediation pursuant to the American Health Law Association ("AHLA") Rules of Procedure. The Parties will share the mediator's fee equally. The mediation will be held in Columbia, Maryland.

This mediation phase of the dispute resolution process will **not** apply if one of the Parties to the dispute is a governmental agency or authority that is prohibited from submitting to non-binding mediation.

Further Resolution

If the Participants cannot resolve the dispute through mediation, the Participants may pursue any legal remedies available.

Immediate Injunctive Relief

The dispute resolution process set forth above does not act to forestall any Participant from seeking immediate injunctive relief based on a good-faith determination that another Participant's actions or inactions are likely to cause irreparable harm to the Participant seeking such equitable relief. Provided, however, that a Participant seeking immediate injunctive relief against another Participant must inform the CRISP Executive Director within three (3) business days of: (i) filing for such relief; and (ii) the outcome of the action. No dispute that is pending before a court of competent jurisdiction will be subject to this dispute resolution process during such pendency.

Notice of Privacy Practices

Under Maryland regulation (Code of Maryland Regulations, 10.25.18.03(J)(3)(a)), Participants must make patients aware of the Participant's use of the CRISP Services, including notice through the Participant's Notice of Privacy Practices. For convenience, CRISP provides a sample update to the Notice of Privacy Practices that a Participant may use. During the onboarding process, Participants must attest that they have updated their Notice of Privacy Practices as required by Applicable Law.

Data Completeness

Participants, by electing to receive Data through CRISP Services, authorize CRISP to transmit results, reports, and other patient information directly from Participant's ancillary providers, such as clinical laboratories and radiology centers. Participants are responsible for the accuracy, quality, and completeness of the Data provided using the CRISP Services. Participants should transmit Data understanding that other Participants may use these Data for important decisions, including decision making for the treatment of patients. If Participants discover that they have submitted inaccurate or incomplete Data, they should immediately notify CRISP, by emailing privacyofficer@crisphealth.org, and cooperate with CRISP for appropriate remediation. Likewise, Participants must understand that CRISP cannot guarantee that the Data submitted to CRISP and made available through the CRISP services are complete and/or free from error.

Fees

CRISP charges appropriate and reasonable fees to Participants for use of the CRISP Services. As a not-for-profit organization, the fees reflect the necessary and reasonable costs to provide the CRISP Services, including technical infrastructure and operational costs, after subsidization provided through state and federal grants. CRISP does as much as possible to keep the CRISP Services accessible to any and all potential Participants. Fees increase each year in line with the Maryland Health Services Cost Review Commission update factor and fees are approved on a yearly basis by the CRISP Board. Participants may ask for the fee structure at any time.

Participants' Responsibilities for the Participant Users

Participant Access Policies for Participant Users

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 must be consistent with the Permitted Purposes in the Terms and Conditions and these Policies and Procedures and must 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 and its clinicians and other appropriate individuals. This authorized individual may also act as the designated point of contact for CRISP correspondence and user verification and updates as described above.

Participants are responsible for promptly informing CRISP when the job status or role of a Participant User within their organization has changed and affects the Participant User's access rights to the CRISP Services. If a Participant User is being terminated from a Participant, the Participant must inform CRISP of this termination within forty-eight (48) hours (excluding weekends and holidays), and prior to actual termination if at all possible. CRISP will terminate the Participant User's account upon notification of termination of employment from the respective Participant. Participants accessing the CRISP Services through third-party EHRs, via SSO/SAML, will be responsible for terminating access through that EHR for the terminated Participant User prior to or at the time of termination. However, Participants must still notify CRISP within 48 hours of the termination, so that CRISP can terminate access to other CRISP tools and services that are not accessed via SSO/SAML.

Minimum Necessary and Role-Based Access

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, however, 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 its Participant Users.

Misuse of System or Data

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 the privacy of personal health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of CRISP Services by Participant and its Participant Users. Any misuse of protected health information in connection with CRISP Services must be reported by Participant to CRISP as soon as discovered by emailing privacyofficer@crisphealth.org. Potential health information misuse will be investigated. CRISP will notify the privacy and / or 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 and/or to protect against further misuse. These actions may include, but are not limited to, suspension and/or termination of use by a Participant or Participant User(s).

Procedures for User Non-Compliance

In accordance with the Participation Agreement, each Participant must implement procedures to mitigate and deter misuse and issue appropriate sanctions to hold its Participant Users responsible for misuse of Data obtained when accessing protected health information through the CRISP Services. As applicable, procedures in place for the appropriate use of other health information systems may be leveraged for the use of Data through the CRISP Services.

Training

CRISP will make training resources available through its website, in addition to other training materials, as appropriate. Participants will be responsible for training their Participant Users on Data consumption in accordance with CRISP Policies and Procedures, the Participation Agreement, and Business Associate agreement, including through the dissemination of any necessary training provided by CRISP and the development and implementation of any additional, internal training needed to ensure appropriate use. If additional training is necessary as a result of system updates, CRISP will provide training through the website and inform Participants of the changes, and each Participant will then be responsible for training all of its Participant Users.

Usernames and Passwords

CRISP utilizes security-industry best practices for authenticating and authorizing user access to CRISP Services. Participants must ensure, in accordance with the Participation Agreement and associated Business Associate Agreement, that each Participant User has the appropriate access and is provisioned accordingly.

CRISP password requirements may differ across the CRISP Services, depending upon the unique characteristics of the tool/service and the Data made available therein. CRISP will communicate requirements as needed for each tool. Participant User passwords will expire every ninety (90) days, requiring that each Participant User creates a new password at that time. Password history settings are enforced.

Participant Users will be able to reset their own password using answers to the challenge questions set during initial login for the Portal. A user will be locked out of the system after five (5) consecutive failed log-in attempts. A Participant User must call the CRISP support desk directly at 1-877-952-7477 for assistance if the Participant User's account is locked, and the support desk will verify the Participant User's information and assist the Participant User in regaining access. Participant User accounts are automatically locked after ninety (90) consecutive days of inactivity. Participant Users not using SSO must have their accounts verified every ninety (90) days by the authorized administrator of the Participant.

HIE Administrators

Participants that are acting as consumers of Data are required to provide at least one, but preferably two, points of contact as "HIE Administrators" for the CRISP Services. The HIE Administrators are 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 HIE Administrators should notify CRISP if a user's employment at the organization has been terminated or if his or her functional role has changed, in accordance with these Policies and Procedures. This notification may be done either using the self-service HIE Admin Tool (recommended) or an email to support@crisphealth.org. HIE Administrators are also responsible for attesting to user identity verification and checking that users have completed all

necessary policy training prior to obtaining access to the CRISP Services, as well as for monitoring the general use and operations of the CRISP Services within their organization.

Auditing

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 healthcare 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 Participant Users' access to and use of the CRISP Services and may take action against any misuse by a Participant User, including suspension and/or termination of CRISP Services access. CRISP uses a privacy tool for additional monitoring of all user activities around access to protected health information to ensure all provisioned accounts are being used appropriately and to protect the privacy and security of protected health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of CRISP Services by the Participant and its Participant Users.

System Operations

Standards

CRISP aims to support and maintain the CRISP Services in a standards-compliant manner and, when possible and appropriate, will use best practices and generally accepted standards that are recognized by state, federal, and/or industry authorities.

Availability and Network Monitoring

CRISP Services are monitored continuously by CRISP and/or third-party vendors. 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 an admission, discharge, or transfer ("ADT") message from the supplying Participant. For each calendar year, scheduled hardware, software, and communications maintenance will 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 the applicable vendor to all Participants via e-mail or other electronic method, such as the website. In the event of unexpected downtime, CRISP will provide notifications to Participants via e-mail or other electronic method, such as the CRISP Portal or CRISP website.

Maintenance

Participants will be required to provide support contact information to CRISP. Participant support staff will be expected to assist with matters related to on-going training, master patient index ("MPI") administration, Data quality, system upgrades and downtime, and privacy and security matters.

Support

With the exception of help desk staffing, CRISP is closed on the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- Memorial Day
- Juneteenth

- Independence Day
- Labor Day
- Thanksgiving Day
- Christmas Day

Implementation Support

CRISP makes available the following implementation support 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; and
- Ensure access to CRISP Services as appropriate.

Operations Support

CRISP makes available the following operational support services 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 using an alternate recovery site, as needed in the event of a catastrophic failure of the primary production site location;
- Maintain uptime of services;
- Maintain datasets (e.g., authorized users) with Data supplied by CRISP or Participant; and
- Support Participant's periodic reconciliation of notification and claims-based encounter information.

User and Technical Support

CRISP offers Participants technical support to respond to technical problems, including support for test and production environments. CRISP technical support personnel can be reached at support@crisphealth.org or 1-877-952-7477. CRISP support uses a ticket logging system that documents and enables triage based on issue severity. 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 a 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.

Patient Rights and Individual Access

Opting Out of CRISP

Unless otherwise required by Applicable Law, CRISP's default patient consent policy is an opt-out model. A patient must proactively, and explicitly, register an opt-out with CRISP for their data not to be exchanged through CRISP except as required by law. 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, unless exceptions in Applicable Law apply. For example, opt-out does **not** limit the following through the CRISP Services:

- Point-to-point secure messaging (results and referrals). For example, if a primary care physician orders a lab test from a national laboratory, the result for that order will still be electronically delivered to the ordering provider. However, the result will not be available to other physicians who query the exchange.
- Any state-mandated program that CRISP facilitates through our technology, such as the Prescription Drug Monitoring Program or public health reportable conditions.

Patient opt out is centrally managed by CRISP. However, it is the Participant's responsibility to adequately educate patients on the opt-out process and to ensure that its Notice of Privacy Practices is updated accordingly. Patients may 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 effective 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 CRISP at any time, but patient data may have been deleted at the time the opt-out went into effect.

Accountings of Disclosures

Patients may request an accounting of disclosures from CRISP that shows Participating Users' access to and disclosure of the patient's information through the CRISP Services. Patients may obtain an accounting twice per year before being charged a reasonable, cost-based fee for preparing and providing an accounting. CRISP requires the accounting of disclosures request include the patient's first name, last name, date of birth, address, and a copy of an unexpired, government-issued, photo identification. Additional information may be required for requests submitted by an individual other than the patient, such as a parent or guardian.

Individual Access

Patient access is a Permitted Purpose. CRISP is actively working towards providing methods for patient information access. As these methods become available, CRISP will provide further information on the CRISP website regarding these methods and the Data available. In addition, CRISP will make available educational materials about best practices and methods for patients wishing to access their information, including privacy and security considerations associated with certain access methods or third-party connections. 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 regarding 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 health information will be directed to the healthcare provider who shared the information.

In some cases, due to legal and/or technical limitations, CRISP is not able to make Data available for certain patients. When these patients ask for access to their information, they will be directed back to the CRISP support team, who will encourage them to reach out to the appropriate provider(s) for more information.

Interstate Data Exchange

External HIEs

One of the main goals of CRISP is to ensure that health Data are where needed for clinicians and patients to make the best decisions, no matter where in the United States and territories a patient receives care. Therefore, CRISP has direct agreements with several neighbor states for robust Data sharing in areas patients in Maryland are most likely to seek care. In addition, CRISP participates in several National Networks; these National Networks electronically connect HIEs and more localized Health Information Networks (HINs) throughout the country. The National Networks provide a common framework for technology, as well as privacy and security standards. Currently, CRISP Participates in the following National Networks and interoperability frameworks:

- The eHealth Exchange network;
- The CommonWell network; and
- The Car*e*quality interoperability framework.

Each of these networks and frameworks has its own governing body, rules, and legal agreements, but how they work conceptually is the same. At this time, CRISP only shares Data with these networks for purposes of Treatment.

National Networks and TEFCA

The Trusted Exchange Framework and Common Agreement ("TEFCA") is a government-endorsed framework for the nation-wide exchange of health information that is intended to further connect existing National Networks. A goal of TEFCA is to make sure all the National Networks are connected so that no one needs to connect to multiple networks. CRISP plans to participate in TEFCA through the eHealth Exchange. Participants will be able to participate in TEFCA through CRISP, if they choose to do so, by executing an addendum to the Participation Agreement. More information on CRISP's planned participation in TEFCA, including FAQs, can be found on the CRISP website.

CSS Partners

By utilizing CSS, CRISP takes advantage of many economies of scale provided to it and other CSS HIE Partners, including Data storage and maintenance costs. CRISP's relationship with CSS requires CSS to ensure that CRISP Participant Data are handled securely and shared only in accordance with the Permitted Purposes. CRISP Participant Data may be shared with other CSS HIE Partners in accordance with Applicable Law and Permitted Purposes.

Reporting Privacy and Security Concerns

In the event that a Participant determines that any Data transmitted through CRISP Services have been requested, accessed, 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, Terms and Conditions, and/or the CRISP Policies and Procedures, the Participant must notify CRISP of the event within two (2) business days of the determination. Notification must include a detailed summary of the relevant facts.

The notification will be treated as Confidential Information, except as otherwise required pursuant to Applicable Law or as used or disclosed by CRISP in connection with the 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 under Applicable Law. The Participant must cooperate with CRISP as to any further investigation or responsive action reasonably requested or taken by CRISP to respond to the event.

In the event CRISP determines that any Participant Data transmitted through CRISP Services has been requested, accessed, 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 under HIPAA, CRISP will comply with the provisions of the Business Associate Agreement.

Requests for Data

Data Extracts

Along with the Data provided through the CRISP Services, Participants may ask for extracts of Data, provided the Participants have the appropriate access rights. A cost-based fee for compiling these Data may be assessed based on the necessary and reasonable costs to provide the Data, including technical infrastructure and operational costs. Participants may request such data by contacting CRISP by phone or email.

Business Associates of Covered Entities

Participants may also request Data be sent to their Business Associates by completing a form attesting to the relationship with the Business Associate and providing a point of contact. A cost-based fee for sending Data or establishing a Data feed to a Business Associate may be assessed based on the necessary and reasonable costs to provide the Data or establishing a Data feed, including technical infrastructure and operational costs. CRISP may also require the Business Associate to enter into an agreement regarding the type of connection and/or appropriate Data use.

Data Retention and Reuse

CRISP retains Data consistent with Applicable Law. Among other things, this retention allows CRISP to maintain an auditable history of each transaction through the CRISP Services.

Termination of Participation and Return or Destruction 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. Data that have been incorporated into a Participant's system of records prior to Participant termination may be retained as permitted by and in accordance with Applicable Law. Additionally, CRISP or Participant may retain one copy of the other's Confidential Information 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.

Policies and Procedures Amendment Process

CRISP reserves the right to make amendments to these Policies and Procedures, as permitted under the Participation Agreement. Notice of amendments may be provided by posting the amendment, along with its effective date, on the CRISP website at www.crisphealth.org, or through other means permitted under the Participation Agreement.

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 interested parties, which can advise CRISP as to the extent of hardship that may be experienced due to a proposed amendment.

Appendix – 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 Participant ("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: