



## Introduction

The [Health Information Exchange \(HIE\) Workgroup](#) has been tasked by the [Health Information Technology Oversight Council \(HITOC\)](#) to assist them and the Oregon Health Authority (OHA) with developing a set of strategies and recommendations to accelerate, support, and improve HIE across the state.

Beginning in May 2022, the HIE Workgroup met monthly to discuss the most pressing HIE needs and opportunities in Oregon. At the request of HITOC, the Workgroup discussed how consumers can take a more active role in their understanding of, and participation in, HIE efforts. Additional concepts important to successful adoption of HIE, like privacy and security standards, and data quality, are included in this concept paper to form a set of additional considerations. This concept paper will be considered by HITOC as they update [Oregon's Health IT Strategic Plan](#).

There is reference throughout this paper to HIE, electronic health records (EHRs), interoperability and other terms used regularly in this policy area. For definitions and other information, please review the [Statewide Vision for HIE](#) concept paper.

### Contents of this Paper:

Introduction	Page 1
Overarching Objectives and Strategies	Page 1
Section 1: Consumers and HIE	Page 3
Consumer Strategy Recommendations	Page 8
Section 2: Privacy, Security, and Data Quality	Page 10
Privacy, Security, and Data Quality Strategy	
Recommendations	Page 12
Helpful Definitions	Page 15

## Overarching Objectives and Strategies

As described in the [Statewide Vision for HIE](#) concept paper, there are six overarching objectives identified by the HIE Workgroup that relate to *Consumers, Privacy & Security, and Data Quality*, each with a set of strategies. These overarching components apply to each of the focus areas described in the rest of this paper. For more information about these objectives, refer to the [Statewide Vision for HIE](#) concept paper.



## Objective 1: Improve health equity

- **Short-term priority strategy:** Prioritize HIE use cases to support transitions in health insurance status and life events, as well as identify SDOH
- Collect and clarify demographic information on patients that can help inform care and support needs
- Identify health inequities at the population level and inform targeted interventions that address these inequities
- Promote HIE data sharing models that take a vendor-agnostic approach to ensure access across broad populations of providers serving the numerous patient populations in Oregon
- Promote a more diverse health IT workforce within organizations to operate and use these systems. HIE end users often drive strategy and direction of how HIE solutions are used, and thus this workforce should reflect the diversity of Oregon communities
- Encourage governance entities that oversee HIE solutions in Oregon to consider the above ideas to ensure that Oregon's HIE infrastructure is aiding OHA in its health equity goals

## Objective 3: Enable broad and timely care coordination

- Increase the use of electronic, closed loop clinical referrals
- Add more high-quality information from different sources
- Ensure that data sources are integrated into EHRs via HIE

## Objective 5: Promote knowledge of HIE and broad contribution of data by all parties

Educate and encourage Oregon entities to participate more broadly in HIE. For example:

- Identify and prioritize the standardized and non-standardized data that should be included in HIE efforts
- Prioritize who should contribute data and when
- Identify barriers to information sharing and develop mechanisms to address these barriers and discourage data silos, which may include governance efforts

## Objective 6: Promote continued improvement of data quality and completeness

- Create more consistent and ongoing data quality practices across HIE solutions in Oregon, particularly those leverage federal standards



## **Objective 7: Promote individual and caregiver understanding of, and access to, health and social needs data**

- Considering activities that increase awareness and understanding for patients for how HIE works in Oregon, as well as understanding of confidentiality and patient rights
- Promoting/supporting the consolidation of multiple personal health records and/or patient portals that consumers may access
- Supporting efforts by health plans and/or providers to engage patients in their information sharing strategies

## **Objective 8: Promote patient privacy and security of data systems**

For detailed strategies tied to Objective 8, see Section 2: Ensuring Health Information Privacy, Security, and Data Quality on page 10.

## **Section 1: Consumers and HIE**

### **Historical Context**

In the U.S., health information is commonly believed to belong to the health care consumer that it relates to. Providers, health plans, and other actors are permitted to collect, share, and use this information only in ways that are defined by federal law, state law, or by individual patient consent (see Informed Consent section below). Consumers themselves are free to share this information in any way they see fit. Policy efforts have been made to encourage consumers to access and interact with health IT, in part to bolster the role of the consumer in health care and to achieve information parity with providers. The [Health Information Technology for Economic and Clinical Health \(HITECH\) Act \(2009\)](#) that created the federal EHR incentive program for providers included expectations that EHRs make data available to consumers via web-based portals, and to communicate in some instances via Direct Secure Messaging. More recent policies, particularly post-COVID-19 pandemic, are taking further steps to put consumers in the center of how HIE operates and functions (see Federal Efforts explained below).

Despite these efforts, most patient portals remain siloed versions of a provider's health record system. Furthermore, some consumers face hurdles in navigating through patient portals or other HIE tools that health care entities use to share information. Few investments have been made to assist consumers in using HIE effectively, e.g., education, technical assistance, customer support, etc. With digital tools now incorporated into so many aspects of daily life, there has been growing demand at the state and federal level for HIE strategies that account for the information needs of health care consumers. Furthermore, with OHA's strategic focus on health equity, exploring the consumer's role in HIE has never been more critical. At the federal level, this emphasis on consumers has occurred through both the establishment of



[information blocking rules in the 21st Century Cures Act](#) and new [Centers for Medicare & Medicaid Services \(CMS\) requirements on health insurers and other entities](#) to make information available and be more responsive to electronic requests from consumers for their own health information. The goal of these more recent policies is to make a consumer's health information more easily accessible and usable, and to encourage more consumers to get involved in data sharing to promote their own health.

## Federal Efforts Explained

Several important, recent federal initiatives will impact what health care consumers can access in terms of their own health information and from which health care entities. Some of the most notable initiatives that are currently underway:

- **Trusted Exchange Framework and Common Agreement (TEFCA):** Part of the 21<sup>st</sup> Century Cures Act, and being implemented by the Office of the National Coordinator for Health IT (ONC), [TEFCA](#) establishes a new national network of qualified health information networks, or QHINs, that will facilitate specific HIE use cases. Individual access to health information is among the priority QHIN use cases. In the future, it is projected that TEFCA will further enable consumer-facing third party applications to query QHINs and provide consumers access to their own health information.
- **Advancing Interoperability and Improving Prior Authorization Processes**  
**Proposed Rule:** Recent CMS final rules under the 21<sup>st</sup> Century Cures Act now require that certain health plans (generally those that touch Medicare, Medicaid, or federal exchange lives) provide application program interfaces (APIs) for key data exchange use cases involving other payers, providers, and the patient. A [current Notice of Proposed Rulemaking from CMS](#), expected to be finalized some time in 2024, would build upon this infrastructure by requiring plans to share more information related to prior authorization processes. Prior authorization requests are made by providers to health plans before certain medical items or services may be rendered to patients.

## Problem Statement

Consumers of health care face inequities in accessing their health care information electronically. These inequities derive from many factors such as location (some communities lack reliable broadband internet access), language preference (many software applications are not available in all languages spoken in Oregon), resources (smart phones and personal computers are not affordable for all), digital literacy (not all consumers are offered the same level of support with technology), and provider (different providers and systems use different tools with variation in how patients may interact). The HIE Workgroup did not discuss how to address all of these broader environmental issues. However, as explained below, the Workgroup believes that strategies which empower consumers to understand and use HIE will



help to bolster the role of the consumer in HIE in the short term. As one Workgroup member stated: “it is our responsibility to ensure that all consumers can comfortably and effectively navigate their health care information, irrespective of their starting point.” Re-centering consumers in HIE strategy is a necessary step toward supporting health equity in Oregon.

## Patient Story: Hillary

Hillary, a 35-year-old female, recently visited her primary care physician for a standard check-up. Prior to this visit, she had not seen her doctor in two years. Hillary has a history of struggling to navigate the health care system due to her anxiety.

After her doctor’s visit, Hillary received an email that there were test results for some blood work available on her doctor’s EHR patient portal. She followed the email link to the portal, logged in, and reviewed the test results. She also reviewed an old note the provider had written two years earlier indicating that Hillary was withdrawn and behaved irritably in the exam room.

Having worked closely with her behavioral health provider to get a handle on her anxiety, Hillary was deeply offended and hurt by this provider note. She contemplated switching primary care physicians before ultimately deciding to have the note removed from her patient record. Uncomfortable saying anything to her physician, who authored the note to begin with, she reached out to her provider’s medical records department. That was three weeks ago and despite several voice mails and emails, no one has responded to Hillary. Furthermore, Hillary does not know if other providers have seen this note through HIE.

Health Information Exchange Questions:

- What is Hillary’s recourse for this physician note she feels is stigmatizing and inaccurate?
- How can she prevent this note from being shared with other providers she may visit in the future?
- Would Hillary’s problem be compounded if she was not a native English speaker, but spoke predominantly Vietnamese in her home? Her patient portal only has options for English and Spanish.
- What if Hillary did not have access to reliable internet? Would she even have seen the note from her provider’s EHR system? Would she have been able to log in to the patient portal and review the same level of information?

## Informed Consent

Informed consent is an agreement between a health care consumer and their provider. In the context of HIE, informed consent is a primary way that consumers can influence or control how



their personal information is shared with other entities. This process acknowledges a consumer's freedom and independence to understand and choose what happens to their body and information about their body. Importantly, providers are permitted to share information without patient consent in many circumstances (see Privacy section below). When those circumstances are not in place, it is informed consent documents which guide how information can be shared.

The Workgroup believes that obtaining informed consent from consumers could be further improved across the state to ensure that in all instances of data exchange—those that required specific consent and those that are permitted without consent—are performed in ways that empower and educate the consumer. For example, Workgroup members noted that adding informed consent documentation to a stack of other intake and survey documents during an intake or waiting room period de-emphasizes the importance of obtaining *informed* consent. “Informed” is emphasized in this sentence to clarify that while consent is routinely obtained from consumers, it is the informational aspect of consent that could be better leveraged to empower consumers—by doing more to explain their rights and how state and federal privacy laws work around HIE. This type of improvement would also serve to better educate the consumer about the value of information exchange and getting more involved in this process.

## **Patient Portals and Personal Health Records**

In 2023, the predominant way most consumers interact with their own health information is through a patient portal. This refers to a website or a software application linked to a provider's EHR, that may allow the consumer to view health history and other patient medical chart information; view follow up information such as hospital discharge instructions; see lab and test results in near real time; communicate with care teams; schedule and cancel appointments; and pay for services. A consumer's experience with these portals is intrinsically tied to their comfort level with the internet or other technology, as well as their comfort level with the health care system in general. Oregon does not currently collect data on how consumers use patient portals, but as mentioned earlier, some consumers of health care face inequities in accessing their health care information via patient portals due to language barriers, digital literacy issues, or lack of access to technology or broadband. Importantly, patient portals are tied to EHR products, and as such, there is little incentive to ensure that the information available to consumers via patient portals is interoperable across multiple providers or health systems. Consumers face gaps in seeing their entire health care history through any particular portal view.

A personal health record (or PHR), like a patient portal, is designed to provide consumers access their own health information. However, in contrast to patient portals, a PHR is also designed to give the consumer greater control over which health care entities may access their personal health information and the level of information they may access. Whereas patient portals are windows into a provider's EHR—and are governed by federal law and policy—a





PHR is intended to put the consumer in the center of what health information is available about them and who may access it. PHRs typically allow consumers to integrate data from multiple sources, whereas patient portals tend to provide access to a health record maintained by one provider or health care entity.

Given OHA's goals for health equity, the HIE Workgroup acknowledges that PHRs may be an important future part of Oregon's HIE landscape.

## **OpenNotes**

[OpenNotes](#) refers to an international advocacy movement to encourage and promote that the full patient record—including physician notes—is available to patients. Established years before the 21<sup>st</sup> Century Cures Act and information blocking rules, this movement urged health systems to make more information available to patients via their EHR patient portal. In addition to being an equitable approach to making information available to patients, the OpenNotes effort has published evidence that this approach positively impacts patient care.<sup>1</sup> Many health care providers in Oregon have implemented OpenNotes and it can be viewed as a positive initiative in the area of consumers and HIE.

## **Consumer Apps and Application Programming Interfaces (APIs)**

Recent federal policy is focused on modernizing health care for consumers in ways similar to banking or other industries. Part of this vision is to ensure that the proper infrastructure is in place to allow consumer apps to access health information about the consumer to improve the patient experience. For example, a consumer could download an app that tracks their diabetes management which pulls vitals and other information directly from the consumer's medical chart maintained by their provider. In the past, this interaction would have required multiple data sharing agreements and/or technical integrations to function. APIs are enabling software tools to quickly tap into other data systems and pull the information they are seeking at the behest of the consumer. This emerging industry—and the consumer demand for it—will likely grow in the next few years. Future iterations of HIE strategy in Oregon will likely need to address privacy and security concerns of these consumer-facing applications, at the very least to ensure that consumers are aware of vendor privacy policies and to prevent misuse of data.

---

<sup>1</sup> OpenNotes maintains a list of peer-reviewed publications on the impact of this program: <https://www.opennotes.org/research/>



## Strategy Recommendations for HITOC: Consumers and HIE

### The Role of Consumers

#### Successful outcomes include:

1. The average health care consumer in Oregon may access their own health information electronically, in a means they understand, for all providers/entities they work with
2. Consumers have a simple and comprehensive way of correcting errors they find when accessing their own health information via HIE solutions, including EHR portals

#### Focused Recommendations:

1. **Conduct a health care consumer survey.** The Workgroup recommends establishing a set of questions that could be added to an existing survey or used to generate a new survey of health care consumers to inform future efforts on consumer-facing health IT/HIE initiatives. While many surveys are used to conduct regular assessments on how individual consumers feel about the health care system, health insurance, and many other topics, few if any surveys in Oregon assess consumers' understanding of health IT, HIE, and other topics relevant to the state's health IT/HIE strategy. The Workgroup emphasized the importance of ensuring that a survey effort specifically address concerns around sharing sensitive information, like patient demographics (including race, ethnicity, language, disability, sexual orientation, and gender identity), substance use disorder treatment information, certain types of infectious diseases, and information about social determinants of health like housing and food needs.
2. **Conduct a consumer education campaign.** HIE Workgroup members suggest a public-facing campaign in Oregon to bring greater consumer attention to the role of data sharing and technology in the healthcare sphere. This should be informed by consumer survey data (see above). Additionally, one HITOC member emphasized the role of education for consumers, including for youth, senior citizens, and even policy makers who do not always understand the role of HIE in health care. Topics of the campaign could span from understanding your rights as a health care consumer, to understanding the barriers to true interoperability, to greater understanding of the complexity of HIE tools and how they support improved patient care. For example, the Workgroup identified break-the-glass functionality<sup>2</sup> as an area where consumers should likely have increased awareness of how their health information is shared in cases of emergency (see Privacy strategies below).

---

<sup>2</sup> Break-the-glass functionality refers to tools that allow an end user to make visible health information that would typically be restricted, due to the presence of a medical emergency. By breaking the glass, the end user is attesting that an emergency is present and viewing the additional information is necessary for patient care.





3. **Support consumers updating their own information.** The Workgroup, as well as HITOC itself, raised the issue of consumers facing hurdles in updating information within patient portals or other health IT tools they may have access to. Anecdotal evidence suggests that consumers can face significant challenges to getting their own medical information changed or updated by a provider (or in some instances a health plan). The Workgroup recommends that future HIE efforts consider how state efforts can support a standard process by which consumers can address these concerns. This topic is also an opportunity to support health equity in the HIE space. Further, one HITOC member recommended encouraging vendors to create the ability for an individual to personalize their story such as including information about themselves in a historical timeline or highlighting a particular health condition within their record.

## Informed Consent

### Focused Recommendations:

1. **Promote bi-directionality between consumers and their providers.** Informed consent in Oregon largely focuses on how data is shared from a provider to another end user, or unilateral data exchange. Similar to other areas of information exchange, the ultimate objective in Oregon is to accomplish bi-directional data exchange between all end users, and this includes consumers. Future work could recommend standardized language for informed consent that promotes bi-directional data exchange.
2. **Support clinicians in changing consent processes.** Workgroup members noted the important role of providers in helping consumers understand their rights and the role of information sharing in their health care experience. Given the burdens facing providers post-COVID-19 pandemic, any technical support or modular training methods that could be offered to support providers, or standardize the informed consent process, will also benefit the consumers they serve to ensure that all data sharing is ultimately informed.

## Patient Portals and Personal Health Records

### Successful outcomes include:

1. When a consumer accesses their own health information via a patient portal, they may access information across multiple providers and/or health care encounters, providing a more accurate picture of their total health care experience.
2. Information is documented and made available to providers so that consumers are not required to re-share their personal story multiple times, increasing efficiency and helping avoid re-traumatization.



## Focused Recommendations:

1. **Explore patient portal consolidation.** Explore opportunities to consolidate health information available via patient portals, including how to encourage or incentivize health systems and providers to make HIE-derived data on patients available through their EHR patient portals. Health care consumers in Oregon should have no wrong door for how they access a longitudinal record of their own health information from multiple providers through their patient portal. For Epic, a common EHR used by health systems in Oregon today, individuals can now access their data from multiple Epic EHRs via their MyChart portal, which relies on Epic's proprietary HIE. In an ideal future, an Oregon consumer who accesses their own information via Epic MyChart should also be able to see, through that same portal access, information that came from a NetSmart MyAvatar or an eClinical Works EHR patient portal. Consumers should not be burdened by the fact that providers in Oregon have selected different EHR vendors for medical charting.
2. **Include PHR adoption in future environmental scan work by OHA.** An important role of OHA currently in supporting the adoption and use of HIE is through its [public-facing analyses of statewide adoption and spread of HIE tools](#). The HIE Workgroup suggests that future efforts would be aided by having clearer data on how many PHRs exist in Oregon and what their use looks like across different geographies and communities. Consumer surveys (recommended above) or other methods could be used to capture this information and assess interest and challenges, or barriers related to PHRs.

## Section 2: Ensuring Health Information Privacy, Security, and Data Quality

### Problem Statement

Interoperability between different technology systems relies on a foundation of trust and reliability. This cannot be achieved without standards around the policies and technical architecture that are used to ensure protected health information does not end up in the wrong hands. Privacy and security are baseline components of any HIE strategy and the HIE Workgroup dedicated time to discussing the present state of privacy and security of HIE solutions in Oregon and developing recommendations for future work. Some of the Workgroup discussion focused on the gaps in knowledge and awareness of privacy and security rules and practices. One HITOC member mentioned that privacy and security are well understood at health systems, but there are large gaps for non-health systems (like social service agencies) and their trusted entities, which may be an important area for future work.



## Health Information Privacy

As a starting point, the HIE Workgroup acknowledges that many health care consumers do not fully understand the complexities of HIPAA—the foundational federal rules around how protected health information may be shared without express patient consent. For example, it is likely that many health care consumers in Oregon are unfamiliar with the permitted disclosures under HIPAA that guide when a provider or health plan may exchange their personal information without their consent for the purposes of treatment, payment, health care operations, or public health purposes.

In addition to HIPAA, federal and state laws can further restrict information sharing among health care entities. This is common for areas that might be considered particularly sensitive like substance use disorder treatment information or certain kinds of infectious disease data. For example, Oregon law typically prevents sharing public health communicable disease data with health plans. In 2021, Oregon law was changed to temporarily allow sharing of COVID case data with coordinated care organizations (CCOs) and insurers in 2021 (ending shortly after the public health emergency ended in May 2023). This change in law facilitated data sharing to support CCOs acting as critical partners for supporting Medicaid members who needed to isolate or quarantine due to COVID-19.

The task of the Workgroup was ultimately to determine whether there were short term needs or any specific policy recommendations related to privacy and security in the HIE space. The Workgroup felt that it would be necessary for any future policymaking in Oregon around privacy and security of health information to have a clear definition and scope of types of data and/or technologies they would apply to. For example, should HIE solutions that collect personal information about patient sexual orientation or gender identity (SOGI) be held to a higher standard than what HIPAA requires in terms of privacy and security? The Workgroup did not address this specific question, but instead recognizes that it is a relevant consideration if Oregon-specific privacy or security requirements are desired. Beyond this consideration, the Workgroup did have some suggestions for future work in this space, discussed in the strategy recommendations section below.

## Health Information Security

Security standards evolve at the rate of technology advancement—which is often faster than state and federal policymaking. As such, most health information security standards are established and assessed by the private market. There are standard procedures for health IT solutions to follow, including Systems and Organizational Controls 2 ([SOC-2](#)), which is the industry standard for health IT vendors including HIE solutions. Having a SOC-2 at a minimum ensures that organizations or individuals who may have security questions or concerns will get them answered through the SOC-2 report. Any entity that holds HIPAA-covered information



(called protected health information, or PHI<sup>3</sup>) must also demonstrate HIPAA compliance on top of SOC-2 compliance.

[HITRUST](#) is a higher bar of security compliance than SOC-2. HITRUST requires certain financial investments and other commitments by vendors to achieve certification. The Workgroup suggested that future work on health information security look into the details of HITRUST certification to explore further what Oregon should expect as a baseline for health information security. For example, should Oregon require all HIE tools to require multi-factor authentication to protect access to information? The Workgroup expects questions like this to come up as security practices evolve.

## HIE Data Quality

Complete, accurate, and timely data are critical for trust and reliability of HIE. We use the term “data quality” to refer to both the accuracy and consistency of data that is flowing in and out of these systems using federally-recognized data standards. Although EHRs produce standards-based data feeds to HIE, these connections do not guarantee that data included in the exchange is accurate. Furthermore, data exchanged between systems needs to be ingested into the receiving system and can be mapped incorrectly (e.g., mapping chief complaint as a diagnosis into a receiving system). The complexity of data exchange can lead to inconsistent quality of data feeds and/or can degrade over time with upgrades, filters, etc. For example, HL7 admit, discharge, transfer (ADT) feeds refer to a common data standard for health care encounter information (including patient demographics, utilization information, etc.). It is fairly simple for HIE solutions to track how often specific data fields (e.g., discharge date, discharge disposition, etc.) are missing within contributed ADT, as well as to understand whether these gaps are temporary or longstanding. It is important for HIE vendors to be working on behalf of end users and consumers to have processes or policies in place to ensure that data feeds do not degrade over time or lead to significant errors or missing data.

## Strategy Recommendations for HITOC: Privacy, Security, and Data Quality

### Health Information Privacy

#### Focused Recommendations:

1. **Promote consumer awareness of HIE privacy and security practices, including but not limited to break-the-glass functionality.** The HIE Workgroup encourages future public educational or awareness campaigns to call greater attention to privacy and security and the role of HIE in health. One area that this campaign may focus on is greater understanding of how break-the-glass functionality is designed to balance

---

<sup>3</sup> See the Helpful Definitions section on page 12.



competing interests of sharing information for specific cases of emergencies while protecting consumer privacy for non-emergency purposes. The HIE Workgroup suggests leveraging existing guidance from the U.S. Department of Health & Human Services and other sources that already exist. For example, the Office of the National Coordinator for Health Information Technology (ONC) has gathered a collection of resources on the topics of [privacy, security and HIPAA](#).

2. **Assess opportunities to streamline HIE related to public health emergencies.** COVID-19 led to many lessons learned around restrictions limiting the exchange of important information during a public health emergency. To ensure that future public health emergencies are not hampered by these restrictions, the Workgroup suggests assessing statutory restrictions and streamlining data exchange in times of public health emergencies to ensure that data can be used to keep both patients and providers safe during infectious disease outbreaks or other emergencies like climate events.

## Health Information Security

### Focused Recommendations:

1. **Explore HITRUST further.** The Workgroup recommends that future work in HIE security, if needed, dig deeper into the specific details and requirements of the HITRUST certification process. This could inform future efforts by Oregon to regulate HIE security more proactively in the future, if through HITOC or the legislative process, it is identified that a security policy is needed.

## Data Quality

The HIE Workgroup recognizes the importance of ensuring a reliable and transparent process for HIE solutions to track data quality and reach for HIE end-users and consumers.

### Successful Outcomes include:

1. HIE solutions used in Oregon are benefitting from broad contribution of data from most health care entities, with few opting out or unnecessarily filtering out important information.

### Focused Recommendations:

1. **Provide greater transparency into HIE solution data quality and scope of exchange.** Acknowledging that no technology system will ever be perfect, the Workgroup recommends that a rule or standard be developed around how any HIE solution operating in Oregon make available their 1) list of data contributors, 2) data sources (e.g., ADT interfaces, C-CDA interfaces), 3) API end points or other connections that allow for more advanced querying, and finally 4) a customer support contact or other way to reach the entity to identify data quality questions or concerns.



The purpose of this would be primarily to give consumers—as the ultimate owners of their own health information—a better way to understand how these systems work.

## Emerging Issues in Health Information Privacy

The Workgroup identified several emerging issues in the HIE privacy space that should be considered for future strategic planning, but were not included in this concept paper:

- **Reproductive health** – with the Dobbs decision overturning Roe v. Wade, there are growing concerns around how data sharing across state lines could impact the privacy, safety, and potential liability of individuals who seek family planning and reproductive health services
- **Sexual Orientation and Gender Identity (SOGI)** – Oregon is planning for more robust demographic data collection including SOGI (per [HB 3159 \(2021\)](#)). There may be concerns around privacy related to SOGI information being shared beyond one's provider through HIE
- **Substance use disorder treatment** – even with expected [revisions to 42 CFR Part 2](#), there are still consent requirements that make it difficult to share behavioral health information like physical health information
- **Mental Health Records** – the sharing of mental health-related information can have significant impacts upon an individual's life and thus necessitates deeper consideration compared to other types of health information.
- HIE implications for protecting **sensitive protected health information** could include a need for better data protections/segmentation related to consent





## Helpful Definitions for this Concept Paper

**Data Quality:** The accuracy and completeness of the data that is captured and shared via HIE solutions. While federal data standards exist to ensure consistency in what and how data is collected, exchanged, and made available within an EHR system (thus promoting interoperability), it is currently up to health IT and HIE solution vendors to ensure the quality of the data exchanged. Standardized data formats can be exchanged with missing and/or inaccurate data fields. Providers and/or consumers may notice this missing data as they use or rely upon HIE solutions and patient access tools, which threatens the credibility of these solutions and has the risk of undermining the value of HIE. Missing data can lead to unnecessary tests or procedures and also means treatment decisions by providers are not fully informed, which could impact patient health outcomes or even risk patient safety.

**Privacy:** The policies and processes by which health information is protected, kept confidential, and only shared with appropriate parties. The cornerstone for health information privacy in the United States is the Health Insurance Privacy and Portability Act (HIPAA) which contains the [HIPAA Privacy Rule](#) governing all health care providers and insurers (among others). This federal regulation sets a standard nationally for health information privacy, and individual states may establish more stringent rules or guidelines on top of HIPAA. NOTE: No state may take a more lenient approach to privacy than what HIPAA mandates.

**Protected Health Information (or PHI):** An individual's personal health information which HIPAA-covered entities are required to protect under the HIPAA Privacy Rule.

**Security:** The technical and operational processes by which electronic information is collected, stored, and transmitted across different technology systems to control access and protect information. This includes whether information is stored via onsite servers or in the cloud, how information is encrypted in transit and at rest, and how organizations safeguard information.

You can get this document in other languages, large print, braille or a format you prefer free of charge. Contact Luke Glowasky at [Luke.A.Glowasky@oha.oregon.gov](mailto:Luke.A.Glowasky@oha.oregon.gov) or 503-576-9041 (voice and text). We accept all relay calls.