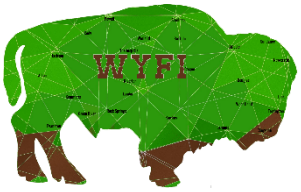

Wyoming Frontier Information (WYFI)

WYFI Policy & Procedure Manual

September 20, 2024

Version 9.0

WYFI **Policy and Procedure Manual** Revision History		
Version	Date	Notes
9.0	September 20, 2024	Updated due to the KPI Ninja Upgrade
8.0	March 14, 2024	Updated
7.0	February 21, 2023	Updated
6.0	April 17, 2020	Clean copy for LPPS approval
5.0	March 3, 2020	Revisions based on LPPS member feedback
4.0	October 22, 2019	Interim Review by Policy Committee ● Major revisions to align with neighboring HIE Participant Agreements and Policies and other Partner Agreements
3.0	March 11, 2019	Included Legal, Privacy, Policy, Security committee comments.
2.0	February 19, 2019	Version 2 with Wyoming Office of Privacy and Security comments.
1.0	December 19, 2018	Wyoming Frontier Information initial work up.

Policy & Standards

The WYFI Policy & Procedure Manual supplements the Wyoming Department of Health (WDH) privacy & security policies that can be found on the WDH website at:

https://health.wyo.gov/admin/privacy/wdh-privacy-security-policies/

Data Exchange Participants and Authorized Users are not legally WDH workforce members, but shall comply with WDH privacy & security policies when using the Data Exchange. These policies apply to entities participating in the Data Exchange.

***Derived from the Connecting for Health Common Framework**

Policy & Standards Table of Contents

1002 Monitoring and Audit Log Reviews
1003 Data Matching Process
1004 System Security
1005 Security Protocols

1100 DURSA
1200 Fees

Definitions

The meanings of the following terms shall be consistent throughout these policies and procedures (these "policies").

Authorized User (or "User") means an individual authorized by a Participant or the WYFI to use the Data Exchange for a Permitted Use as outlined in WYFI Policy and Procedure Manual.

Compliance Concern means a complaint from an Individual or Patient, security breaches or other concerns relating to compliance with a Participant Agreement or Authorized User Agreement, WYFI Policy and Procedure Manual, and applicable laws and regulations.

Data means protected health information, or information that identifies a patient that is used, stored, or exchanged between Participants and Authorized Users with the Data Exchange. Protected health information is defined by the Health Insurance Portability and Accountability Act (HIPAA).

Data Exchange means the system operated by the WYFI that allows Participants and Authorized Users to electronically use, store, or exchange Data.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

DURSA means the Data Use and Reciprocal Support Agreement.

Exchange Operations means activities that are necessary to run the Data Exchange and to support the core functions.

Individual means a person, generally a patient, who is the subject of the health information and has the same meaning as the term "Individual" in 45 C.F.R. § 160.103.

Patient means an individual who has received or will receive treatment for healthcare services from a Participant, Authorized User, authorized users of other health information exchanges, or whose records are stored in a public health registry.

Participant means an entity that has entered into a Participant Agreement with WYFI to use the Data Exchange. Participants contribute their Patients' Data to the Data Exchange.

Re-disclosure is the act of sharing or releasing health information that was received from another source (e.g., external facility or provider) and made a part of a patient's health record or the Participant's designated record set.

Site Administrator means the Participant's workforce member assigned to enroll and maintain the Participant's Authorized Users.

Wyoming Department of Health (WDH) privacy & security policies are available on-line and can be located at https://health.wyo.gov/admin/privacy/wdh-privacy-security-policies/

Connecting Principles

1. **Openness and Transparency.** Openness about developments, procedures, policies, technology and practices with respect to the treatment of personal health data is essential to protecting privacy. Individuals should be able to understand what information exists about them, how that information is used, and how they can exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence in individuals with regard to data privacy, which in turn can help increase participation in health data networks.

2. **Purpose Specification and Minimization.** Data must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

3. **Collection Limitation.** Personal health information should be obtained only by fair and lawful means and, if applicable, with the knowledge and consent of the pertinent individual. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected because electronic collection methods may be confusing to average users. Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method.

4. **Use Limitation.** The use and disclosure of health information should be limited to those purposes specified by the data recipient. Certain expectations such as law enforcement or security may warrant reuse of data for other purposes. However, when data is used for purposes other than those originally specified, prior de-identification of the data can help protect individual privacy while enabling important benefits to be derived from the information.

5. **Individual Participation and Control.** Every individual should retain the right to request and receive in a timely and intelligible manner information regarding who has that individual's health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend such personal information. Because individuals have a vital stake in their own personal health information, such rights enable them to be participants in the collection and use of their data. Individual participation promotes data quality, privacy and confidence in privacy practices.

6. **Data Integrity and Quality.** Health data should be accurate, complete, relevant, and up-to-date to ensure its usefulness. The quality of health care depends on the existence of accurate health information. Moreover, individuals can be adversely affected by inaccurate health information in other arenas like insurance and employment. Thus, the integrity of health data must be maintained and individuals must be permitted to view information about them and amend such health information so that it is accurate and complete.

7. **Security Safeguards and Controls.** Security safeguards are essential to privacy protection because they help protect data loss, corruption, unauthorized use, modification and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Design and implementation of various technical security precautions such as identity management tools, data scrubbing, and hashing, auditing, authenticating and other tools can strengthen information privacy.

8. **Accountability and Oversight.** Privacy protections have little weight if privacy violators are not held accountable for compliance failures. Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by holding accountable those who violate privacy requirements and identifying and correcting weaknesses in their security systems.

9. **Remedies.** The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization's commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

Category 100: Compliance with Law and Policy

Privacy Principles: Openness and Transparency; Data Integrity and Quality; Accountability and Oversight; Remedies.

Purpose: Policies to establish comprehensive privacy protection, compliance, enforcement procedures, and remedies following violations are crucial to maintaining health information privacy. This policy category recognizes that formal promulgation of internal policies and procedures which require that Participants and Authorized Users comply with applicable law is an indispensable feature of essential privacy protections. When there is a conflict between WYFI policies and Participant or Authorized User policies, the policy that is most protective of individual privacy should govern decision making. This is designed to make clear that these policies provide a floor and that Participants may choose to enhance privacy protections when appropriate. This deference to more protective policies echoes the federal pre-emption requirements of HIPAA.

The requirement that Participants and Authorized Users develop internal policies will help implement the principles of sound data management practices and accountability as well as ensure that decisions affecting individuals' privacy interests are made thoughtfully, rather than on an ad hoc basis. Written documentation of such policies facilitates the training of personnel who will handle health information and enhances the accountability of Participants and Authorized Users. Finally, the existence of internal policies for compliance by Participants and Authorized Users with applicable law creates transparency surrounding the handling and safeguarding of data by entities participating in the Data Exchange.

Policies

101. Compliance with Laws and Regulations
102. Compliance with WYFI Policies
103. Compliance with Participant Policies

Policy 101: Compliance with Laws and Regulations

101. Each Participant or Authorized User shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participant or Authorized User shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure constant and consistent compliance with all applicable laws and regulations.

Policy 102: Compliance with WYFI Policies

102. Each Participant or Authorized User shall, at all times, comply with all applicable WYFI policies, which may be revised and updated from time to time upon reasonable written notice to Participants and Authorized Users. Each Participant or Authorized User is responsible for ensuring it has a copy of and is in compliance with the most recent version of these policies. Each Participant or Authorized User shall reasonably cooperate with WYFI on issues related to the WYFI Participant Agreement and these policies; transact Message Content only for a Permitted Purpose; use Message Content received from another Participant or Participant User in accordance with the terms and conditions of this Agreement; as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant; and refrain from disclosing to any other person any passwords or other security measures issued to the Participant

User by the Participant.

Policy 103: Compliance with Participant Policies

103. Each Participant or Authorized User is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and regulations and with WYFI policies. In the event of a conflict between WYFI policies and a Participant or Authorized User's own policies and procedures, the Participant or Authorized User shall comply with the policy that is more protective of individual privacy and security.

    To ensure the Participant or Authorized User is in compliance with WYFI policies, WYFI may, on a periodic basis, require Participants to provide information regarding Participant's policies, procedures, Authorized Users, or work environments for audit or review purposes.

Category 200: Notice of Privacy Practices and Individuals' Right to Opt-out

Principles: Openness and Transparency; Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control.

Purpose: These policies incorporate HIPAA requirements obligating entities to provide a notice of the privacy practices to individuals upon request.

Policies

201. Content of the Notice of Privacy Practices
202. Provision of the Privacy Notice to Individuals
203. Individual Acknowledgement of the Privacy Notice
204. Opt-out Procedure
205. Opt-in Procedure

Policy 201: Content of the Notice of Privacy Practices

201. Each Participant or Authorized User shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and with these policies. The Notice shall inform individuals of the entity's Data Exchange participation and use, and provide individuals the opportunity to opt-out using the procedure established by the WYFI. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule and comply with all applicable laws and regulations.

Policy 202: Provision of the Privacy Notice to Individuals

202. Each Participant or Authorized User shall have its own policies and procedures governing distribution of the Notice to individuals, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

    For Participants and Authorized Users that are health care providers, the Notice shall be:

    (i) Available to the public upon request
    (ii) Provided to a patient at the date of first service delivery
    (iii) Available at the institution

(iv) Posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.

Policy 203: Individual Acknowledgement of the Privacy Notice

203. Each Participant or Authorized User that is a health care provider shall make a good faith effort to obtain each individual's written acknowledgment of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgment of the Notice shall comply with all applicable laws and regulations. Each Participant or Authorized User shall have its own policies and procedures governing the process of obtaining an acknowledgment, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

Policy 204: Opt-out Procedure

204. Pursuant to 42 C.F.R. 164.522, individuals have the right to request that their health information not be shared through the Data Exchange. Each Participant or Authorized User will provide notice to individuals of this right and upon request, provide a copy of the opt-out form to individuals. Participants and Authorized Users shall send completed opt-out forms to WYFI. WYFI shall process the individual's request and notify the Participant or Authorized User. The Participant or Authorized User will notify the individual upon completion of the opt-out procedure. An individual's choice to not share information through the Data Exchange shall apply to information sharing through the Wyoming Frontier Information System platform. Certain information pertinent under law to be shared regardless of opt-out (e.g., simple results delivery to Participants with which the Individual has an established relationship; lab results), or exchanges of Patient Information among Participants with which the Individual has an established relationship, also known as Direct Exchange, may still take place through the Data Exchange.

An individual may submit their opt-out request directly to the WYFI.

Policy 205: Opt-in Procedure

205. If an Individual decides that they want to opt back into WYFI after they have opted-out, an Opt-In consent form will need to be completed and signed by the Individual. Participants and Authorized Users shall send completed Opt-In forms to WYFI. WYFI shall process the individual request and notify the Participant or Authorized User. The Participant or Authorized User will notify the individual upon completion of the opt-in procedure. Any individual may submit their opt-in request directly to WYFI. In these instances, the WYFI will notify the individual directly of completion.

Category 300: Uses and disclosures of Health Information

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight.

Purpose: These policies integrate the general premise of HIPAA that health information may be used

only for permissible purposes and its more specific requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose. In general, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA, will be permitted following the minimum necessary requirements. Furthermore, subject to certain limitations, and under certain circumstances, requesting disclosure of and using health information for law enforcement, disaster relief, research, and public health purposes also may be permissible. Under no circumstances may health information be accessed or used for discriminatory purposes.

Requiring consideration of the purpose of a use and minimization of the use of information reduces the likelihood of inadvertent or intentional misuses of information. By ensuring that Participants and Authorized Users have legally required documentation prior to the use or disclosure of information, these policies help enhance the fair and legal collection and use of data, the oversight of data use and accountability for privacy violations. In addition, the integration of HIPAA's accounting of disclosures and individual access to information requirements allows individuals to understand how health information about them is shared and to exercise certain rights regarding information about them.

These policies also require security measures essential to identify and remedy loss, unauthorized access, destruction, use, modification, or disclosure of personal health information. Entities should implement policies to prevent security violations, assess security risks, and examine data storage and access technology. To prevent unauthorized access of information and maintain data integrity and quality, the authentication provision of this policy requires that both the identity and authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy Rule and Security Rule.

In order to provide Participants the ability to request health information through the Data Exchange from facilities located outside of the State of Wyoming, WYFI may enter into Participant Agreements ("Affiliated Agreements") that enable health information exchange across other communities, states or regions. Some of these exchanges may be parties to the Data Use and Reciprocal Support Agreement (DURSA). The DURSA is a legal, multi-party trust agreement that is entered into voluntarily by all entities, organizations, and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services, and policies developed in coordination with the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services (HHS). Though WYFI may not directly join the DURSA, Participants of WYFI may be required to adhere to DURSA Policies when requesting health information through the Data Exchange on patients treated outside state borders. DURSA policies are publicly available.

When entering into Affiliated Agreements with Health Information Exchanges (HIEs) or other healthcare organizations, WYFI shall ensure that the Policies and Procedures, Participants Agreement and other agreements are at least as protective of Patient Information as specified in these WYFI Policies and Procedures, Participant Agreement(s), and any other applicable agreements.

By entering into Affiliated Agreements, it is WYFI's intent to provide additional Patient Data to Participants and Authorized Users from outside the State of Wyoming which may otherwise be unavailable. In no case shall Participants or Authorized Users use such Data in a manner to avoid supporting the Health Information Exchange infrastructure in the geographic area served by those exchanges.

The combination of these policies' use and security provisions helps guarantee that health information is used and accessed only as authorized and that Participants and Authorized Users have proper measures in place to identify and address privacy violations.

Policies

Policy 301: Disclosure Compliance with Laws and Regulations

301. All disclosures of health information through the Data Exchange and the use of information obtained from the Data Exchange shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting Participant or Authorized User shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing Participant.

Policy 302: Permissible Purpose Required for Use or Disclosure

302. A Participant or Authorized User may request health information through the Data Exchange only for purposes permitted by applicable law. Each Participant or Authorized User shall provide or request health information through the Data Exchange only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations, and by these policies. Individually identifiable information may not be requested for marketing or marketing related purposes, or for research purposes. Regardless of whether permitted by Law, information may not be requested for 1) any Marketing purposes; 2) any Fundraising purposes; 3) any Health Insurance Underwriting purpose; or 4) for any decisions related to health insurance enrollment and eligibility except as permitted pursuant to an agreement executed between WYFI and a Government Agency Participant. If the Participant is neither a Covered Entity, a Business Associate nor a Governmental Participant, the Participant shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations as if it were acting in the capacity of a Covered Entity. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through the Data Exchange. No Participant or Authorized User may use the Data Exchange to perform comparative studies/analysis or data aggregation without written consent from the Participant owning such data.

    Participants and Authorized Users acknowledge that the data transacted through the Data Exchange may not include the Patient's full and complete medical record or history. Data transacted through the Data Exchange is not a substitute for the professional judgment of a Health Care Provider or for the proper treatment of a patient. Participants and Authorized Users acknowledge that they are responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for his/her/its respective patients.

Policy 303: WYFI Uses and Disclosures for Exchange Operations

303. WYFI may use analysis summary information that has been de-identified to no longer meet the definition of protected health information. This type of reporting has been summarized on a statewide basis (all WYFI reporting entities) or summarized as per provider with no individually identifiable information (for benchmarking and comparisons between providers). For example, if a provider had 100 individuals requiring diabetes testing, and 50% of individuals received this testing, this summary metric would be reported, but would not include a specific list or details on individuals requiring diabetes testing. If a provider requires specific information on one client, that information is available using the normal Continuity of Care Document (CCD) and Consolidated-Clinical Data Architecture (CCD-A) processes inherent in the Data Exchange as a health information exchange and those functions do not need to be supported through reporting. Summary benchmark data will only be available to the specific provider versus the Data Exchange statewide average, and to WDH employees for public health activities as authorized by law. When detailed information is required for reporting, the WYFI will de-identify the Data using the Safe Harbor Method allowed by 45 CFR §164.514(b). WYFI will not use the expert determination.

Policy 304: Disclosure Compliance with WYFI Policies

304. Uses and disclosures shall comply with all WYFI policies, including, but not limited to, WYFI Minimum Necessary Use of Health Information (500s).

Policy 305: Disclosure Compliance with Participant and Authorized User Policies

305. Each Participant or Authorized User shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and the documentation that shall be obtained, if any, prior to making such disclosures.

Policy 306: Accounting of Disclosures

306. Each Participant or Authorized User disclosing health information through the Data Exchange shall document the purposes for which such disclosures are made, as provided by the requesting entity, and any other information that may be necessary for compliance with the disclosure requirements of the HIPAA Privacy Rule. Each Participant or Authorized User is responsible for ensuring its compliance with such requirements and may choose to provide Individuals with more information in the accounting than is required. Each requesting Participant or Authorized User shall provide information required within thirty (30) days for the disclosing entity to meet its obligations under the accounting of disclosures requirement of the HIPAA Privacy Rule.

Policy 307: Disclosure Audit Logs

307. The Data Exchange shall maintain an audit log documenting which Participants have posted information and which Participants and Authorized Users have received information. WYFI shall implement a system allowing patients to request and receive a listing of Participants who have posted and which Participants and Authorized Users have received information about them. Individual patient requests for audit information are exercised through the Participant.

Policy 308: Disclosure Authentication Requirements

308. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating Authorized Users within their entity that have access to information through the Data Exchange.

Policy 309: Disclosure Access Process

309. WYFI will provide individuals with a copy of their CCD upon receipt of a written request. Participants and Authorized Users will provide individuals with a copy of their health records maintained by the Participant or Authorized User.

Policy 310: Occurrence of a Health Information Breach

310. As set forth under HIPAA, notification to individuals is required if their health information has been breached. Breach is defined as the unauthorized acquisition, access, use or disclosure of protected health information. However, it is not a breach:
    - Where an unauthorized person who receives the health information cannot reasonably have been able to retain it;
    - If an unintentional acquisition, access or use occurs within the scope of employment or a professional relationship and the information does not go any further (i.e., it is not further acquired, accessed, used or disclosed); or
    - It is an inadvertent disclosure that occurs within a Participant facility, and the information does not go any further.

Only breaches of "unsecured" protected health information, as defined by 45 CFR § 164.402, trigger the notification requirement. In the event of a data breach, Participants, WYFI, and WYFI's System Provider will take appropriate steps to mitigate the impact of the breach and comply with all applicable federal, state, and local requirements in relation to the breach.

Policy 311: Identification of Compliance Concerns

311. WYFI will notify Participants and/or Authorized Users no later than seven (7) days following the discovery of a Compliance Concern, not classified as a breach. WYFI reserves the right to suspend Participants and Authorized Users, including Site Administrators, for Compliance Concerns and may do so at its sole discretion in order to protect the Data and other Participants and Authorized Users.

Category 400: Information Subject to Special Protection

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies facilitate individualized privacy protections by requiring Participants and Authorized Users to heed any special protections of specific information types as set forth under applicable laws or regulations. In complying with these special protections, the collection, use and disclosure of health information by Participants and Authorized Users is limited to permitted purposes.

Moreover, in guaranteeing deference to the law or policy most protective of privacy, the provisions below echo the federal preemption requirements of HIPAA which defer to state laws that are more protective than the privacy provisions of HIPAA.

Policies

401. Information Subject to Special Protection

Policy 401: Information Subject to Special Protection

401. Some health information, such as information related to substance use, mental health, HIV/AIDS, or sexually transmitted diseases, may be subject to Federal or State law, e.g., 42 CFR Part 2, that may be stricter than the HIPAA Privacy Rule's use or disclosure requirements or standards. Each Participant or Authorized User shall be responsible for identifying and determining the applicable Federal or State law(s), and ensuring compliance with all applicable law prior to disclosing any information through the Data Exchange.

Category 500: Minimum Necessary

Principles: Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies incorporate the HIPAA requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose. These policies exempt treatment disclosures from this minimum necessary requirement to balance the protection of privacy with the provision of quality health care. In assessing the smallest amount of information that is necessary to accomplish a particular purpose, Participants and Authorized Users are less likely to collect, use or disclose information for an unauthorized purpose. Minimal collection, access, use and disclosure increases public confidence in the privacy practices of Participants and Authorized Users, enhances information privacy, and diminishes the potential for data corruption and security violations.

Policies

501. Minimum Necessary Use of Health Information
502. Minimum Necessary Disclosure of Health Information
503. Re-disclosure of Health Information
504. Minimum Necessary Health Information Requests

Category 501: Minimum Necessary Use of Health Information

501. Each Participant or Authorized User shall use only the minimum amount of health information obtained through the Data Exchange as is necessary for the specific purpose of such use. Each Participant or Authorized User shall share health information obtained through the Data Exchange, and shall allow access to such information by only those workforce members, agents, and contractors who need the specific information in connection with their job function or duties.

Policy 502: Minimum Necessary Disclosure of Health Information

502. Each Participant or Authorized User shall disclose through the Data Exchange only the minimum amount of health information as is necessary for the specific purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

Policy 503: Re-disclosure of Health Information

503. Participants may not re-disclose Patient Information accessed through the Data Exchange to other persons except for the purposes for which the Patient Information was accessed, or as required or permitted by Law.

Policy 504: Minimum Necessary Health Information Requests

504. Each Participant or Authorized User shall request only the minimum amount of health information through the Data Exchange as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by qualified health care providers for treatment purposes.

Policy 600: Workforce, Agents, and Contractors

Principles: Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints. Because Participants and Authorized Users are responsible for implementation of privacy practices, proper training is vital to ensure the legitimate use of health information and the prompt identification, reporting, and correction of any security vulnerability or privacy spill. Individual accountability in the form of sanctions for those persons responsible for privacy violations is fundamental to encouraging compliance with privacy practices. Without such incentive for compliance, privacy violations and security risks may go unchecked and lead to larger privacy problems.

Similarly, providing for the reporting of non-compliance enables Participants and Authorized Users to discover and correct privacy violations and identify and sanction privacy violators. These policies help guarantee the legitimate use of health data, the proper implementation of Participants' or Authorized Users' privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

Policies

601. Participant Access to the Data Exchange Services
602. Participant Training for Use of the Data Exchange Services
603. Participant Discipline for Non-Compliance
604. Participant Reporting of Non-Compliance
605. Suspended Access for Persistent Non-Compliance

Policy 601: Participant Access to the Data Exchange Services

601. Each Participant shall allow access to the Data Exchange only by those workforce members, agents, and contractors who have a legitimate, appropriate, and lawful need to use the Data Exchange and have been set up as Authorized Users. No workforce member, agent, or contractor shall be provided with access to the Data Exchange without first having been trained on these policies. Participants shall follow identification and authentication requirements as required by applicable laws and WYFI Policies or Procedures to verify the identity of Authorized Users granted access to the Data Exchange.

WYFI shall provide Authorized Users with Credentials and shall maintain a master list of all Authorized Users for whom such Credentials have been established. WYFI shall establish terms and conditions for log-in using WYFI supplied Credentials.

In addition to user level authentication, where applicable, the WYFI System will also authenticate the requesting organization using agreed upon technical standards at the time a request is made. To the extent technically feasible, WYFI shall support federated user authentication through the use of cross-enterprise secure transactions that contain sufficient identity information to make reasonable access control decisions and produce appropriate audit logs.

Each Participant shall designate at least one person as the Site Administrator, who must be recognized by WYFI as such, and will be the administrative point of contact to WYFI. Such individuals shall be responsible for ensuring compliance with any applicable agreements and these Policies.

Participants shall be responsible for updating their list of Authorized Users including the removal of any Authorized Users who no longer have a legitimate need to access the Data Exchange (i.e. change in role, termination, resignation).

Participant or Authorized User access may be blocked if WYFI becomes aware that the Patient Information they are contributing has been corrupted, compromised, or is otherwise in violation of the WYFI Participant Agreement, these Policies and Procedures, or other applicable agreements.

Policy 602: Participant Training for Use of the Data Exchange Services

602. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the Data Exchange to ensure compliance with these policies, and applicable laws and regulations. The training shall include a detailed review of applicable WYFI policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these policies.

Participants shall maintain documentation regarding their training program and acknowledgement processes in accordance with applicable laws and these Policies. Such documentation shall be provided to WYFI from time to time, as requested, for audit and review purposes.

Policy 603: Participant Discipline for Non-Compliance

603. WYFI maintains a zero-tolerance policy regarding inappropriate, unauthorized, or unlawful use of the Data Exchange. Each Participant shall implement clearly defined procedures to discipline and hold workforce members, agents, and contractors accountable to ensure that they do not use,

disclose, or request health information except as permitted by these policies and that they comply with these policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, and shall provide for retraining where appropriate.

Policy 604: Participant Reporting of Non-Compliance

604. Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with these policies to the Participant. Each Participant also shall establish a process for individuals whose health information is included in the RLS to report any non-compliance with these policies or concerns about improper disclosures of information about them.

Policy 605: Suspended Access for Persistent Non-Compliance

605. Each Participant shall be subject to denial of access to the Data Exchange if repeated efforts to train and discipline all workforce members, agents and contractors of that Participant result in persistent non- compliance with these policies. If, after completing a preliminary investigation WYFI determines that there is a substantial likelihood that a Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party, WYFI shall immediately suspend the Participant's Digital Credentials and provide a written summary of reasons for the suspension. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three (3) business days. If the Participant submits a plan of correction, WYFI shall, within five (5) business days, review and either accept or reject the plan of correction. If the plan of correction is accepted, WYFI shall, upon completion of the plan of correction, reinstate the Participant's Digital Credentials. If the plan of correction is rejected, the Participant's suspension will continue, during which time the WYFI and the Participant shall work in good faith to develop a plan of correction that is acceptable to both the Participant and the WYFI. In the event a Participant is in material default of the performance of a duty or obligation imposed upon it by the Participant Agreement or these Policies and such default has not been substantially cured within thirty (30) calendar days following receipt of the suspension notice, Participant may be subject to Termination for Cause as outlined in Section 12.20 (b) of the Participant Agreement.

Category 700: Amendment of Data

Principles: Openness and Transparency; Individual Participation and Control; Data Integrity and Quality; Accountability and Oversight.

Purpose: These policies integrate the right granted to Individuals by the HIPAA Privacy Rule to amend health information about them under certain circumstances. Accurate health information not only is indispensable to the delivery of healthcare, but is important to individuals' applications for insurance and employment and in a variety of other arenas. Allowing individuals to verify the accuracy and completeness of information concerning them contributes to the transparency of Participants' and Authorized Users' operations and fosters confidence in Participants' and Authorized Users' privacy practices and commitment to data accuracy. These policies will enable Participants and Authorized Users to more readily rely upon the integrity and quality of their health care data and more easily monitor, account for, and remedy systemic data inaccuracies, corruption, and other data deficiencies or privacy lapses.

Policies

701. Amendment of Individual Data

Policy 701: Amendment of Individual Data

701. WYFI shall not make changes to Patient Records. If an individual makes a request directly to WYFI that their information be amended, WYFI will refer that individual back to the Participant that contributed the information to the Data Exchange. Each Participant or Authorized User shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. If an individual requests, and the Participant or Authorized User accepts, an amendment to the health information about the individual, the Participant or Authorized User shall make reasonable efforts to inform other Participants or Authorized Users that accessed or received such information through the Data Exchange, within a reasonable time, if the recipient entity may have relied or could foreseeably rely on the information to the detriment of the individual. Participants making amendments may access or, if necessary, request an accounting of disclosures from WYFI for the purpose of notifying other Participants, as may be required to comply with the HIPAA rules.

Category 800: Requests for Restrictions

Principles: Use Limitation; Individual Participation and Control; Accountability and Oversight.

Purpose: These policies require Participants who agree to individual requests for restrictions in accordance with the HIPAA Privacy Rule to comply with such requests with regard to the release of information from the Data Exchange. Such compliance ensures permissible use of health information and accountability on the part of Participants who agree to individually requested use restrictions. Without the ability to request restrictions and without assurance that Participants will honor these agreed-upon restrictions, Individuals may remain silent about important information that could affect their health. By creating confidence in Participants and their privacy protections and encouraging individual participation, these policies foster dialog between individuals and Participants, thereby reinforcing traditional standards of confidentiality between a patient and their health care provider. Effective communication between a provider and a patient improves the overall delivery of health care.

Policies

801. Individual Requests for Restrictions

Policy 801: Individual Requests for Restrictions

801. If a Participant agrees to an Individual's request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information. If an agreed-upon restriction will or could affect the requesting agency's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting (or referred to) entity of the fact that certain information has been restricted, without disclosing the content of any such restriction.

Category 900: Mitigation

Principles: Openness and Transparency; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA requirement that entities have procedures and take breach steps to mitigate harm resulting from an impermissible use or disclosure of health information. Without the duty to mitigate harm from privacy violations, Participants may not promptly address data security weaknesses or breaches which could lead to greater privacy lapses in the future, diminish the confidence that Individuals have in Participants' privacy practices, and compromise the accuracy, integrity, and quality of Participants' data. Remedial action and mitigation are essential both to reassure individuals that Participants are vigilant in addressing privacy violations and ameliorating any harm from such violations and to help Participants ensure that their data oversight practices and security measures are functioning and effective.

Policies

901. Appropriate Remedial Action
902. Breach Notification

Policy 901: Appropriate Remedial Action

901. Each Participant or Authorized User shall recognize, mitigate and take appropriate remedial action, to the extent practicable, in response to any harmful effect that is known to the institution of a use or disclosure of health information through the Data Exchange in violation of applicable laws and/or regulations and/or these WYFI policies by the entity, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participant notification to the Individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

Policy 902: Breach Notification

902. Breaches of unsecured protected health information trigger the Breach Notification requirements under HIPAA. Participants must provide notice to WYFI as soon as reasonably practicable following the discovery of the breach, but no later than within five (5) business days after discovering that a breach occurred. Public Notice and notification to the Individual(s) impacted must be afforded no later than 60 days after the discovery of the breach. A breach is considered to be "discovered" when at least one employee of the Participant (other than the person responsible for the breach) knows, or reasonably should know, about the breach. Notice is required to be provided to media outlets if the information of more than 500 individuals is involved. Notice of all breaches must also be provided to the Secretary of the U.S. Department of Health and Human Services. This notice must be immediate if the breach involves the information of more than 500 individuals.

    These breach provisions do not expressly preempt any applicable State breach notification laws or regulations.

Category 1000: Security Safeguards

Principles: Security Safeguards and Controls; Data Integrity and Quality; Accountability and Oversight.

Purpose: These policies require security controls to avoid, detect, counteract, and minimize security risks. These controls protect the confidentiality, integrity and availability of information.

Policies

1001. Passwords
1002. Monitoring and Audit Log Reviews
1003. Data Matching Process
1004. System Security
1005. Security Protocols

Policy 1001: Passwords

1001. Passwords must be regarded as sensitive and confidential, and never revealed to anyone. Participants and Authorized Users shall change their password every 60 days. All passwords shall meet the "strong password" criteria comprised of at least one upper case letter, one lower case letter, one number, and one punctuation or other special character. Passwords may not be common dictionary terms or personal information (e.g., names of pets or family members). Participants and Authorized Users shall immediately report any suspected compromise of a User's account or password to WYFI.

Policy 1002: Monitoring and Audit Log Reviews

1002. WYFI shall track the date and time of activity; origin of activity; identification of user performing activity; description and monitor account use; start and stop times; failed authentication attempts; general log-in activity; password change activity; and data modification. Audit log reviews shall be conducted on a regular basis; examine user login information, including login successes and failures; examine whether security incidents were reported and proper follow-up was performed; and examine whether WYFI policies are being followed. Audit logs shall be protected against unauthorized access, modifications, and deletion. System activity review documentations shall be retained for six years and in accordance with WDH Documentation and Retention Policy.

Participants shall monitor and ensure all user access lists are current and all unauthorized user access has been removed.

Participants and Site Administrator may request audit or review of specific Authorized User activities and receive associated documentation of such activity.

Policy 1003: Data Matching Process

1003. WYFI shall establish a Master Patient Index (MPI) of specific demographic data with associated systematic links between the records to facilitate access to the information in the Data Exchange. WYFI shall protect the Patient Information stored in the MPI in accordance with all applicable Laws and WYFI policies. WYFI shall use a computer-based configurable algorithm to assist in linking records in the MPI that pertain to the same Patient when receiving Patient Records from Participants. WYFI will build, maintain, and as appropriate, share with Participants reports to review ambiguous or potentially duplicate

records submitted by Participants. When WYFI provides feedback to a specific Participant, that Participant shall use all reasonable efforts to research the situation(s) in a timely manner and respond with the results of its internal review and analysis. Participants agree to conduct quality improvement efforts to minimize, avoid and correct potentially ambiguous or duplicative data submissions.

An Authorized User shall query the MPI and view Patient demographic information only in accordance with these WYFI Policies. If the Participant does not have an established clinical relationship with the Patient, the Authorized User may be required to take additional actions to access Patient Information. Participants that are not health care providers shall only be given access to Patient Information that has been specifically authorized by agreement with WYFI. Health Plan Participants may only access Patient Information pertaining to individuals with whom they have a current relationship, defined by the Participant Agreements, other applicable agreement(s), and applicable Laws.

Participants shall report search results that indicate an incorrect Patient match has occurred to WYFI as soon as possible. WYFI will review these instances and take appropriate action.

If an Authorized User recognizes that Patient Information received from WYFI does not apply to the Patient about whom information was requested, the Authorized User shall take reasonable steps to immediately destroy the Patient information received, including properly disposing of any paper or electronic copies. The Authorized User shall contact WYFI, or the appropriate Site Administrator who shall alert WYFI to the occurrence. WYFI shall maintain records, including audit logs, as required by these Policies and Law, and will follow its breach response procedures, as appropriate.

Policy 1004: System Security

1004. WYFI and its System Providers shall maintain industry standards for security in the course of implementing and maintaining its hardware and software services that support the Data Exchange.

Policy 1005: Security Protocols

1005a. WYFI, its System Providers, and Participants shall only allow Authorized Users and WYFI System operations personnel to access the Data Exchange from secured end user environments. For more detailed technical security specifications see WDH Policies: S-010 Physical Security, S-011 Facility Access Control, S-015 Information Access Control, Policy S005d Password Use and Management.

1005b. Patient Information or the transmission of Patient Information submitted to, managed, or delivered by the Data Exchange shall be encrypted and secured in accordance with WDH Policy S-019 Electronic Transmission Security.

1005c. WYFI, its System Providers, and Participants shall employ security controls for all media and devices according to WDH Policy PSC-4002 (formerly S-014) Electronic Media and Device Controls Policy.

1005d. Unless specifically authorized, WYFI, its System Providers, and Participants shall not modify or enrich any Patient Information in compliance with WDH Policy S-017 Integrity. WYFI will employ technical methods, in compliance with applicable Laws, to prevent unauthorized modification of Patient Information while in transmission and at rest on the Data Exchange. WYFI may enrich or modify Patient Information to support patient matching functions (See Policy 1003 Data Matching Process).

1005e. Participants shall periodically conduct a risk analysis in accordance with the requirements outlined in WDH Policy S-001a Risk Analysis and Management.

1005f. All Participants, whether or not they are HIPAA Covered Entities must comply with all regulations and laws enforcing and related to enforcement of HIPAA and the HITECH Act both on the Federal and State level, and are subject to additional review of their HIPAA compliant policies and procedures by WYFI.

1005g. Participants acknowledge that the Transaction of Data between Members is to be provided over various facilities and communications lines, and information shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Members' control. Provided a Member uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this Agreement and the Collaborative Policies and Procedures, the Members assume no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted over those carrier lines, which are beyond the Members' control, or any delay, failure, interruption, interception, loss, transmission, or corruption of any Data or other information attributable to transmission over those carrier lines which are beyond the Members' control. Use of the carrier lines is solely at the Members' risk and is subject to all Applicable Law.

Category 1100: DURSA

Wyoming Frontier Information shall be a member of the eHealth Exchange. The eHealth Exchange is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through secure, trusted, and interoperable health information exchange.

Principals: Transact message content for a permitted purpose.

Purpose: Participants shall only Transact Message Content for a Permitted Purpose.

1100a. Public Health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e)

1100b. Recipients may retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient's record retention policies and procedures.

1100c. Participants hereby grant to WYFI the right to provide oversight, facilitation and support for the Participants who Transact Message Content with other Participants.

Category 1200: Fees

WYFI has adopted the Wyoming Department of Health (048), Wyoming Frontier Information Exchange Program rules, Chapter 1, Section 10(i) reference Number: 048.0074.1.09152022 (see https://rules.wyo.gov/) which authorizes the Department's collection of reasonable participation fees for connection and access to the Health Information Exchange.

Participants will receive information in reference to the process and an invoice displaying the amount of the fees that will be charged by the Department. The Department also has discretion over the waiving of fees when there is a Public Health Emergency or at its discretion.