findhelp

Consumer Privacy and Consent:

Implications for Social Care and Social Drivers of Health in the United States

Introduction

The COVID-19 pandemic accelerated awareness of and access to new technology focused on health and wellness. Usage of new apps, websites, and wearable technology skyrocketed, with millions of people in the United States taking advantage of this newfound convenience and accessibility as they sought care in a number of different areas of their lives.

Specific to telehealth and tele-therapy offerings, State legislatures acted quickly to ensure claims for new models of care delivery could be processed, and many niche startups in the telehealth space became mainstream. Industry leaders agree that healthcare required this innovation and policy attention to modernize how people receive care in their moments of need; however, there is often a dark side that accompanies progress. In this case, some companies are taking advantage of the people using these new services by inappropriately selling their personal data.

Joanne Kim, a researcher with the Duke Sanford Public Policy School, **contributed to a report** on data brokers and the sale of sensitive mental health data in the United States.

Key Highlights from the report:

- 11 out of 37 contacted data brokers were willing and able to sell mental health data and health care records.
- 10 data brokers advertised highly sensitive mental health data on Americans, including those with depression, insomnia, and anxiety. The data also included ethnicity, age, gender, ZIP Code, religion, children in the home, marital status, net worth, credit score, data of birth, and single parent status.
- A specific data broker went as far as to offer names and postal addresses of individuals including those with obsessive compulsive disorder (OCD), personality disorders, and strokes, and included their race and ethnicity.
- Pricing for this information varied: some offered licensing models of $75-$100k, while others charged only hundreds of dollars for 5,000 records.

Consumers, policymakers, and the industries that serve health and wellness need to pay attention to the implication of personal health data being sold for a profit without consent. We must improve consumer protection across all sectors that serve the health of Americans; we cannot assume existing safeguards will prevent the violation of private information.

In the age of abundant digital technology, data privacy issues and considerations are complex. How data is acquired, shared, used, owned, sold, and matched with other data is confusing at best. While there are some federal rules in healthcare, education, and through the Federal Trade Commission, there are many gaps in addressing consumer privacy, including the fact regulations can differ from state to state (and sometimes even conflict with each other).

Hossein Rahnama and Alex "Sandy" Pentland in the Harvard Business Review, The New Rules of Data Privacy, captured the data economy conundrum:

"The data harvested from our personal devices, along with our trail of electronic transactions and data from other sources, now provides the foundation for some of the world's largest companies. Personal data [is] also the wellspring for millions of small businesses and countless startups, which turn it into customer insights, market predictions, and personalized digital services. For the past two decades, the commercial use of personal data has grown in wild-west fashion. But now, because of consumer mistrust, government action, and competition for customers, those days are quickly coming to an end."

For most of its existence, the data economy was structured around a "digital curtain" designed to obscure the industry's practices from lawmakers and the public. Data was considered company property and a proprietary secret, even though the data originated from customers' private behavior. That curtain has since been lifted and a convergence of consumer, government, and market forces are now giving users more control over the data they generate. Instead of serving as a resource that can be freely harvested, countries in every region of the world have begun to treat personal data as an asset owned by individuals and held in trust by firms."

Quite simply, technology companies today must have transparent privacy policies, terms of use, and data use explanations. They risk their business's success and loss of consumer trust if they ignore consumer privacy concerns or sell consumer data under false pretenses.

Like other areas of health and wellness, the American social safety net is modernizing at an unprecedented pace. Millions of people are using technology every month to connect to social service providers, community organizations, and other forms of social care. They are sharing their most sensitive information at their most vulnerable moments to determine their eligibility for the help they need. We must be wary of those vendors and technology companies that are poised to take advantage of skirting privacy and consent in the name of health equity.

The following paper illustrates the gaps in existing laws, exposing current risks in social care. In addition, we'll review example approaches that can modernize consumer directed privacy and consent.

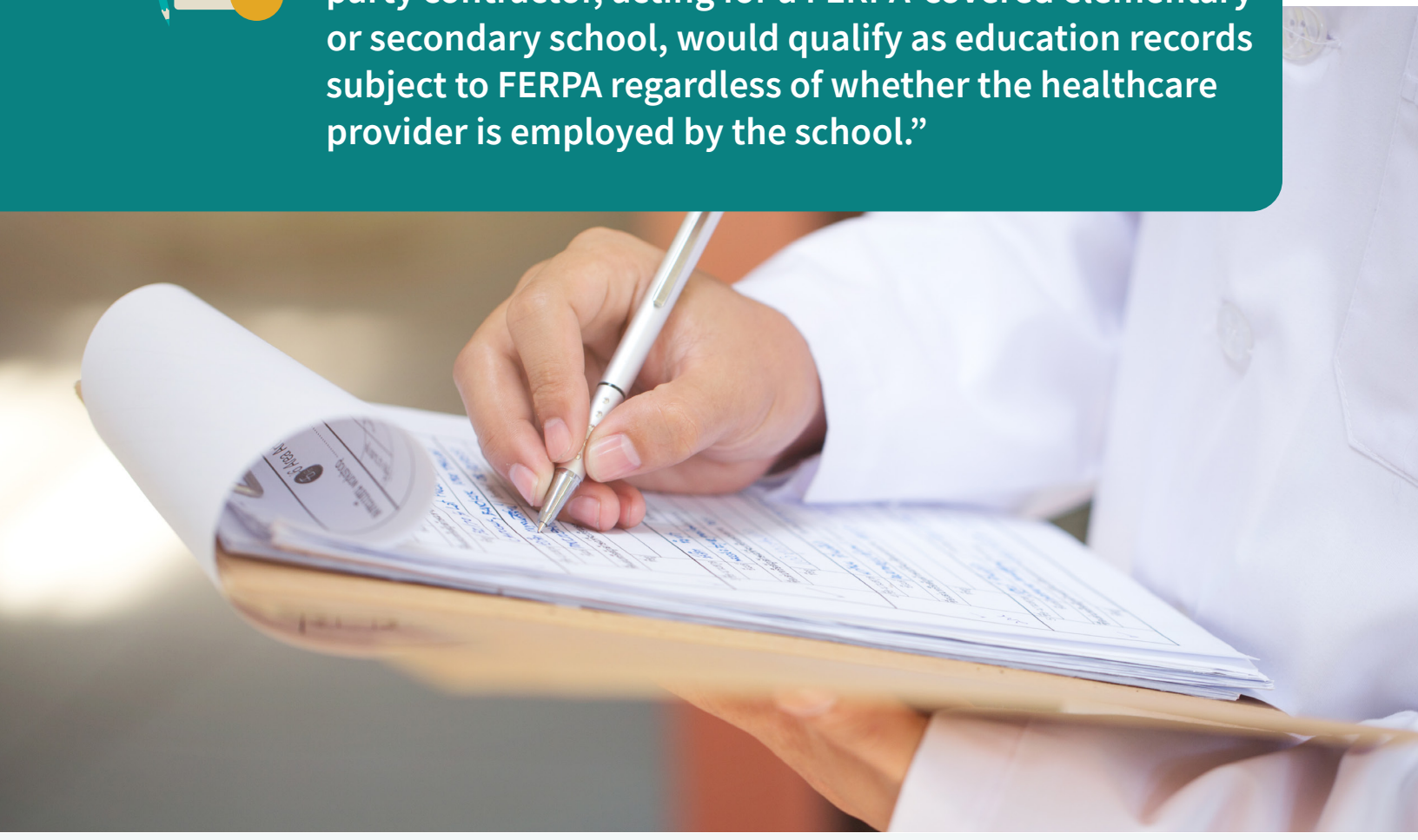
Current Laws That Protect Health Data and What They Mean:

The United States does not have a single, comprehensive federal law related to data protection and privacy. Instead, there are several disparate federal regulations and many state laws and regulations.

The U.S. has HIPAA, FERPA, FCRA, the FTC section 5, COPPA, and others. These rules are mostly industry-specific, open to legal interpretation, and do not solve for cross-industry data use.

For example, on the U.S. Department of Health and Human Services' website (HHS.gov), they determine that school healthcare data isn't actually healthcare data under HIPAA when they write:

"Health records that directly relate to students and are maintained by a healthcare provider, such as a third party contractor, acting for a FERPA-covered elementary or secondary school, would qualify as education records subject to FERPA regardless of whether the healthcare provider is employed by the school."



Federal Trade Commission Section 5

Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits ‘‘unfair or deceptive acts or practices in or affecting commerce.’’ The prohibition applies to all persons engaged in commerce, including banks. An act or practice is unfair when it causes or is likely to cause substantial injury to consumers, cannot be reasonably avoided by consumers, and is not outweighed by countervailing benefits to consumers or to competition.

HIPAA

The HIPAA (Health Insurance Portability and Accountability Act of 1996) Privacy Rule establishes national standards to protect individuals' medical records and other individually-identifiable health information (collectively defined as “protected health information”). It applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain transactions electronically.

The Privacy Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. It also grants individuals rights over their protected health information, including to examine and obtain a copy of their health records, direct a covered entity to transmit to a third party an electronic copy of their protected health information via an electronic health record, and request corrections.

HIPAA Rules Apply to Covered Entities and Business Associates

Individuals, organizations, and agencies that meet the **definition of a covered entity under HIPAA** must comply with the Privacy Rule's requirements to protect the privacy and security of health information. They must also provide individuals with certain rights with respect to their health information. If a covered entity engages a third-party business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement that establishes specifically what the business associate has been engaged to do and requires them to comply with the Privacy Rule. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

Covered entities include the following:

1 Healthcare Providers*

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

2 Health Plans

- Health insurance companies
- Health maintenance organizations (HMOs)
- Company health plans
- Government programs that pay for healthcare, such as Medicare, Medicaid, and military and veterans programs

3 Healthcare Clearinghouses

Includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

* but only if they transmit any information in an electronic form and in connection with a transaction for which the Department of Health and Human Services has adopted a standard.

Non-covered entities are not subject to HIPAA regulations

Examples include:

Health social apps that are not administered by a covered entity

Wearables such as FitBit that are pure consumer devices

Personal Health Record (PHR) vendors that are not provided by a covered entity

Community-Based Organizations (CBOs) – such as food pantries, housing support organizations, immigration help centers, and other services. Whether the CBO is a covered entity depends on the HHS definitions above, though most of the million or so nonprofits in this country are not recognized as covered entities.

Social Care and the Social Safety Net Digital Transformation

The creators and stakeholders of social care related data include, but are not limited to, the following:

- Hospitals
- Health plans
- Physician medical offices
- Dentistry clinics
- Outpatient clinical centers
- Federally qualified health centers (FQHCs)
- Employers
- Schools
- Colleges
- Prison systems
- Government agencies
- Community-based organizations
- Libraries
- Consumers / constituents
- And more…

Social care data can originate from many different industries, and is treated differently based on its origin. Below are two examples that illustrate how the health privacy laws apply, or don't apply, based on who is involved in a social care referral process.

Covered by HIPAA

a food pantry referral that originates from a hospital discharge planner is considered personal health information and is protected by HIPAA rules, and the patient has a consumer right via the Cures Act to access this data.

Not covered by HIPAA

if a consumer originated that same food pantry referral on a public kiosk of their own accord, this data is not considered to be personal health information, and it would only be bound by the terms of use and privacy policy of the technology company that provided the kiosk.

If the consumer walked into a food pantry themselves and completed a walk-in referral using the food pantry's case management system, the consumer may or may not have the choice to accept or sign a consent for their information to be used by this organization.

As we can quickly see, none of the consent and privacy rules, laws, and processes are consistent or easy to navigate. Each of these stakeholders may have their own privacy terms and/or technology systems with additional terms, and may be using vendors with yet another layer of terms.

Should consumers have to wait for Federal legislative action in order to protect their social care privacy and data? Let's look at the kinds of data we're talking about in social care.

For illustrative purposes, below is a subset of the data that is typically collected when helping a person address their social needs:

- **Demographic Data:** Mary Smith - 123 Main St, Portland, ME
- **Identifier:** 12345
- **Subscriber Coverage:** State insurance ABC
- **Personal Data (like income):** 26,000/year salary, Veteran, cancer survivor
- **Social Care Assessment questions:** Have you been a victim of domestic violence?
- **Social Care Assessment results:** Yes
- **Social Risk:** Food insecure
- **Social Goals:** Healthy food access and affordability
- **Forms/Documents:** Utility bill on record
- **Navigator Referrals:** Food bank referral
- **Navigator Note:** Mary is willing to travel less than 5 miles for groceries
- **Organization Referrals:** Referral to domestic violence support group
- **Personal Referrals:** Referral to substance abuse counseling
- **Navigator Orders:** Veteran medical appointment free rides
- **Care Team Notes:** Mary is unwilling to engage relatives for support
- **Responses:** Foodbank is providing weekly food delivery
- **Outcomes:** Mary is not yet food secure
- **Risk Profiles:** Mary is legally married, Mary is going through foreclosure

Put yourself in the shoes of a person in need. Perhaps you are trying to find childcare at 2 am so you can work your second job. Perhaps you are worried about paying for medication or don't have a refrigerator to keep the medication stable. Most importantly, you may not be ready to discuss these personal issues with stakeholders in your community, however well-meaning those individuals may be.

Additionally, when you are ready to share your story, wouldn't you want (and don't you deserve) to have transparency into which organizations will have access to your most personal social care data?

Let's take a look at an example of a patient, Maria, who has diabetes. Maria is ready to tell a social worker that she is looking for nutrition information and needs assistance to obtain medication that can help manage her condition. The social worker wants to refer Maria to a counselor to discuss her food needs and clinical condition, and Maria consents to share that information. Does consenting to share that specific information also mean that the counselor now has access to all of Maria's other needs, referrals, social care history, and documentation? It shouldn't, unless she specifically chooses to share it. Should getting help from a counselor require a person to give consent to share their entire social care history?

In some cases a person may receive a referral to an organization that will do more of the care coordination, such as an Area Agency on Aging (AAA), a community care hub, or the Pathways Community HUB Institute® Model. We should ensure the person knows how their information will be shared among these secondary provider networks by disclosing the organizations who are part of that network.

There is a blurred line in some industries when it comes to consent, privacy, and sharing or selling data. For example, if a covered entity (like a hospital) collects your social care needs in an assessment and makes some referrals for you at your request, that hospital has the right to share your personal information (per HIPAA) for care coordination purposes with other covered entities. The Office of Civil Rights explains that as long as the disclosure is for health care operations, the information can be disclosed.

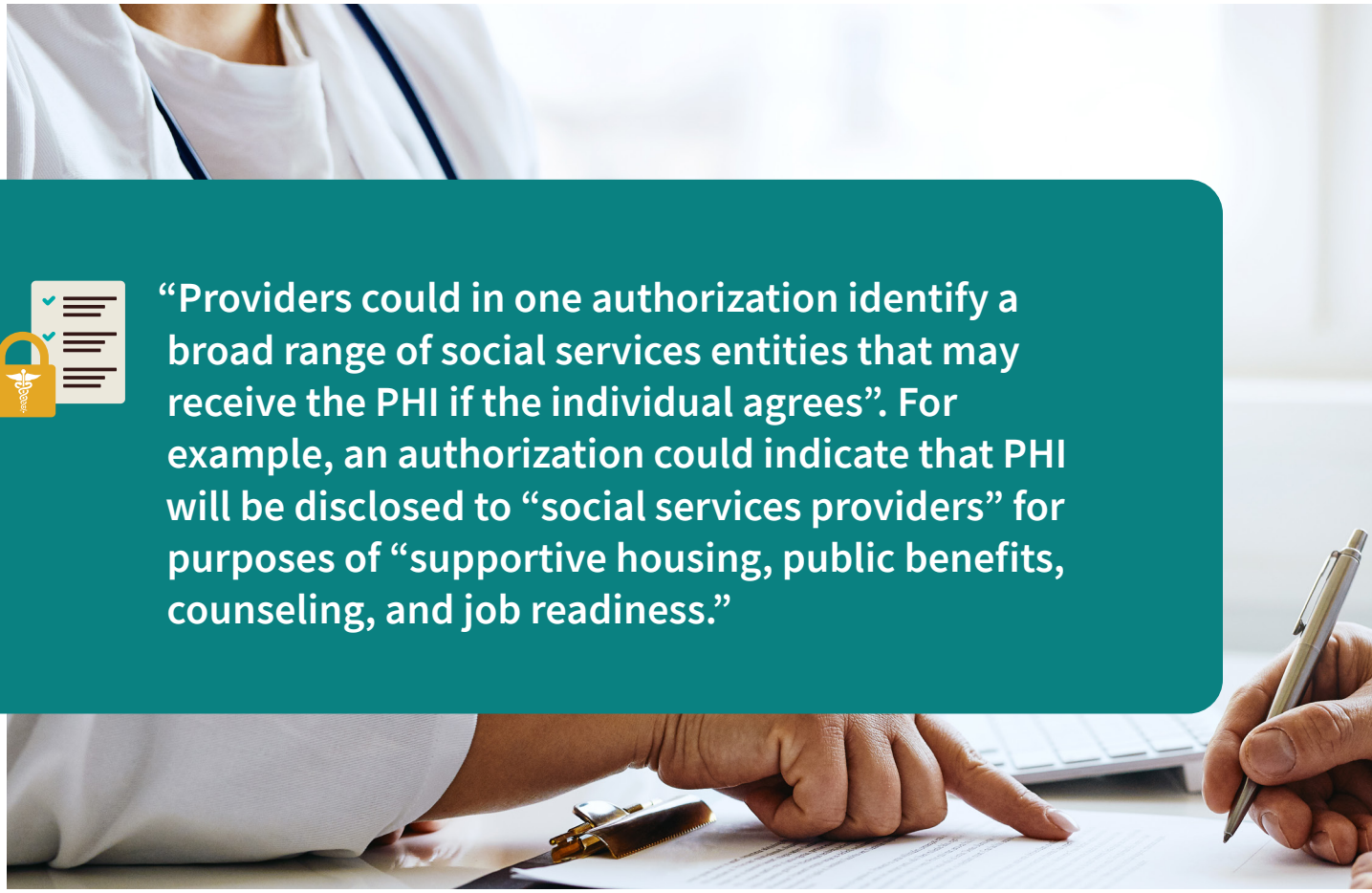
Now, what about a covered entity sharing personal health information with a non-covered entity? This is where it becomes unclear.

From the website of the Department of Health and Human Services:

A healthcare provider may disclose a patient's Personal Health Information (PHI) for treatment purposes without having to obtain the authorization of the individual. Treatment includes the coordination or management of healthcare by a healthcare provider with a third party.

Health care means care, services, or supplies related to the health of an individual. Thus, healthcare providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual's health or mental healthcare may disclose the minimum necessary PHI to such entities without the individual's authorization. For example, a provider may disclose PHI about a patient needing mental health supportive housing to a service agency that arranges such services for individuals.

From the Office of Civil Rights:



"Providers could in one authorization identify a broad range of social services entities that may receive the PHI if the individual agrees". For example, an authorization could indicate that PHI will be disclosed to "social services providers" for purposes of "supportive housing, public benefits, counseling, and job readiness."

It's our belief that collecting consent is always the best practice, especially as information in social care will nearly always be going to non-covered entities that may not have business associates (or liability agreements) with covered entities to protect data.

The Problem

Now that we've covered some background information, let's examine another important aspect of social care data privacy: **consent**.

Here are real quotes from active social care vendors in the United States:

> **Information** may be shared with agencies within or outside of the ******* platform"

> You agree to share **information** with a network"

> CIE [community information exchange] and its partner agencies may share your personal, financial, and health **information**"

> This consent covers all information shared by you or by anyone that has the right to share **information** on your behalf"

Medical Consent

Protects covered entity staff from liability if harm is caused to a patient (e.g. consent for surgery to take place).

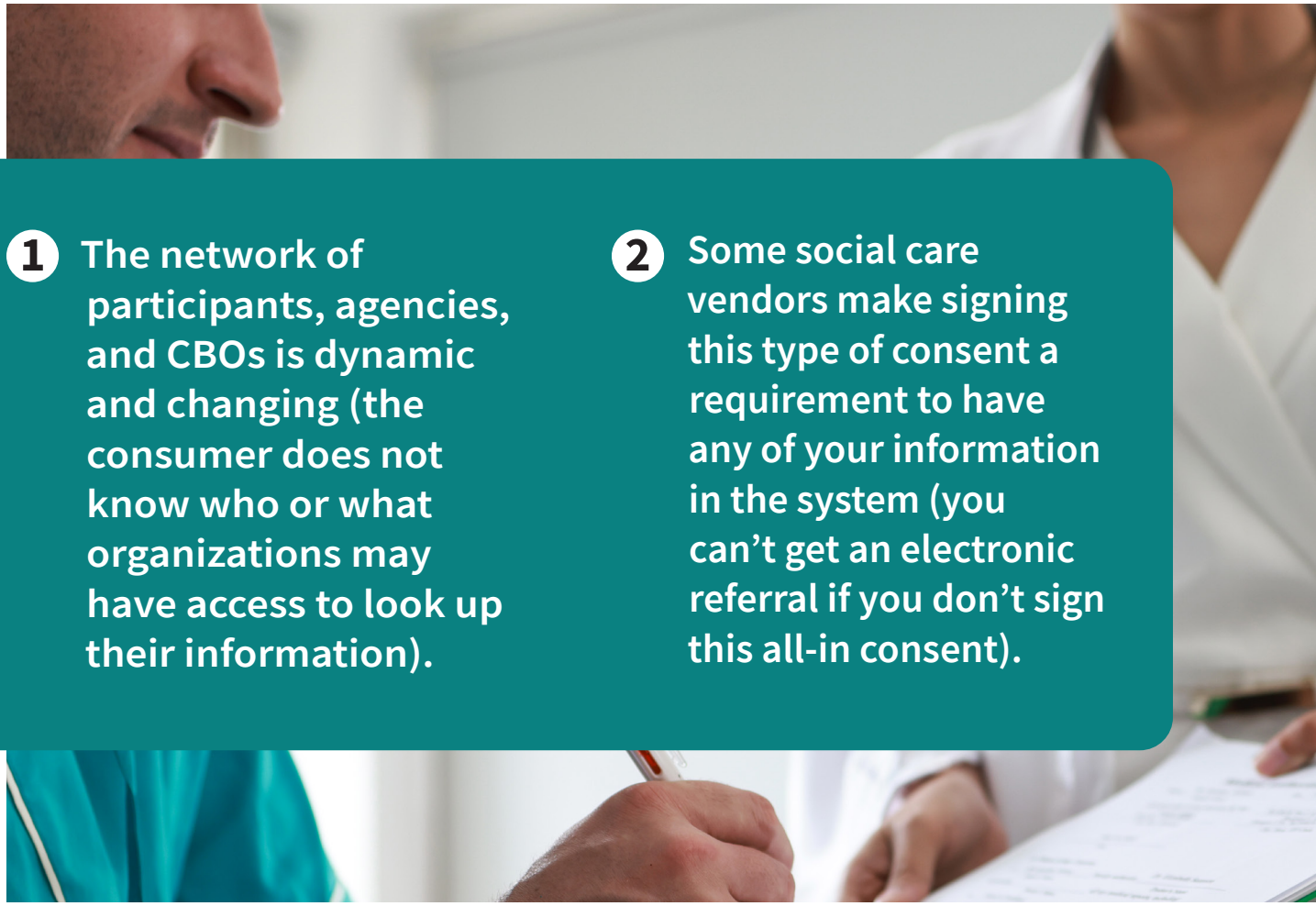
Expressed Consent

Agrees to specific terms of data use or disclosure.

Informed Consent

Is often a written consent with specific provisions, terms, or data use language.

A consent that covers all information and future sharing of information is often an "all-in" consent, meaning:



1. The network of participants, agencies, and CBOs is dynamic and changing (the consumer does not know who or what organizations may have access to look up their information).

2. Some social care vendors make signing this type of consent a requirement to have any of your information in the system (you can't get an electronic referral if you don't sign this all-in consent).

There are vendors operating in social care today that oppose policies that restrict the sale of this sensitive data. In fact, one vendor is actively promoting the fact that they are a "solution for consumer insights at scale, along with individual-level SDoH scoring and monitoring for every adult in the United States." Personal data is already being sold to help risk stratification companies make a profit off of our most sensitive information.

Vendors may configure their systems to keep certain types of referrals (for example, those related to 42 CFR Part 2, like substance abuse) private, as they should. However, this takes the control away from the consumer. The consumer may want to keep a food referral private, but make a substance abuse referral available for their housing coordinator to help determine eligibility.

This is an unacceptable gap in privacy and consent, and we must and can do better with policy and consumer transparency. Vendors shouldn't be choosing the rules of privacy; consumers should be in control.

Strengthening Privacy and Social Care

We must act quickly to stay ahead of social care digitization and advances in the technology we use to help people receive care. The following are the principles we believe should be followed as legislators consider strengthening consumer protections:

1 The principle of consumer-directed privacy

In social care, this means that the person in need completes consent and has transparency to see which organizations have access to their personal social care record within a technology system. This principle can be implemented through an informed consent at the time of assessment or referral, requiring an opt-in to having information shared with a specific service provider. **If the consent is to a network, the person should also have transparency into the list of the individual organizations who have access.**

2 The principle of permissioned-based access

In social care, this means that across hospitals, schools, nonprofits, and more, only the people directly involved in delivering care and services should have access to personal records. This principle can be implemented through role-based security, which modern technology systems can implement effectively.

3 The principle of no vendor quid pro quo

No person should be denied a service or electronic referral on the basis of refusing to sign an all-in consent that requires data-sharing to a broad or undefined network. This principle can be implemented through Federal and/or State legislation and would act as a stop gap to prevent vendors from unauthorized data-sharing.

Legislation and Advocacy We Support

We are pleased to see NH Bill SB 423 recognize these gaps in privacy and act to protect constituents in New Hampshire. We're also pleased to support Assembly Member Weber in California, who is championing AB 1011 to prevent the sale of private data in California. We support and will help champion these and future efforts to close the privacy gap in the social care space, to ensure that constituents have transparency, control, and continued dignity in their journey to a better quality of life for themselves and their families.