Wyoming Department of Health

Privacy Impact Assessment

Wyoming Frontier Information (WYFI) Health Information Exchange

August 17, 2022

Program Contact:
Jesse Springer, Medicaid Technology and Business Operations Section Manager
Healthcare Financing, Technology and Business Operations Unit
307-777-8048

Project Manager:
Timothy Caswell, Health Information Technology Manager
307-777-5414

Note: This Privacy Impact Assessment is completed with minor modification in compliance with guidance documents provided by the U.S. Department of Homeland Security and meets the requirements of the e-Government Act of 2002.

Abstract

The Wyoming Department of Health, Division of Healthcare Financing – Medicaid is conducting this PIA to identify and mitigate risks to the privacy and security of the protected health information (PHI) maintained and transmitted through the WYFI Health Information Exchange system. This PIA serves as an update to the PIA published on March 24, 2020.

Overview

The WYFI contracted with Medicity, Inc., which has since been acquired by Health Catalyst, Inc. (HCI) for the design, development, and implementation of the Health Information Exchange. The software is owned by the Wyoming Department of Health, Division of Healthcare Financing – Medicaid. The purpose of the Health Information Exchange system is to allow a medical care team to share clinical information across institutions and practices, making patient information available wherever and whenever needed to provide high-quality, efficient care. The WYFI's mission is to promote a healthier Wyoming by developing a statewide secured, connected, and coordinated health information technology system that supports effective and efficient healthcare. Information that will be maintained in the Health Information Exchange includes clinical records from all data sources such as laboratory results, radiology reports, transcribed reports, medications, and clinical care summaries. The components of the Health Information Exchange system include the community health record, direct secure messaging, electronic results distribution, clinical event notifications, and analytics. The community health record provides access to a patient's clinical records from all the WYFI data sources. Direct secure messaging allows providers to electronically send and receive clinical information quickly and securely from one healthcare provider to another. Results from the WYFI data sources, including laboratory results and radiology reports, can be routed directly into the provider's certified Electronic Health Record (EHR) system through electronic results distribution. Clinical event notifications create alerts for patients who have been admitted, discharged, or transferred from community healthcare facilities. Under the authority granted in Wyoming Statute § 9-2-106(a)(vii), the WYFI promulgated rules to govern the establishment and operation of the Health Information Exchange by the WYFI. The Wyoming Frontier Health Information Exchange Rules, Chapter 1, establishes how data is used, stored, and exchanged between participants and authorized users.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The Health Information Exchange provides health records from the connected health care providers to authorized individuals for treatment, payment, and

healthcare operation purposes. At a minimum, the WYFI platform will support clinical data and interoperability standards, including but not limited to HL7 v2.x and 3.x, ADT, and C-CDA (XML), as well as Integrating the Healthcare Enterprise (IHE) standards. The Health Information Exchange queries the health records of connected EHRs to create a single health record, typically a CCD or CCDA. The Health Information Exchange maintains a copy of each CCD or C-CDA created by the system and a copy of each message transmitted by the system. The system is capable of performing data analysis on the health information maintained by the Health Information Exchange for approved purposes.

1.1.1 What personally identifiable information or protected health information is collected or stored in the system?

General Personal Data - Direct Identifiers	General Personal Data - Indirect Identifiers
Name: ☒	Date of Birth: ☒
Previous Name: ☒	Place of Birth: ☒
Alias/Preferred Name: ☐	Age: ☒
Address: ☒	Gender: ☒
Telephone Number: ☒	Race/Ethnicity: ☒
Email address: ☒	Component of Home Address (for example, city or county without specific street address): ☒
Other (specify):	Education Level: ☒
	Religion: ☒
	Military Service: ☒
	Physical Characteristics (weight, height, eye color): ☒
	Criminal History: ☐
	Other (specify):
Identifying Numbers	Distinguishing Features or Biometrics
Social Security: ☒	Fingerprints: ☐
Alien Registration: ☒	Palm prints: ☐
Tribal ID: ☒	Photos: ☐
Other state or federal ID: ☒	Voice recording: ☐
Financial Account(s): ☒	Scars, marks, tattoos: ☐
Driver's License: ☒	DNA profile: ☒
Vehicle Registration: ☐	Dental profile: ☒
VIN: ☐	Voice recording/signature: ☒
Employee ID: ☐	Other (specify):
Passport: ☒	
File/Case ID (issued by agency): ☒	

File/Case ID (issued by another agency or organization): ☒	
Credit card: ☐	
Patient or Medical Record ID: ☒	
Insurance Policy Number: ☒	
Other (specify):	
Work Related Information	Financial Information
Occupation: ☒	Tax returns (provided by individual) ☐
Employer: ☐	Tax information (from IRS) ☐
Job Title:☐	SSA/Disability information (provided by individual): ☒
Work Address:☐	SSA/Disability information (provided by SSA): ☒
Work Telephone:☐	Other benefit information (provided by individual): ☒
Work Email: ☐	Other benefit information (provided by issuing agency): ☒
Salary: ☐	Income verification (provided by individual): ☐
Work History: ☐	Income verification (provided by third party): ☒
Disciplinary History (for licensed professions): ☐	Credit information: ☐
Other (specify):	Insurance Information: ☒
	Other (specify):
Medical Information	Other Information
Medical History: ☒	Background Check: ☐
Medical Condition or Diagnosis: ☒	Credit Check (credit bureau): ☐
Medications: ☒	Other (specify):
Other (specify):	
Treatment Information: ☒	

1.1.2 What information does the system create?

The Health Information Exchange provides access to a consolidated, longitudinal health record for patients whose providers are connected and contributing data to the Health Information Exchange. Qualified and authorized users can query and view the system for information such as lab results, hospital Alert, Discharge, and Transfer (ADT) notifications, face sheets, treatment plans, and other data contributed to the system. For providers that have interfaces connected to the Health Information Exchange, these results can be delivered directly to the provider's EHR system. The system can also generate Continuity of Care Documents

(CCDs) which a provider can use to share patient information with other appropriate providers.

1.1.3 If the system receives information from another system, what information is returned to the system?

The Health Information Exchange receives health records/health information from various health care providers who connect their EHR system. EHR systems would receive back an acknowledgment (ACK) for transactions. It would be in the form of an HL7 or CCD/XML acknowledgment.

1.2 What are the sources of the information in the system?

The Health Information Exchange receives information from various healthcare providers who connect their Electronic Health Record systems to the Exchange and contribute their data. Currently, the entities and organizations that contribute data to the Health Information Exchange include:

Aspen Mountain Medical Center Campbell County Memorial Hospital Cheyenne Regional Medical Center Cody Regional Health Crook County Medical Services District Hot Springs Health Ivinson Memorial Hospital Johnson County Healthcare Center Memorial Hospital of Carbon County Memorial Hospital of Converse County Memorial Hospital of Sweetwater County Niobrara Community Hospital North Big Horn Hospital Platte County Memorial Hospital (Banner) Powell Valley Healthcare Star Valley Medical Center Summit Medical Center Torrington Community Hospital (Banner) Washakie Medical Center (Banner) Weston County Health Services Wyoming Medical Center (Banner)	Hospitals/ Critical Access Hospitals
Albany Community Health Center Arrowhead Family Medicine Healthworks Community Health Center of Central WY	Rural Health Clinic & Federally Qualified Health Center

Casper Family Residency Program CCMSD-Hulett Clinic CCMSD-Moorcroft Clinic CCMSD-Sundance Cheyenne Family Medicine Residency Program Cody Regional Rural Health Clinic Crossroads (Community Action of Laramie County) Dubois Medical Clinic Fremont County Pediatric Clinic Heritage Health Center, Greybull Clinic Heritage Health Center, Powell Clinic Lander Community Health Center - Pediatrics Laramie Peak Rural Health Clinic North Big Horn Hospital Clinic Oregon Trail Rural Health Clinic Rawhide Rural Health Clinic Register Cliffs Rural Health Center Riverton Community Health Center South Lincoln Medical Clinic Weston County Newcastle Clinic	
Cheyenne Regional Medical Group Cody Regional Health - Medical Clinics Star Valley Medical Clinics Campbell County Memorial Hospital Clinics Crook County Medical Services District Clinics Family Medical Center Clinics (Johnson County) Memorial Hospital of Carbon County Clinics Memorial Hospital of Converse County Clinics Memorial Hospital of Sweetwater County Clinics Hot Springs Health Clinics North Big Horn Hospital Clinics Powell Valley Healthcare Clinics Star Valley Medical Center Clinics Weston County Health Services Clinics Lander Medical Clinic Carol Fischer's Office Casper Childrens Center Laramie Pediatrics Sweetwater Pediatrics Health Medical Institute Paul Washburn MD Optimal Performance Medicine, LLC	Ambulatory Providers

Frontier Neurosciences Rocky Mountain Family Medicine Wyoming Medical Health Group	
WY Medicaid Health Management Vendor Telligan Colorado Regional Health Information Organization WY Medicaid System Integrater Utah Health Information Network South Dakota Health Link WY Dept of Corrections WY Medicaid Pharmacy Claims - Change Healthcare Public Health Nursing Offices WY Emergency Medical Services	Trading Partners

Entities or organizations that have access to query and view information, but do notcurrently contribute data to the Health Information Exchange include:

South Lincoln Hospital District Three Rivers Health	Hospitals/ Critical Access Hospitals
Banner Health Clinic Guernsey Banner Health Clinic Wheatland Glenrock Health Center	Rural Health Clinic & Federally Qualified Health Center
1st Choice Imaging 212 Degrees LLC A Child And Family Psychiatry, LLC A Woman's Place A+ Community Services ACM Therapy Group, LLC Affinity Case Management, LLC All About Independence Aspen Family Dental Associates in Therapy for Infants and Children B.A.C.A. Case Management Babson & Associates Primary Care, P.C. Banner Health Clinic Torrington Banner Health Clinic Worland Banner Imaging Associates of North Colorado Basin Vision Center Best Home Health and Hospice, LLC	Ambulatory Providers

Black Hills Orthopedic and Spine Center - Bowman, ND Black Hills Orthopedic and Spine Center - Chadron, NE Black Hills Orthopedic and Spine Center - Dickinson, ND Black Hills Orthopedic and Spine Center - Gillette, WY Black Hills Orthopedic and Spine Center - Hot Springs, SD Black Hills Orthopedic and Spine Center - Newcastle, WY Black Hills Orthopedic and Spine Center - Philip, SD Black Hills Orthopedic and Spine Center - Rapid City, SD Black Hills Orthopedic and Spine Center - Spearfish, SD Black Hills Orthopedic and Spine Center - The Spine Center Black Hills Orthopedic and Spine Center - Williston, ND Brant Audiology and Tinnitus Canyon Hand Therapy Casper Women's Care Cathedral Home for Children CDC+ Audiology/ Therapy Center for Surgical Excellence Cheyenne OB-GYN Cheyenne Women's Clinic, PC Christine Guelde City Drug Cloud Peak Chiropractic, P.C. Corner Stone Pharmacy Crossroads of Wyoming Recovery Davis ENT Specialists, PC Davis Home Health (Healing Hearts) Dean Bartholomew, MD Donor Alliance Downtown Clinic Eden Valley Telehealth Epsilon Health Solutions Forward Unity Fremont Counseling Fremont Wellness Education Center Frontier Access & Mobility Frontier Home Health and Hospice Fyzical Therapy and Balance Centers Glenrock Health Center Gottsche Rehab Center-Basin Gottsche Rehab Center-Cody	

Gottsche Rehab Center-Meeteetse Outreach Clinic Gottsche Rehab Center-Powell Gottsche Rehab Center-Shoshoni Gottsche Rehab Center-Thermopolis Gottsche Rehab Center-Worland Granite Rehab & Wellness Center HealthReach High Country Behavioral Health High Plains Vision Center Hospice of Sweetwater County Hospital Pharmacy West Laramie Reproductive Health Life Skills Wyoming Lion's Pride Care, LLC Medicap Pharmacy Meridian Psychological Mission at Castle Rock Rehabilitation Center Mountain West Speech Services Mud Springs Vision Clinic, LLC National Diabetes Prevention Program (DPP) New Beginnings Counseling North Star Pharmacy and Infusion Northeast Wyoming Pediatric Associates Orthopedic Urgent Care - Gillette Orthopedic Urgent Care of Rapid City Pain Care Center-Casper Pain Care Center-Evanston Pain Care Center-Jackson Pain Care Center-Lander Pain Care Center-Rock Springs Pain Consultants of the Rockies Pain Consultants of the Rockies, PC- Casper Palmer's Playhouse Pieper & Marsh Family Dentistry, pc Pivot Prosthetics and Orthotics, LLC Platte Valley Clinic Pole Mountain Pharmacy, LLC Popp Chiropractic & Rehabilitation P.C. Powell Vision Clinic Precision Prosthetics and Orthotics Premier Bone and Joint Casper Clinic	

Premier Bone and Joint Cheyenne Clinic Premier Bone and Joint Gillette Clinic Premier Bone and Joint Laramie Clinic Premier Bone and Joint Rawlins Clinic Premier Bone and Joint Riverton Clinic Premier Bone and Joint Rock Springs Clinic Premier Bone and Joint Torrington Clinic Professional Pathology of WY ProMotion Baken Park Quality Home Health Care Ramsey Eye Care Center Rising Sun Wellness Center Riverton Physician Practices Rocky Mountain Lions Eye Bank Seattle Children's Hospital-Psychiatry PAL Seitz Dermatology Sensational Kids Therapy, LLC Sheridan Health Center Smith Psychological Services Sternitzke Consulting Stitches Acute Care Centers Teton Orthopedics The Eye Clinic SurgiCenter The Eye Institute of Wyoming, PC UC Health University of WY-School of Pharmacy UW Education Health Center of Wyoming Volunteers of America Northern Rockies WDH-Dept of HCF, Developmental Disabilities Section WDH-Pharmacy Program WDH-Provider Oversight Western Sleep Medicine, LLC Willow Creek Counseling Associates Wind River Ear Nose and Throat Wind River Family and Community Health Worland Pharmacy Wyoming Eye Associates, LLC Wyoming Girls School Wyoming Life Resource Center Wyoming Medical Associates, LLC Wyoming Medical Billing Services LLC	

Wyoming Medication Donation Program Wyoming Otolaryngology, PC Wyoming Recovery	
Clareto Social Security Administration Aledade	Trading Partners

The Data Exchange is also a source of information as it creates a CCD / C-CDA from the information available on a specific individual in each connecting EMR.

1.3 Why is the information being collected, used, disseminated, or maintained?

The purpose of the Health Information Exchange is to allow a medical care team to share clinical information across institutions and practices, making patient information available wherever and whenever needed to provide the highest quality and most efficient care. The WYFI's mission is to promote a healthier Wyoming by developing a statewide secured, connected, and coordinated health information technology system that supports effective and efficient healthcare.

1.4 How is the information collected?

The healthcare organizations and entities contributing data to the Health Information Exchange make their clinical information available to other participants in the Exchange through electronic transmission utilizing interfaces connecting their EHR systems to the Health Information Exchange. Participants in Exchange can query, view, create and receive CCDs/C-CDAs from the information. Those CCDs/C-CDA are also maintained within the Health Information Exchange as part of the community health record. HL7 interfaces as well as CCD data makes up the patient's record in the Community Health Record (CHR).

1.5 How will the information be checked for accuracy?

The WYFI Policy and Procedure Manual (the Policy Manual) states that health data contributed to the Health Information Exchange should be accurate, complete, relevant, and up-to-date to ensure its usefulness. However, the Policy Manual also

states that the WYFI shall not make changes to the patient records contributed by the data contributors. It is the responsibility of the participants to ensure the data being contributed is accurate. Participants agree to maintain sufficient safeguards and procedures to ensure the security, privacy, and accuracy of the data. Participants and authorized users acknowledge that the data transacted through the Health Information Exchange may not include the patient's complete medical record or history, and data transacted through the Health Information Exchange is not a substitute for the professional judgment of a health care provider for the proper treatment of a patient.

Participants and authorized users acknowledge in the execution of the Participant Agreement that they are responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients. Each participant or authorized user is required to comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendments to their health information. If an individual requests an amendment to their health information and the participant or authorized user accepts, the participant or authorized user is required to make reasonable efforts to inform other participants or authorized users that accessed or received such information through the Health Information Exchange. The Health Information Exchange participants can access audit logs or, if necessary, request an accounting of disclosures from the WYFI to notify other participants as required by the HIPAA Privacy Rule's amendment of health information provisions.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Under the authority granted in Wyoming Statute § 9-2-106(a)(vii), the WYFI promulgated rules to govern the establishment and operation of the Health Information Exchange by the WYFI. The Wyoming Frontier Health Information Exchange Rules, Chapter 1, establishes how data is used, stored, and exchanged between participants and authorized users. The WYFI enters into a Participant Agreement with health care providers connecting their system, along with a Business Associate Agreement, which is required by the HIPAA Privacy Rule. The WYFI enters into End User Licensing Agreements (EULAs) with health care providers who are not providing data but using the system to receive data.

1.7 <u>Privacy Impact Analysis</u>: What privacy risks have been identified with the data collection and source of information? How were the risks mitigated?

As stated above, the WYFI Data Exchange system is supporting and working towards the vision of creating community-based virtual medical records and other clinical applications to promote a healthier Wyoming through a statewide secure, connected, and coordinated health IT system. The Data Exchange provides a platform for the sharing of virtual medical records for those purposes.

The WYFI assures secure access to patient data through the following security measures: Once new users are connected to the WYFI Health Information Exchange they are immediately trained on how to use the software. The training is web-based however, our training team is available to train on-site.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Participant Agreement permits the use of health information made available through the Health Information Exchange for the following purposes: (1) Uses for treatment, payment, and healthcare operations, as each is defined by HIPAA; (2) Any other use that is permitted or required under HIPAA, the WYFI Policy and Procedure Manual, or other applicable law governing the use and disclosure of Data; and (3) To facilitate the implementation of "meaningful use" criteria as required under the American Recovery and Reinvestment Act of 2009 and its related federal regulations, as permitted by HIPAA. Subject to certain limitations, and under certain circumstances as outlined in the Privacy Rule, other permitted disclosures include requesting disclosure of and using health information for law enforcement, disaster relief, research, and public health purposes. No participant or authorized user may use the Health Information Exchange to perform comparative studies/analysis or data aggregation without written consent from the participant owning such Data.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The Health Information Exchange allows a participant or authorized user to query data available in the network on a specific patient and aggregate that data into a consolidated view either through the Provider's EHR or over a web portal. The system matches patient data from the sending sources (data contributors) to create the aggregated view. Referrals management allows providers to send, receive, and track patient referrals and patient documentation across different healthcare settings. Electronic results distribution from Health Information Exchange data sources, including laboratory results and radiology reports, can be routed directly into the provider of record's certified EHR. For providers who do not have a certified EHR, the Exchange provides a local platform that enables sending and viewing of clinical results data. Clinical event notifications create alerts for patients who have been admitted, discharged, or transferred from community healthcare facilities. The consolidated view of the longitudinal health record of the patient can be aggregated and applied to standards-based, clinical documents such as C32 CCDs or C-CDAs. These new documents, once created, remain in the Exchange for future query and use by participants or authorized users for permitted purposes.

The system standardizes data to common structures and vocabularies for query and display. The data can then be classified into appropriate buckets for analysis.

2.2.1 Does the system create or make new or previously unutilized information about an individual? If yes, explain.

The WYFI has established a Master Patient Index (MPI) of specific demographic data with associated systematic links between the records to facilitate access to the information in the Health Information Exchange. The WYFI shall protect the patient information stored in the MPI per all applicable laws and the WYFI policies. The 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. The WYFI will build, maintain, and as appropriate, share with participants reports to review ambiguous or potentially duplicate records submitted by participants. When the WYFI provides feedback to a specific participant, that participant shall use all reasonable efforts to research the situation(s) promptly 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.

2.3 Does the system use commercial or publicly available data, or open-source software? If so, please identify the commercial or publicly available data, or open-source software and explain how it is used.

The Health Information Exchange does not use commercial or publicly available data at this time.

2.4 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Participants in the WYFI agree to allow access to the Health Information Exchange only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the Health Information Exchange and have been set up as authorized users. They also agree to ensure that no workforce member, agent, or contractor shall be provided with access to the Health Information Exchange without first having been trained on the WYFI policies. Participants agree to follow identification and authentication requirements as required by applicable laws and the WYFI Policies or Procedures and to verify the identity of authorized users granted to access the Health Information Exchange. In addition, participants agree to 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 the WYFI policies and that they comply with the policies. Finally, the WYFI maintains the authority to restrict access to or revoke privileges from participants or authorized users that are found

to violate the WYFI Participant Agreement, the WYFI Policies, and Procedures, or HIPAA requirements.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The WYFI retains Health Level Seven (HL7) clinical data. This includes patient records such as past medical history, medications, laboratory orders and results, progress notes, referrals, discharge summaries, radiology reports, patient insurer information, patient demographics, and other types of patient information available in providers' EHRs.

3.2 How long is information retained?

Data archiving requirements will meet Agency standards which are currently at a minimum of seven (7) years. Clinical data from Wyoming hospitals and private provider offices will be stored electronically in the Health Information Exchange.

3.3 Has the retention schedule met State and Federal requirements?

The current retention schedule meets the State and Federal requirements at a minimum of seven (7) years.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

No risks were identified.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Wyoming Department of Health.

4.1 Which WDH divisions, programs, or facilities is information from the software or information system shared or disclosed?

The WYFI plans to make multiple connections to internal systems within the Wyoming Department of Health. Participants will sign a Data Use agreement and will be held to the same standards as described above.

Connections may include connecting to Public Health Division for immunizations, electronic lab reporting, and exchange of data to disease registries. WYFI will have automated bio-surveillance which can include data submission triggered on

laboratory results values or scanning of laboratory results and routing of results of interest to local, regional, or state reporting and surveillance repositories. Incoming data will be registered and indexed in the clinical data repository based on patient matching rules.

Current WDH divisions, programs, or facilities:

WDH Division	Program or Facility
Healthcare Financing	Health Management
Healthcare Financing	Pharmacy
Healthcare Financing	Eligibility
Public Health	Public Health Nursing Offices
Public Health	Emergency Medical Services
Public Health	WY State Labs
Directors Office	Vital Statistic Services
Directors Office	WY Life Resource Center

4.1.1 What information is shared or disclosed internally, and for what purpose?

In most of the circumstances surrounding internal sharing, the interfaces will be uni-directional such as with certain laboratory results being scanned and routed to surveillance repositories or disease registries. In the case of immunizations, the Health Information Exchange may electronically route required reporting of immunizations on behalf of a Participant. These are all transactions and reporting currently required and accomplished through other, potentially less secure means, but which could be routed through the Health Information Exchange more securely and efficiently on behalf of the reporting Providers.

4.1.2 What authority does your division, program, or facility have to share or disclose the information internally? Does the receiving division, program, or facility have authority to receive, use, or disclose the information?

The authority granted in Wyoming Statute § 9-2-106(a)(vii) also applies to establishing these internal system connections.

4.2 How is the information accessed, transmitted, shared, or disclosed?

Electronic interfaces will be built between the Health Information Exchange and the data repositories or systems of the entities listed in 4.1 above. These interfaces function similarly to the interfaces built between the Health Information Exchange and hospitals or ambulatory provider groups contributing data to the Health Information Exchange.

4.2.1 What security measures safeguard its transmission?

The WYFI Policies require security controls to avoid, detect, counteract, and minimize security risks. These controls protect the confidentiality, integrity, and availability of the information in the Health Information Exchange. The WYFI Policies require participants to adhere to HIPAA and all applicable Laws regarding accessing, the permitted use of, secure transmission of, and storage of any shared data within the Health Information Exchange.

The WYFI maintains data encryption standards applicable to sensitive information including PHI/PII, log-in, or other credentials through AES-CBC (AES in Cipher Block Chaining mode) with a 128-bit key minimum, or triple DES (3DES-CBC) containers for data at rest. Whole disk encryption may also be employed for data at rest. TLS 1.2 or 1.3 for data in motion. Systems powering the WYFI and products employ encryption to data in motion and at rest.

The WYFI uses the following encryption to protect data transmitted over public networks:

• For data transmitted over our grid (Connect solution), all payloads are double encrypted once at the data level using 2048-bit symmetric encryption and a second time via the channel streamed over 128-bit encrypted SSL.

• The WYFI's Community Health Record and Organize solutions encrypt data transmissions using 128-bit TLS or SSL encryption. This included web-based access to results using our inbox (SSL encryption is used for all browser displays) and data transmitted via web services.

• The WYFI's encryption algorithms are compliant with FIPS 140-2/3 standards.

• User Access: The WYFI documents the granting and approval of access to client data. Users receive access based on their roles, which aligns user and client data for appropriate levels of access. De-provisioning, revocation, or modification of user access to the

systems, information assets, and data implemented is done in real-time (if possible) for changes in the status of employees, contractors, customers, business partners, or third parties. Any change in status, such as termination of employment, contract, or agreement, change of employment, or transfer within the organization, triggers reassessment of access privileges. The WYFI's applications support two-factor authentication methods built on standards that integrate into Internet Information Server (IIS).

• Encryption: The WYFI can create unique encryption keys for each client. We support client-generated encryption keys and permit clients to encrypt data to an identity without access to a public key certificate (e.g., Identity-based encryption). The WYFI encrypts client data at rest (on disk/storage) within the WYFI environment. We leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances and can manage encryption keys on behalf of the WYFI. To support the encryption capabilities, we maintain key management procedures.

• Vulnerability and Patch Management: the WYFI conducts application-layer, local operating system-layer, and network-layer vulnerability scans regularly as prescribed by industry best practices. Results of vulnerability scans are available at any request.

• Antivirus/Malicious Software: The WYFI has anti-malware programs installed on all systems, which support cloud service offerings.

In each of the Data Sharing Agreements that the WYFI has with internal WDH Divisions, there are these requirements.

The Disclosing Program confirms:

- The disclosure of protected health information is permitted under applicable state and federal law, including HIPAA.
- The disclosure includes only the minimum amount of protected health information necessary to accomplish the intended purpose.

The Disclosing Program shall:

- Notify the Receiving Program of any restriction on the use or disclosure of protected health information that the Disclosing Program has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect the

Receiving Program's use or disclosure of protected health information.

The Receiving Program shall:

- Use and disclose the protected health information only for the stated purpose.
- Not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Disclosing Program.
- Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than provided for by the Internal Data Sharing Agreement.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

As stated above, the WYFI Data Exchange system is supporting and working towards the vision of creating community-based virtual medical records and other clinical applications to promote a healthier Wyoming through a statewide secure, connected, and coordinated health IT system. The Data Exchange provides a platform for the sharing of virtual medical records for those purposes.

The WYFI assures secure access to patient data through the following security measures: Once new users are connected to the WYFI Health Information Exchange they are immediately trained on how to use the software. The training is web-based however, our training team is available to train on-site.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to WDH which includes Federal, state, and local government, and the private sector.

5.1 Will information be shared with or disclosed to external organizations?

Yes, the WYFI provides access to healthcare records from data contributing healthcare entities, facilities, and providers across the State (see table 1.2 above) to other participating healthcare entities, facilities, government entities, and providers, and their authorized users, which may include the organizations and entities listed in the tables in 1.2 above. Participants determine who within their organization will be an authorized user.

5.1.1 What information is shared or disclosed externally, and for what purpose?

Authorized users can query and view the system for clinical records on a patient which includes information such as lab results, hospital Alert Discharge and Transfer (ADTs) notifications, face sheets, treatment plans, radiology reports, transcribed reports, medications, clinical summaries, and other data contributed to the system. For providers that have interfaces connected to the Health Information Exchange, results can be delivered directly to the provider's Electronic Health Record (EHR) system. The system can also generate Continuity of Care Documents (CCDs) which a provider can use to share patient information with other appropriate providers and which are retained
in the community health record and can also be queried. Direct secure messaging allows providers to electronically send and receive clinical information quickly and securely from one healthcare provider to another.

5.1.2 Is the disclosure of personally identifiable information (PII) or protected health information (PHI) with each external organization compatible with the original collection? Please describe the legal mechanism or authority permitting or requiring each external organization to use or disclose the information.

The WYFI executes a Participant Agreement with each participant that identifies the permitted uses and requires compliance with the WYFI Policies and Procedures. The WDH, the WYFI is the business associate to participants contributing data, so the BAA outlines the WYFI's privacy & security responsibilities. authorized users electronically agree to the EULA terms. These documents provide details as to the permitted uses of the data within the Health Information Exchange and require compliance with the HIPAA Regulations. Participants and authorized users acknowledge that certain uses of Data, including without limitation treatment, payment, and certain healthcare operations (as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164, Subpart E) do not require specific consent by a Patient under HIPAA to share. However, participants and authorized users acknowledge their responsibility for securing any patient consent or authorization to access Data through the Health Information Exchange as required by the WYFI Policies and Procedure Manual, or as otherwise required by law.

5.2 How is the information accessed, transmitted, shared, or disclosed?

Participants and Authorized Users can query and view the system for clinical records on a patient on a case-by-case basis or for providers that have interfaces connected to the Health Information Exchange, results and alerts can be delivered directly to the provider's EHR electronically. For providers who do not have a

certified EHR, the Data Exchange provides a local platform that enables sending and viewing of clinical results data.

5.2.1 What security measures safeguard its transmission?

The WYFI Policies require security controls to avoid, detect, counteract, and minimize security risks. These controls protect the confidentiality, integrity, and availability of the information in the Health Information Exchange. The WYFI Policies require participants to adhere to HIPAA and all applicable Laws regarding accessing, the permitted use of, secure transmission of, and storage of any shared data within the Health Information Exchange.

The WYFI maintains data encryption standards applicable to sensitive information including PHI/PII, login, or other credentials through AES-CBC (AES in Cipher Block Chaining mode) with a 128-bit key minimum, or triple DES (3DES-CBC) containers for data at rest. Whole disk encryption may also be employed for data at rest. TLS 1.2 or 1.3 for data in motion. Systems powering the WYFI and products employ encryption to data in motion and at rest.

The WYFI uses the following encryption to protect data transmitted over public networks:

• For data transmitted over our grid (Connect solution), all payloads are double encrypted once at the data level using 2048-bit symmetric encryption and a second time via the channel streamed over 128-bit encrypted SSL.

• The WYFI's Community Health Record and Organize solutions encrypt data transmissions using 128-bit TLS or SSL encryption. This included web-based access to results using our inbox (SSL encryption is used for all browser displays) and data transmitted via web services.

• The WYFI's encryption algorithms are compliant with FIPS 140-2/3 standards.

• User Access: The WYFI documents the granting and approval of access to client data. Users receive access based on their roles, which aligns user and client data for appropriate levels of access. De-provisioning, revocation, or modification of user access to the systems, information assets, and data implemented is done in real-time (if possible) for changes in the status of employees, contractors, customers, business partners, or third parties. Any change in status, such as termination of employment, contract, or agreement, change of employment, or transfer within the organization, triggers reassessment of access privileges. The WYFI's applications support two-factor authentication methods built on standards that integrate into Internet Information Server (IIS).

• Encryption: The WYFI can create unique encryption keys for each client. We support client-generated encryption keys and permit clients to encrypt data to an identity without access to a public key certificate (e.g., Identity-based encryption). The WYFI encrypts client data at rest (on disk/storage) within the WYFI environment. We leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances and can manage encryption keys on behalf of the WYFI. To support the encryption capabilities, we maintain key management procedures.

• Vulnerability and Patch Management: the WYFI conducts application-layer, local operating system-layer, and network-layer vulnerability scans regularly as prescribed by industry best practices. Results of vulnerability scans are available at any request.

• Antivirus/Malicious Software: The WYFI has anti-malware programs installed on all systems, which support cloud service offerings.

5.3 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

As stated above, the WYFI Data Exchange system is supporting and working towards the vision of creating community-based virtual medical records and other clinical applications to promote a healthier Wyoming through a statewide secure, connected, and coordinated health IT system. The Data Exchange provides a platform for the sharing of virtual medical records for those purposes.

The WYFI assures secure access to patient data through the following security measures: Once new users are connected to the WYFI Health Information Exchange they are immediately trained on how to use the software. The training is web-based however, our training team is available to train on-site.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Wyoming is an opt-out State (patients' health information is sharable by participating medical groups, hospitals, labs, radiology centers, and other health care providers through secure, electronic means unless the patient opts out). Each participant or authorized user agrees to develop and maintain a Notice of Privacy Practices (the “Notice”) that complies with applicable law and with the WYFI Policies. This Notice informs individuals of the entity’s Health Information

Exchange participation and use and provides individuals the opportunity to opt-out of using the procedure established by the WYFI.

6.1.1 Is the notice provided for the collection of information adequate to inform those impacted by the system that their information has been collected and used appropriately?

Each participant has their own Notice. The WDH's notice is available on the Department's website.

The WYFI provides an Opt-Out form to the hospitals and clinics that are sharing patient data through the Health Information Exchange to provide to patients who wish to Opt-Out. The Opt-Out form also can be accessed through the WYFI website. The WYFI Opt-Out Form

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Certain uses and disclosures of Data, including treatment, payment, and certain healthcare operations (as defined by the HIPAA Privacy Rule) do not require prior authorization from the individual. The HIPAA Privacy Rule does afford individuals the right to request that uses and disclosures of their Data to carry out treatment, payment, and healthcare operations are restricted. If a participant agrees to a restriction, the participant must comply with the WYFI Policies on restrictions. However, the sharing of health information through the Health Information Exchange is voluntary and a patient has the right to Opt-Out of participation in the Exchange.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Currently, The WYFI does not offer granular consent. An individual either chooses to participate fully in the Health Information Exchange or exercises their right to Opt-Out.

6.4 <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice of data collection to the individual is the responsibility of the participant that is submitting the data as outlined in the Participant Agreement and the WYFI Policies and Procedures. The notice is required to meet the content requirements

set forth under the HIPAA Privacy Rule and comply with all applicable laws and regulations. HIPAA establishes the requirements for when and how notice is provided and made available to individuals.

Section 7.0 Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may request a copy of the Continuity of Care Document (CCD) created by the system from the health information provided by data contributors by submitting a written request to the Department. Individuals may use the WDH Authorization to Release Health Records to request a copy of their CCD or authorize/instruct WDH to send a copy of their CCD to a third party. However, the Health Information Exchange does not provide direct access for patients wishing to access or view the health information about them maintained and owned by Health Information Exchange participants who are Data contributors. Individuals are referred to their healthcare / contributing provider for access to their health information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Due to the clinical nature of the data accessed through the Health Information Exchange, the WYFI Policies prohibit it from amending data within the Health Information Exchange. If an individual makes an amendment request directly to the WYFI, the individual will be referred to the participant who owns the health record. Each participant or authorized user is required by the WYFI Policies to comply with applicable federal, state, and local laws and regulations regarding an individual's right to amend their health information in the event of inaccurate or erroneous information.

7.3 How are individuals notified of the procedures for correcting their information?

The participant's Notice of Privacy Practices will contain information for correcting the health records created or maintained by the participant. Informing the individual of the Provider's process for correcting inaccurate information is the responsibility of the participant that is submitting the data as outlined in the WYFI Policies and Procedures. The process will vary from participant to participant.

7.4 Privacy Impact Analysis: Discuss the privacy impacts associated with the redress available to individuals. Identify privacy risks and mitigation.

Due to the clinical nature of the data accessible through the Health Information Exchange and to protect the Provider-Patient relationship, it is essential that all issues relating to redress flow through the Provider-Patient relationship. The WYFI policy of not amending data directly protects the WYFI and the individual from data being incorrectly amended outside of the Provider-Patient relationship. Therefore, all requests for amending data within the Health Information Exchange are referred back to the participant providing the data. Participants may access or, if necessary, request an accounting of disclosures or other information from the WYFI to notify other participants of any changes to patient data as may be required to comply with the HIPAA rules. Clients are unable to access their information they would be unaware of any information that needs to be corrected at this time.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Qualified organizations must first go through the process of becoming participants in the WYFI through the processes outlined in the Participant Agreement and the WYFI Policies and Procedures. Once an organization complies with the onboarding processes, which include ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and regulations and with the WYFI policies, organizations will begin the process of onboarding authorized users. Access to a patient's clinical data in the WYFI is determined by the authorized user's role in the organization and their relationship to the patient. End users may be associated with multiple facilities through the identification of entities in their profiles. Access rights and levels are based on a user's function and role, using the concepts of least privilege and need-to-know to match access privileges to defined responsibilities. Users are granted an initially limited set of default permissions to access resources. Requests for additional access follow a formal process that involves a request and approval from a data or system owner, manager, or other executives, as dictated by security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies, as well as regular re-certification of privileges. Users have role-based access and roles are created in partnership with each client and specific to their user community. Role-based access and security provide for restriction and un-restriction of data, including PHI information at a user level, to ensure privacy and appropriate access permissions for each user group and audience.

Users from other agencies will follow the same process as outlined above and only be granted access to the system if the agency has the right to view the data as outlined for all participants.

The WYFI uses role-based access with setting up users. Based on the user will determine what patient data they can see. Clinicians can see all data whereas billing users would only have access to the patient demographics.

8.2 Will Department contractors or third-party vendors have access to the system?

Department contractors would only have access to the system if they have a legitimate reason for viewing the data in the Health Information Exchange under applicable law and have a Business Associate Agreement executed with the Department. Any such contractors would be held to all of the same restrictions as other participants and must comply with all the WYFI Policies.

8.3 What privacy training is provided to users either generally or specifically relevant to the program or system?

During end-user training HCI and the WYFI provide an overview of the types of activities end-users should comply with the WYFI policies and HIPAA. During Organization Administrator training we review the roles and responsibilities of the designated Organization Administrator (see the Roles and Responsibilities documents for a detailed list of Administration and Account Maintenance Activities. HCI also reviews the WYFI patient consent process for opt-in and opt-out procedures. HCI reviews the Management Reports accessible to Organizations for end-user audits as well as EULA and activities to comply with HIPAA:

1. Only access information that is necessary for you to perform your job duties.
2. Do not access your own records or those of anyone else (relatives, co-workers, acquaintances, etc.) unless it is directly related to the provision of care.
3. Do not share your username or password or other authentication information with anyone.
4. Remember to log out of the WYFI after each use so that others may not use your identification to access information through your account.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Health Catalyst Inc. is Health Information Trust Alliance (HITRUST) certified. Under HITRUST, HCI provides that data foundation and integrated workflow solutions enable today's population health management objectives, including timely clinician engagement, the improved transition of care, reduction in

duplicative services, and the opportunity for patients to take an active role in their personal health. In HITRUST, you must have a monitoring program in place to determine if the controls continue to operate effectively over time, no data security breach reportable to a federal or state agency by law or regulation has occurred, no significant changes in the business or security policies, and timely completion of the interim review as defined in the HITRUST Assurance Program Requirements. The data centers maintain HIPAA/HITECH, HITRUST, PCI DSS, SOC 1, 2, and 3 Type 2, ISO 27001 certifications.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The WYFI has a tool that lets administration users perform their own audits on their users. WDH administration can audit all users of the WYFI. An audit is kept of every transaction received by the network. The log documents every step in the information exchange process who it was sent to when it was sent and received, and what happened to the data upon receipt (was it printed, viewed, or acknowledged by an EHR interface). Furthermore, the original message as it was received, along with the message as it was transformed for delivery is kept to assist in troubleshooting.

Key events such as a user logon/logoff, successful authentication, and other events are logged. Data that is maintained in the logs include User ID/context, Patient ID/context, Data type, Event date/time, Encounter context, Data descriptor/index, Event type, what Software module, and other Event-specific information. All relevant transactions executed in the solution and through the HIE adaptor are recorded in the audit database.
Transactional history may be retrieved on request and is stored encrypted using a FIPS 140-2 cipher. All-access or modification to a record is stored in the event log and logs can be correlated.

See 5.3.2 and 5.4.2 above for a description of the encryption protocols and other security measures in place to ensure the security of the data.

The WYFI leverages two-factor authentication for all users to access the system. As a user enters his/her password into the application, the system masks entries with asterisks (*) on the screen display. User passwords are hashed and stored within the application database. Administrators can set passwords to expire after a certain number of days. If a user enters either an invalid username or password a configurable number of times (WYFI set to 5), the system will lock the account until an administrator resets it. Local IT staff can handle password maintenance or the WYFI staff can assist. User password lengths are configurable and set to an eight-character minimum.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Policies to establish comprehensive privacy protection, compliance, enforcement procedures, and remedies following violations are crucial to maintaining health information privacy. The WYFI policies recognize 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 the WYFI policies and participant or authorized user policies, the WYFI policies stipulate that the policy that is most protective of individual privacy should govern decision-making. This is designed to make clear that the WYFI 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 helps 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 Health Information Exchange.

participants in the Health Information Exchange, due to their clinical nature, already must comply with rigorous HIPAA and other privacy laws and regulations. The WYFI policies leverage these requirements and ensure that all participants follow them at a minimum.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.

9.1 What type of project is the program or system?

The WYFI is an infrastructure system. Wyoming healthcare stakeholders have recognized a need for electronic healthcare Health Information Exchange since 2004, with several initiatives designed to promote information sharing. These efforts have led to the initiation of this statewide HIE in the summer of 2016. Since that time, Wyoming stakeholders, including the Wyoming Department of Health

(WDH) have worked together to design, develop and implement the WYFI initiative. This is an operational initiative in partnership with the community to develop the infrastructure for health information exchange throughout Wyoming.

9.2 What stage of development is the system in and what project development life cycle was used?

Phase 1 – Phase 1 of the implementation has a focus on the integration of the 27 identified Wyoming hospitals with the HIE. The integration of the 27 hospitals will allow clinical data to flow between the hospitals (directly via the hospital EHR, where possible) and with the HIE. Per the RFP, Phase I shall include DDI of the core HIE technologies, clinical data interfaces for 27 eligible hospitals, encryption, security, audit, hosting and Service Level Agreements (SLA), and help desk support for all stakeholders.

Phase 2 – Phase 2 of the implementation has a focus on the integration of service providers such as laboratories, public health systems, and other data contributors and service providers. Integration with service providers and public health systems will allow for reporting to public health systems and services, and also allow data from data contributors and service providers to flow to providers and the HIE (laboratories, etc.). Per the RFP, Phase II shall include the integration of laboratories, existing public health systems via the Total Health Record (THR) Gateway, and the THR EHR (MIE) for data contribution and RLS integration into the MIE EHR.

Phase 3 – Phase 3 of the implementation has a focus on the integration of ambulatory EHRs with the HIE, allowing ambulatory data and providers to share data, including directly within the EHR when possible. Per the RFP, Phase II shall include the integration of ambulatory EHRs as data contributors to the HIE and the integration of the HIE RLS into the Ambulatory EHRs.

Currently, the project is in a combination of all three phases as the WYFI continues to integrate new connections to the Health Information Exchange. The hosting of the WYFI services is currently in the maintenance stage of the development life cycle.

9.2.1 Was the system assessed through the OCIO Project Proposal review process?

A Business Case was completed and approved by the OCIO office on August 20, 2020. An amended Project Proposal was submitted to ETS on December 09, 2021, and is awaiting approval.
Data Dictionary
WYFI High-Level Architecture

WYFI Architecture
Network Architecture Diagram

9.3 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

Given the highly regulated nature of the environment within which the Health Information Exchange operates and the fact that all participants are already held to the standards outlined in HIPAA and other local, federal, and state regulations, no privacy concerns beyond what are already addressed through the WYFI Policies & Procedures and the discussion above have arisen.

This section is for OPSC use only.

Privacy Impact Assessment Review Results

Date reviewed:
Reviewer:

Evaluation and Determination:

☐ Approved. This IS NOT a privacy sensitive software or information system.
Approval Number:
☐ Denied. The privacy and security risks to PHI or PII have not been properly mitigated.

Comments: