IDC

DATA SHARING PRIVACY AND CONSENT:

The New Payer Requirements and the Connected Content Technologies Required to Fulfill Member, Regulator, and Patient Needs

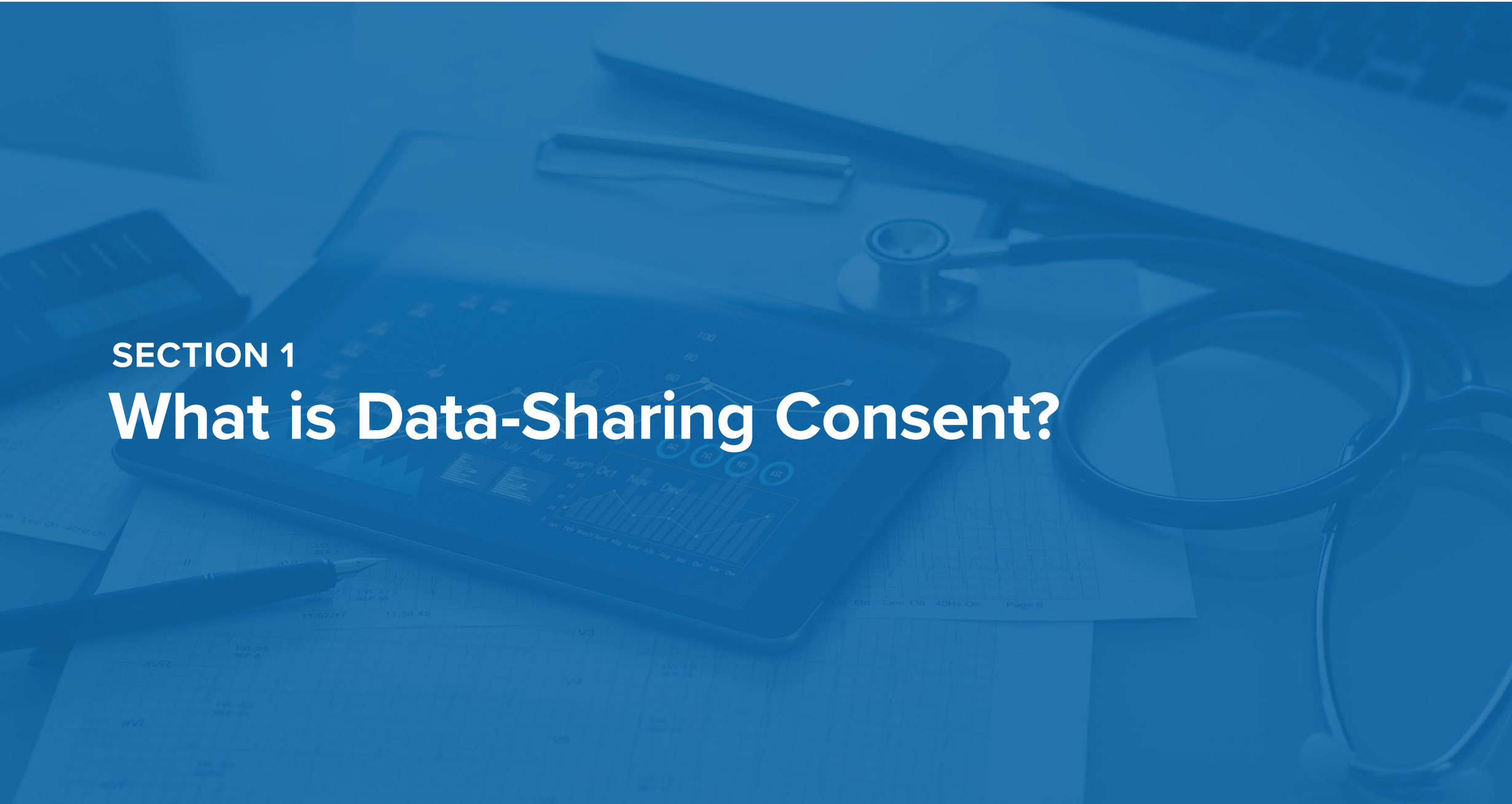
RESEARCH BY:

Jeff Rivkin, M.Sc, PAHM, CHRS, CPEHR, CBIP, CCP, CDP
Research Director, IDC Health Insights

January 2022 | IDC Doc. #US48679522

This eBook is organized into the following sections:

Click on titles or page numbers to navigate to each section.



SECTION 1

What is Data-Sharing Consent?

What is Top of Mind for Healthcare Providers?

Health IT Evolution

- Recalibrating toward next-generational consumerism, documentation, and digital member experiences
- Data proliferation (volume, variety, velocity, and value)
- System, regional, and nationwide interoperability
- Cybersecurity and resilience

Digital Era Challenges

- Pre-existing challenges (ACA, MLR, aging populations, chronic conditions, Value-Based-Care (VBC), cost pressures, shifting regulatory environment)
- Emerging challenges (mergers/payviders, resiliency, COVID-19 variants, vaccine management, talent shortages, rise of consumerism, cyberthreats)

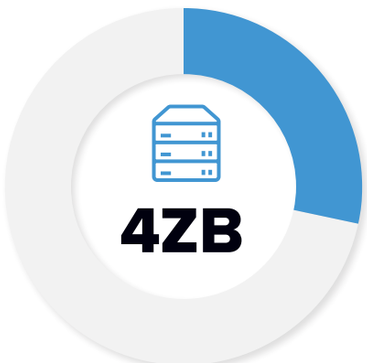
Next-Gen Emergence

- Disruption redefined
- Cloud-based platforms and ecosystems (next-gen claims, care management, wellness, reimbursement transformation)
- Emerging technologies and interoperability standards (IoT, AI/ML/DL, RPA, FHIR, cybersecurity, AR/VR, blockchain)

Intelligence in Action

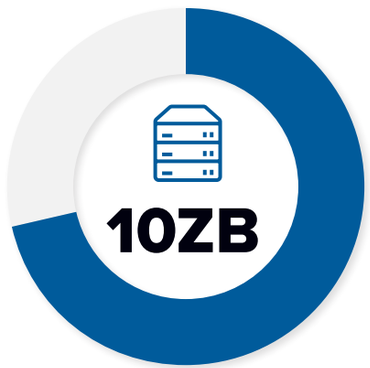
- Shift from “data-rich” to “information-driven”
- Better ingestion, aggregation, integration, and orchestration of data to improve outcomes and streamline operations
- Data excellence and member satisfaction

The Current State of Data in Healthcare



of data in healthcare by **2022**

Average amount of data that healthcare organizations currently manage



of data in healthcare by **2025**

longer retention rate of data in healthcare versus other industries

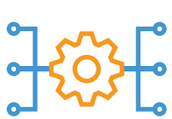
Source: IDC's *Data Readiness Condition (DATCON) Index*, 2021

Evolving Towards an End State of "Data Excellence"

According to IDC, **data excellence marks the endeavor to harmonize and treat "data as an asset"** with particular attention given to data management and quality, working toward the goal of enabling inimitable technological capabilities and organizational differentiation.

The attainment of data excellence in healthcare requires that structured and unstructured data and clinical and non-clinical content be seamlessly integrated with interoperability to improve access, exchange, and utilization of health information with new and lasting efficiencies in workflows.

IDC predicts that **by 2022, 20% of healthcare organizations will have achieved data excellence,** aligning with industry expectations of a more shared, open, and interoperable future; and that **by 2023, 30% of healthcare organizations' business and clinical decisions will be informed by AI insights** that will revolutionize human-machine collaboration in the future of work.[1]



Once cultures and technologies align inside payers to achieve internal data excellence, the challenge then goes to **sharing that data in an equally excellent way.** The ability to execute and control access to the data via "data-sharing consent" becomes the measure by which this "excellence" is tested.

Source: IDC's *FutureScape — Worldwide Healthcare Industry 2022 Predictions*

What is "Data-Sharing Consent"?

It is impossible to address health data-sharing consent without defining what a member/patient is consenting to:

A loosening of member/patient health data privacy via electronic means through a health information exchange (HIE), whether through a formal body or not, for treatment, payment, and healthcare operations purposes.

Source: *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

To explain the characteristics of data-sharing consent, we address:

- Types of formal HIE organizations
- Consent decision qualities
- Consent options
- Provenance
- Covered entities and authorizations
- Delegating consent decisions beyond the individual

Types of Data-Sharing Organizations

Data-sharing organizations that are formally created are also known as "Health Information Exchanges" (HIEs).

Types of Formal HIE Organizations

An HIE organization **oversees and governs the exchange of health-related information among organizations** according to nationally recognized standards. There are several different types of HIEs currently operating across the United States and its territories:

Hybrid HIEs are often collaborations between organizations within a state or region, such as an accountable care organization (ACO) and a vendor network. The Kentucky Health Information Exchange is an example of a hybrid model.

Private/proprietary HIEs concentrate on a single community or network, often based within a single organization, and include overall management, finance, and governance. Examples may include hospital/integrated delivery system networks, payer-based HIEs, and disease-specific HIEs. Some software vendors have also established an HIE network for their clients across the United States.

Regional/community HIEs are inter-organizational and depend on a variety of funding sources. Most are not-for-profit. Indiana Health Information Exchange and Chesapeake Regional Information System for Our Patients (CRISP) are examples of regional HIEs.

Statewide HIEs are run by the governments of their respective states or, in some cases, by the state's designated entity. Some state-wide (and regional) HIEs use an umbrella approach and serve as the aggregator for disparate private health information exchanges. Statewide Health Information Network for New York and Arizona's Health Current are examples of state-wide HIEs.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Consent Decision Qualities

Patient trust must be ensured, and patients may often be asked to make a "data sharing consent decision." A meaningful consent decision consists of six aspects. The decision should be:

Made only after the patient has had sufficient time to review educational material

Commensurate with circumstances for why health information is exchanged

(i.e., the further the information-sharing strays from a reasonable patient expectation, the more time and education is required for the patient to make a decision)

Consistent with patient expectations

Not used for discriminatory purposes or as conditions for receiving medical treatment

(Consumers are not a monolithic block; some individuals have varying levels of education and English proficiency)

Commensurate with acceptable circumstances for why individually identifiable health information is exchanged

Revocable at any time

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Consent Options

Consent options for electronic data sharing include the following:

- **No consent.** Health information of patients is automatically included (patients cannot opt-out).
- **Opt-out.** Patient health information is available for sharing automatically. Patients must actively express their desire not to have information shared if they wish to prevent sharing. Patients may be automatically enrolled in the HIE but are given the opportunity to opt-out of having their information stored and/or disclosed.
- **Opt-out with exceptions.** Default is for patients' health information to be included, but patients can opt-out completely or allow only select data to be included. Patients are given the opportunity to:
  - Allow the exchange of their information only for specific purposes
  - Limit exchange of their information only for specific purposes
  - Limit exchange of their information to specific providers or provider organizations
  - Selectively exclude categories of data or specific data elements
- **Opt-in.** Default is that no patient health information is included. Patient consent is required for all patient health information to be stored and/or disclosed.
- **Opt-in with restrictions.** Default is that no patient health information is included, but the patient may allow a subset of data to be included. Patients have the option to:
  - Allow information to flow only to specific providers
  - Include only specific categories of data or data elements

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

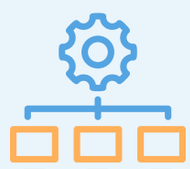
Provenance

Provenance is a metadata concept, which details:

- The origin of clinical information when first created
- Information about the source of the data — organization versus provider versus individual entering the data
- Information about what processing/transitions the data has undergone

There is considerable variability in how provenance is marked and retained in EHRs and HIEs. At the same time, there are different levels of:

- **Granularity** (document level versus section level versus data element level)
- **Practices when detailing the importing/exporting of data** (list original source versus modifying source to list importing organization)



Provenance is important considering that if it is captured using a standard methodology, it enables **segmentation of information based on source.** This segmentation **enhances trust** in the information exchanged between providers and the information received from a patient.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Covered Entities and Authorizations

The HIPAA Privacy Rule covers health plans, healthcare clearinghouses, and providers that conduct financial and administrative transactions electronically, such as electronic billing and fund transfers.

Covered entities are bound by privacy standards even if they contract with others (called "business associates") to perform some of their essential functions.

The HIPAA Privacy Rule requires covered entities to **enter into written contracts** or other arrangements with business associates, which protect the privacy of protected health information; but **covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards** or the extent to which the business associate abides by the privacy requirements of the contract. **Nor is the covered entity responsible or liable for the actions of its business associates.**

The Privacy Rule permits, but does not require, a "covered entity" to voluntarily obtain patient "consent" for uses and disclosures of protected health information for treatment, payment, and healthcare operations.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Covered Entities and Authorizations (continued)

By contrast, an **"authorization"** is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule.

Where the Privacy Rule requires patient authorization, **voluntary consent is not sufficient to permit a use or disclosure of protected health information** unless it also satisfies the requirements of a valid authorization.

An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or healthcare operations, or to disclose protected health information to a third party specified by the individual.

An authorization must specify a number of **elements,** including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Consent Delegation

Given the potential that a patient can be incapacitated, **users can delegate healthcare consent decisions** to an ecosystem of third parties, including relatives, legal guardians, lawyers, caregivers, friends, experts, groups, and, perhaps, AI entities (knowledge repositories used by bots).

Three distinct factors contributing to trust in a delegate relate to how the patient perceives:

- The delegate's competence or ability to make authoritative decisions
- The delegate's intention in the decision-making process
- The delegate's moral integrity

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

The selection of a delegate is usually based on either a pre-existing relationship of trust or a dependency (e.g., due to the lack of own knowledge in the field).

Delegation in this context means that the delegator expects the outcome to be in a range of "acceptable" options and hence predictable to a certain degree. As a result of these stable expectations, one can speculate that delegation within trust relationships leads to a reduction of complexity and uncertainty leading to an increased feeling of security.

Simply put, even if people delegate consent, they still want to feel like they are in control.

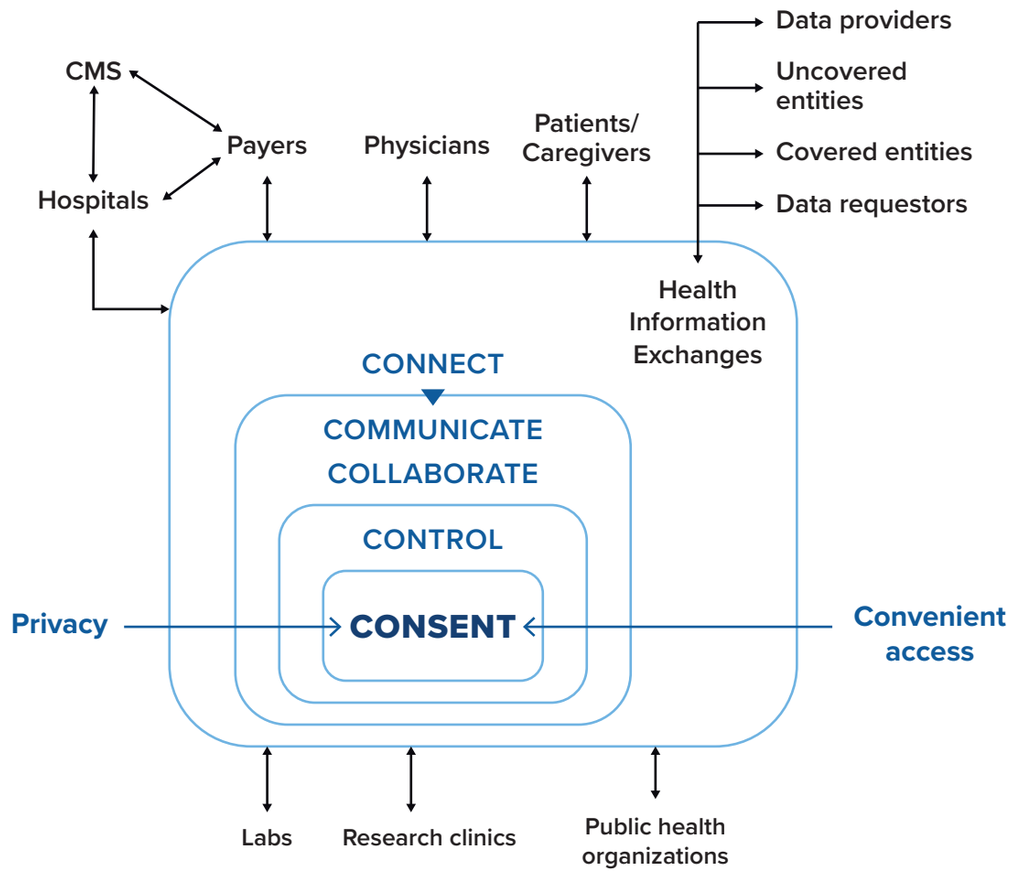
Data-Sharing Consent

With the consumer in mind, the most important aspects of data sharing incorporate three elements of transparency:

- What is individual control?
- Who has access — (device, person, application)?
- What is the intended use of the data?

Consent exists in a contradictory relationship between the users' desire for data protection privacy versus the necessity for services and their convenience.

Consent 2.0 Ecosystem



SECTION 2

Why Is a Consent Re-Think Important To Payers Now? What Are the Drivers Compelling Payers to Focus on Data-Sharing Consent?

Consent Drivers for Payers

Why are payers concerned about consent?

- Requesting and Providing Data
- Telehealth
- Cloud
- Interoperability
- Consumer Safety and Patient Satisfaction
- Wearables
- Mobile Technologies
- "Payviders" Sharing Care and Insurance Data
- Payers Sharing Data with Each Other
- Member Data Sensitivity
- Empowered Minors
- Public Health Information
- Genomics Data
- Delegation Over Time

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Requesting and Providing Data

The interoperability mandates' implementations at payers exposed the complexity of being **both a provider and requester of data to/from the healthcare community.**

Gone are the days where a payer fantasized about being the "data hub" around which all parties would revolve; payers are equal partners in this complicated data-sharing dance.

Although distributed, internet-based solutions (such as cloud-based systems) can already connect data requesters and data providers, the difficulty of ensuring compliance from both parties remains.

Data providers/sharers face the problem of unambiguously defining consent.

Data requesters face the issue of clearly stating their intentions.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Telehealth

A payer sponsors and/or pays for telehealth.

An agreement between the provider and the patient that is explicitly for telehealth services is **usually part of any consent portfolio.**

In fact, informed patient consent is a recommended best practice by the American Telemedicine Association (ATA) and can be put upon a provider by a payer as a condition of being paid, and it is a requirement in many states.

This agreement, covering overheard conversations, confidentiality, rights, disputes, security breaches, technical snooping, enabling/disabling recordings, risks of telehealth, and fees, is usually signed or verbally agreed to at the start of telehealth treatment.

The payer, having "sponsored" the telehealth network by directing the member to the telehealth services, has vague consent responsibility for the actual telehealth instance but has explicit responsibility for ensuring that the provider has consent in place as a requirement of being in the payer's network.

"Electronic forms" with "witnessed signatures" are the preferred method today of obtaining patient telehealth consent. Translating these forms, signatures, and witnesses into electronic "information" that is portable for enterprise use and transmissible to others is challenging for payers and their vendors.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:
Cloud

Payers are moving to the cloud, and ePHI is rampant throughout the architecture, both inside and outside the payer walls.

With the proliferation and widespread adoption of cloud computing solutions, HIPAA-covered entities and business associates are **questioning how they can take advantage of cloud computing while complying with regulations** protecting the privacy and security of electronically protected health information (ePHI).

For example, cloud-based systems store large data aggregates in datacenters. To move toward decentralized data-sharing models, individual users must be empowered to steer data-sharing practices.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Interoperability

With the 2022 interoperability mandates, consumerism and CMS combine to demand standards and access which drive data visibility and data exchange between payers, members, and providers.

Regulatory Change

An interoperable environment requires **a set of accurate payer data that will be made public,** and therefore must be accurate. This drives to Member360 as payers continue in their attempt to accomplish three goals:

- **Evolve claim engines,** separating commodity functionality from exception processing
- Recognize that **data homogenization and curation** is a necessary component of payer infrastructure
- Focus on **flexible security models** that can react to contact tracing, mobile device inputs, consent, and HIPAA flexing in response to consumer and vendor capability

Source: IDC Perspective's *Eight Drivers for Payer Interoperability Implementation, Now!*, Jun 2020

PAYER DRIVER:

Interoperability (continued)

Payers are forced to comply with the CMS interoperability mandates, and one can foresee that this is just the beginning of mandated data sharing.

CMS requires **four types of data** to be available to the member through open API (medical and drug claims data, clinical data possessed by the plan, current provider directory data, and formulary or preferred drug lists) **and forces plan-to-plan access.** HIMSS states that organizational (Level 4) interoperability includes:

- Governance, policy, social, legal, and organizational considerations to facilitate the secure, seamless, and timely communication and use of data both within and between organizations, entities, and individuals. These components enable shared consent, trust, and integrated end-user processes and workflows.

This can be extrapolated to imply that:

- All electronic health information (EHI) will have **provenance** (reference the preceding Provenance section) metadata.
- All EHI will have sensitivity **tagging.** Payers need mechanisms for identifying highly sensitive data, such as notes, procedures, and medications, related to behavioral healthcare, birth control, pregnancy, sexually transmitted disease, testing and treatment for HIV/AIDS, and other conditions. Interoperability does not yet require data segmentation, mainly because CMS decided the technical specs are not yet widely adopted. That said, CMS did indicate payers should anticipate data segmentation, and payers must prepare now for future filtering and masking of data types and highly sensitive data.
- Payers will need to **journal external data movements,** both received and sent, with traceability to consents and authorizations. Patients, personal representatives, and many internal users will need visibility into these consents and data movements ("Where have you sent my data in the last 90 days?").

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Consumer Safety and Patient Satisfaction

In response to consumerism and COVID-19, payers are focusing on patient safety, convenience, and satisfaction.

Payers and providers have always known that having a complete view of a patient's health through access to disparate data can better inform clinicians on the patient's medical history, preferences, and past encounters.

This can help avoid duplicate testing, reduce adverse events, inform care decisions, and facilitate appropriate follow-up to ensure adherence with care management.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:
Wearables

A payer sponsors and/or pays for wearables.

Wearable technologies are anticipated to have a major impact in the health sector as **physicians remotely receive updates** on patients' vitals. Wearables enable better patient monitoring, drug management, asset monitoring, tracking, and early medical interventions. In general, physicians, insurers, patients, and caregivers are anticipated to have unparalleled access to information.

On the one hand, companies can gather and trade data gleaned from smartphone sensors and wearables to learn of moods, stress levels, habits, well-being, sleep patterns, exercise, movement, and so forth to make decisions ostensibly about healthcare, but in the process are compromising privacy and possibly even erecting barriers to healthcare.

Additionally, information overload gets in the way of informed consent.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

The value of personal information is often not known when it is collected (i.e., when notice and consent are normally given); also, the relationship between users and processors of personal data has become increasingly complicated, as data sets are combined, transferred, shared, or sold. Consent notices that do not disclose the identity of third parties that can access user data forestall consumers' ability to provide genuinely "informed" consent. In addition, consent notices are often written so broadly or in voluminous detail that they inhibit users' comprehension, and thus render "conscious choice" meaningless. Such notices, which create the illusion of consent, often distract users from their own privacy protection.

In effect, consumers do not currently "share" data so much as they "surrender" consent to their information in the wearables space.

PAYER DRIVER:

Mobile Technologies

A payer sponsors and/or pays for mobile technology.

The interoperability mandate requires **data to be made available via API to whoever asks,** including developers inventing access via mobile devices.

Third-party applications that can serve as "vaults" of "personal health data" have been tried before, with spectacular failure. This failure was due to a lack of standards, a lack of government mandate, and a lack of interest by consumers to "put in the work" required to build and maintain their own version of aggregated data without common formats, interface standards, and user interfaces.

Now, with common API standards, mandated FHIR formats, and forced compliance to release meaningful data in a usable format to interested consumers, these **third-party applications become feasible, attractive, and potentially ubiquitous.**

Therefore, lots of data will be flying around, with lots of apps accessing, and lots of people looking at this data, and that data better be **correct and release consent assured.** If not: lawsuits, lawsuits, and more lawsuits.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

"Payviders" Sharing Care and Insurance Data

Payers are increasingly merging, acquiring, diversifying, and becoming "payviders," sharing care and data.

As covered entities, payers increasingly share data with providers and others to support the permitted purposes of treatment (e.g., care management and concurrent review), healthcare operations (e.g., quality management and reporting), and payment (e.g., prior authorization and claims adjudication).

In 2021 alone, Centene, Humana, Aetna, United, and Cigna have all been involved in merger or acquisition activity around melding care and insurance.

This means that traditional "insurance data" like administrative and limited care (care management, wellness) data will now merge with real "clinical" data, and the interoperation of this data will encourage the company's data culture to become more "health sensitive," evolving beyond just the limited PHI of the past.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Payers Sharing Data with Each Other

Payers increasingly share care data across other payers.

Care coordination and continuity of care are a focus of the CMS Interoperability Act.

For example, if Covered Entity A provides health insurance to an individual who receives access to the provider network of another plan provided by Covered Entity B, Covered Entity A is permitted to disclose an individual's PHI to Covered Entity B for care coordination, without the individual's authorization.

Similarly, if an individual had been enrolled in a health plan of Covered Entity A and switches to a health plan provided by Covered Entity B, Covered Entity A can disclose PHI to Covered Entity B, without the individual's authorization, to facilitate Covered Entity B's coordination of the individual's care.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Member Data Sensitivity

Consumers/members are increasingly sensitive about data disclosure.

Some federal and state laws require patient consent for the sharing of "sensitive health information." Some laws and frameworks recognize that certain health conditions may put individuals at a higher risk for discrimination or harm based on that condition.

Sensitive health information is defined as **specific types of health information or health information generated by a specific type of provider.** Some of the categories of sensitive health information that may receive increased protection are:

- **Subject of information** (e.g., alcohol and drug abuse, genetics, domestic violence, mental health, and human immunodeficiency virus [HIV]/acquired immune deficiency syndrome [AIDS])
- **Provider type** (e.g., substance abuse treatment provider)
- **Type of information** (e.g., psychotherapy notes)

This sensitivity is federally recognized. The ONC has sponsored the Behavioral Health Data Exchange Consortium, created to pilot the interstate exchange of behavioral health treatment records. Similarly, the ONC DS4P Standards and Interoperability Initiative strive to enable an HIE's varying disclosure policies to be implemented and managed in an interoperable way.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Empowered Minors

Minors are increasingly empowered around data disclosure and demand protection.

State and federal laws generally **authorize a parent or guardian access to adolescent/minors' health information.** Depending on age and health condition (e.g., reproductive health, child abuse, mental health) and applicable state law, minors also have privacy protections related to their ability to consent for certain services under federal or state law. Applicable federal laws are the Family Educational Rights and Privacy Act (FERPA), the Genetic Information Nondiscrimination Act (GINA), and Title X of Public Health Service Act.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

As a great example of unforeseen "data sharing consent" questions, FERPA was recently tested during COVID-19. The U.S. Department of Education was asked if a school could identify a particular student who has COVID-19 to parents and students in the school community without prior written consent.

The Department of Education responded:

> *School officials may determine that it is appropriate to disclose such information to parents or students if the disclosure is necessary to allow parents and students to take appropriate precautions. School officials should make this determination on a case-by-case basis, taking into account the totality of the circumstances, including the risks presented to the health of students or other individuals, and the need for such individuals to have the information in order to take appropriate actions.*

Note the wording. How can a set of codes be written to ensure "necessary," "appropriate," "case by case," "totality of circumstance," and so forth?

The specificity challenge around minors indeed makes it daunting to electronically and properly communicate the intent of consent.

PAYER DRIVER:

Public Health Information

Public health organizations are reaching out to payers.

In the context of COVID-19, before and after, there is a need for multi-provider geographic data about health to be available to public health authorities.

HIPAA is being tested. Payers, as good sources of multi-provider data, are being queried and are required to respond.

The Privacy Rule permits a covered entity or its business associate to use health information exchanges to disclose protected health information for public health activities.

This rule covers:

- Exchange for reporting of disease
- Exchange for the conduct of public health surveillance, investigations, and interventions
- Exchange subject to Food and Drug Administration (FDA) jurisdiction (device recall)
- Exchange for persons exposed to communicable disease and for related public health investigation
- Exchange in support of medical surveillance of the workplace

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Genomics Data

Genomic data is emerging as a legitimate health data set to payers.

As far back as 2014, NIH was concerned with the public perception of the uses of genomic data.

At the core of their policy is the expectation that researchers obtain explicit informed consent from study participants for the potential future use of their de-identified data for research and sharing.

They stated:

> *To simply de-identify data for research use without an individual's consent is no longer ethically justifiable. Broad consent and data sharing policies may assuage the ethical concerns and will facilitate access to greater volumes of data, reducing the costs and burdens associated with sharing research data.*

Of course, the genomic use case is more relevant to life sciences use cases (clinical trial or real-world data consent), but it can be foreseen that if a consumer chooses to release genomic information to a payer for a better value (reduction premium/lower deductible), that use case would be valid in insurance, complicating consent.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

PAYER DRIVER:

Delegation Over Time

Delegation to multiple parties over time is a requirement.

Future, complex consents, and authorizations will require the complexity of masking and filtering based on sensitivity labels and more. A member would not need or likely want to share, for example, her mental health data with an orthopedic surgeon to whom she's referred for ACL repair.

Technically, we need to **enable delegation to any party (permissions access) of control as if the patients (data access) were making decisions themselves.**

Nimble architectures, simple user interfaces, and tracking activity over time as people change their minds about consent and their delegates seems a minimum.

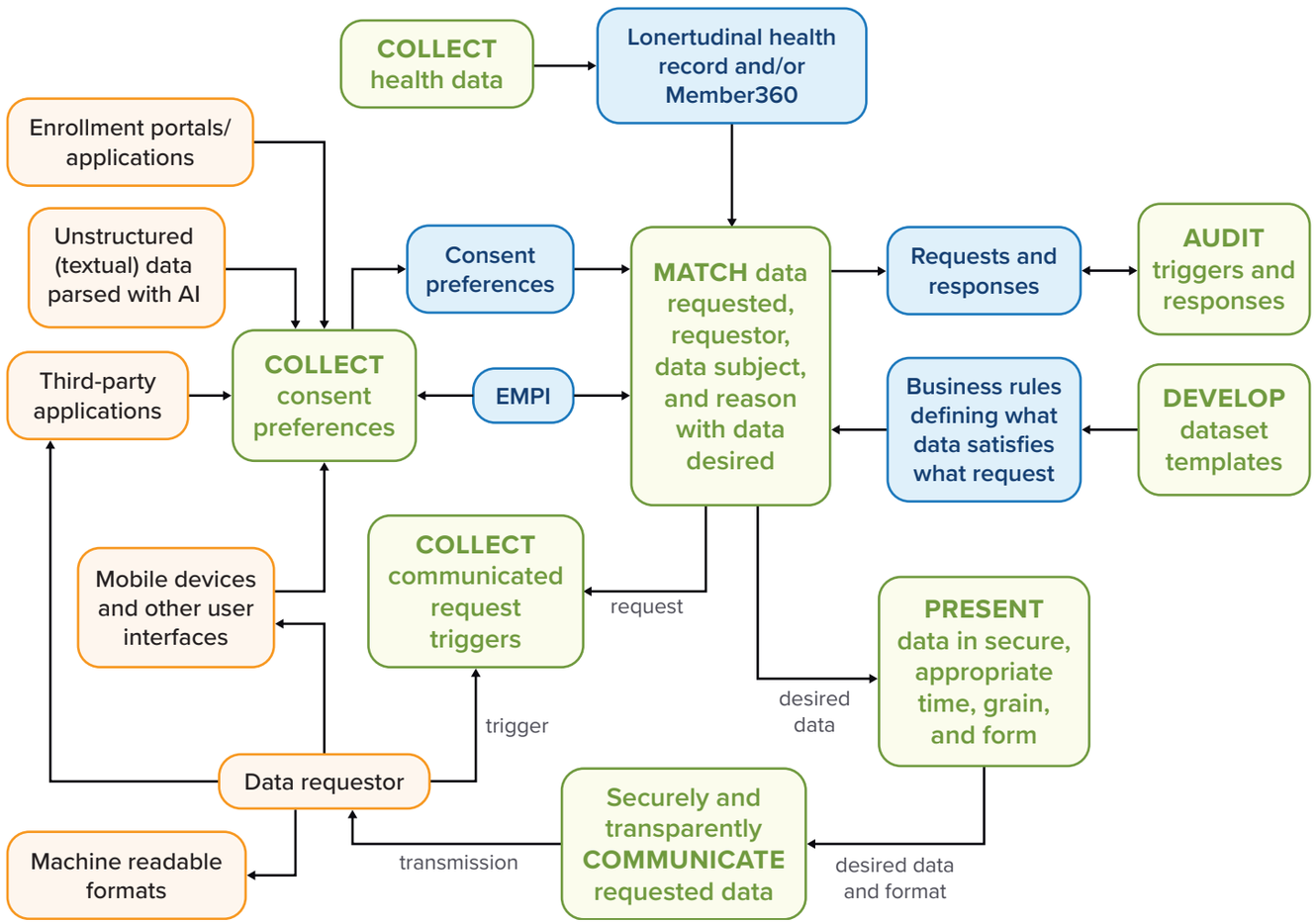
Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

SECTION 3

What Technologies Address Payer Data-Sharing Consent?

DATA-SHARING CONSENT:

Functional Requirements



To construct a consent-based model, payers should address the following questions regarding processes for:

- **Educating** consumers about consent, collection, and access
- **Collecting, cleansing, and matching** health data to one and only one person
- **Collecting and managing** (device, app, and person) consent, and maintaining a verifiable history of changes over time (provenance)
- **Representing** consent in a machine-readable way
- **Connecting** the users and allowing appropriate, efficient, secure, seamless access
- **Dynamically matching** the purpose of use of data requesters to the consent of data providers
- **Preparing** for audits and for proving the "state of being" at any time

Source: IDC's *Health Data Sharing Consent — An Architecture to Implement this new required Payer Technology*, June 2021

DATA-SHARING CONSENT:

Technologies

- Identity and access management
- Data ingestion, curation, and cleansing of data via ETL or advanced engines
- EMPI, an "enterprise" master patient index (a centralized, cross-platform solution designed to link/match and reconcile records in real-time, from diverse systems, to correctly assign records to a unique "person")
- Longitudinal health records in a Member360, data warehouse, data lake, and/or FHIR server
- Business rules engines
- Data encryption
- API management
- Data use logging and audit
- Content services platform with workflow capability

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

SECTION 4

Parting Thoughts on Connected Content for Healthcare

Consent Is Creating a New Set of Requirements

Payers collect and generate large amounts of information. Much of it is in the form of digital documents or unstructured content, and a consequential amount is still on paper. This information ends up disconnected from payer business processes. Workarounds are required to manage unstructured content, and manual processes can be fraught with inefficiency and error, especially when content must be shared across departments.

The challenge of managing unstructured content increases costs, leads to member abrasion, and negatively impacts other stakeholders. When payers can connect processes across the organization and provide access to unstructured content, they become more efficient, reduce costs, and improve relationships with employers, providers and members, and simultaneously better prepare themselves to support interoperability requirements.

As we have seen, consent forms, signatures, text, website clicks, portal sign-ons, intake documents, enrollment processes, and countless other inputs drive the consent process, and none are standard. Payers are required to obtain, cleanse, match, store, and track this data and document content in a coherent, auditable way. **Reconciling federal and state controls with consumer demands for transparency will be the payer challenge of the next decade** in a reinvented "Consent 2.0" paradigm.

Source: IDC's *Health Data Sharing Consent — What it is and Why Payers Should Start Afresh*, May 2021

Consent Is Just One "Use Case" for Connected Content

Payers must manage many other use cases demanding that unstructured data be coordinated and merged to enable seamless workflow processes and integrated data. A robust content services platform manages these use cases and all other unstructured content for member communications.

Medicaid Referrals

The ability to review form content and route for referral determination with decreased human intervention.

(Medicare Advantage or Medicaid) Transportation

Facilitating the forms and processes to enable care transportation.

Appeals and Grievances

Receipt, investigation, and determination with decreased human intervention and standard letter generation and reporting.

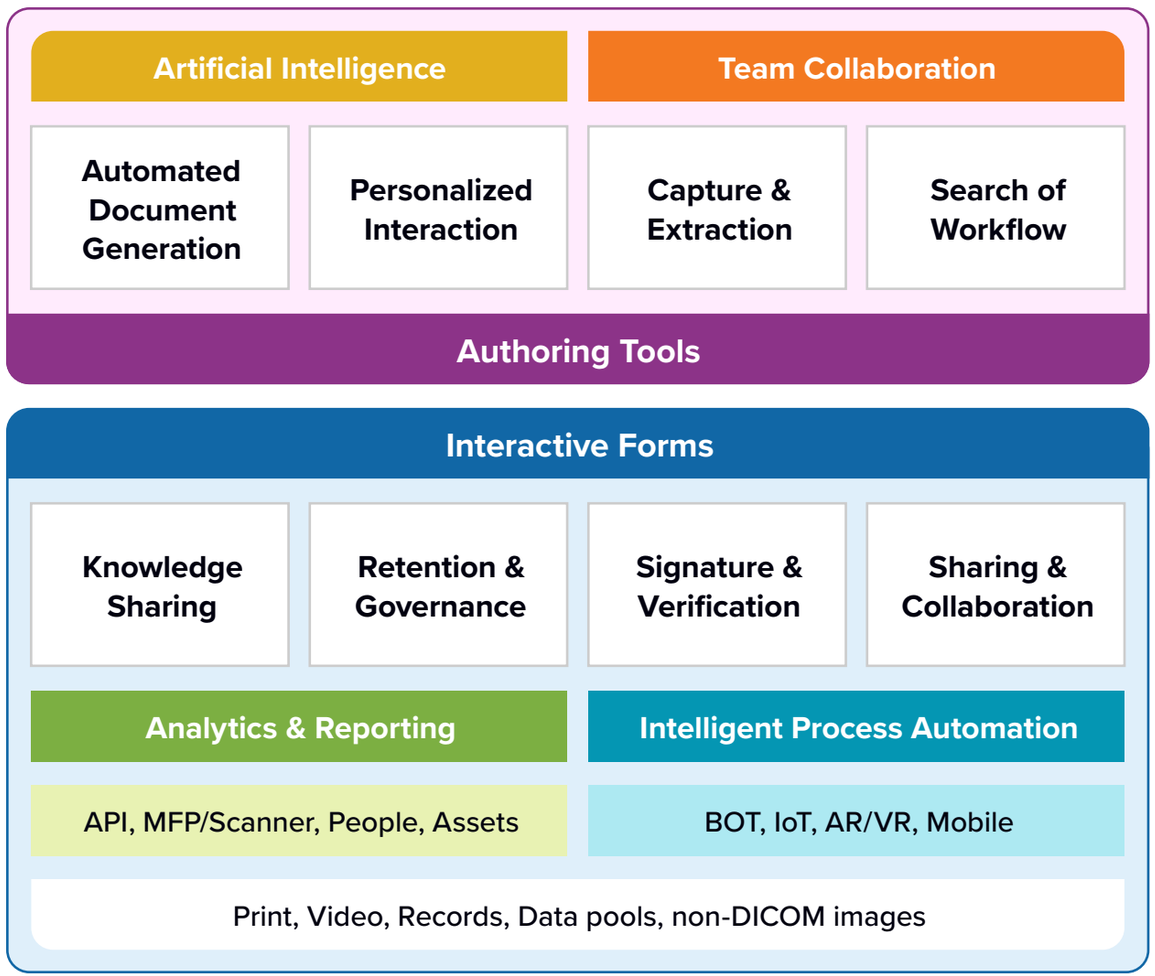
Medical Record and HEDIS Request Tracking

The ability to route and store medical charts for validating HEDIS scores.

Connected content strategy is indeed enterprise-wide and is rivaling the overall "data is an asset" mentality that is driving payers to hire Chief Data Officers to complement their Customer Experience Officers.

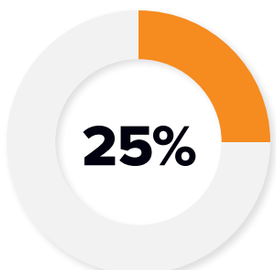
Connected Content Workflows and Use Cases

- **Enterprise content strategies** include the rapidly evolving digital content services to capture, manage, process and secure business content, records and knowledge.
- **Document applications** enable users to create, author, edit, and publish content, including spreadsheets, text documents and presentations. Applications include office suites, forms, surveys, eSignature, diagramming, eLearning and document generation software.
- **Capture applications** convert unstructured data to structured information that can be passed to another enterprise application and/or consumed by a downstream task or process.
- **Content sharing and collaboration** applications enable users to store, synchronize, and share file-based content and folders across designated devices, people, and applications.
- **Enterprise content management** provides a foundation for regulatory compliance in context of automating content-centric business processes and establishing a system of record.



Making the Case for Connected Content

IDC predicts that by 2025, **80% of the total global datasphere will be in the form of unstructured data,** which will grow to 144.3 zettabytes.[1]



of healthcare organizations indicated that **leadership and commitment of top management as well as people with technology skills are necessary for successful DX** to occur in order to drive data excellence in a digital-first health IT strategy.[2]

Organizations need to **use DX to connect clinically relevant information** across the healthcare enterprise from the following sources:

- Business content
- Financial and claims data
- Medical imaging data and content
- Medical device data
- Interoperability of patient data from external providers
- Social determinants of health data
- Patient-generated health data
- Real-world data and evidence
- Research and academic data
- Consumer data

Source: **1.** Worldwide Global DataSphere and Global StorageSphere Structured and Unstructured Data Forecast, 2021–2025, July 2021. **2.** IDC's *Digital Transformation (DX) Executive Sentiment Survey 2021,* May 2021

Benefits of Connected Content

Digitize manual processes

Transitioning to cloud content management improves business continuity, especially in light of process gaps exposed during the COVID-19 pandemic. Examples include business functions such as accounts payable, invoice processing and sales order processing.

Improve content accessibility

Difficulty finding the information needed to perform job specific tasks was one of the key drivers for organizations to digitize document workflows. Employees and external stakeholders need secure access to data and information independent of their location or device to perform work tasks and collaborate across people and processes.

Unlock value and insight

Data is a key enabler for customer engagement as organizations harness valuable business insights to deliver real-time nd personalized experiences. Customer experience investments drive 5X the return. Providing structured, unstructured, and medical imaging data to drive workflow automation solutions allows for AI utilization to assist in generating powerful insights from content workflows.

n = 700, Source: IDC's *US Enterprise Content Strategies — Use Cases Survey,* December 2020. n =791, Source: IDC's *Future Enterprise Resiliency & Spending Survey,* July 2021.

Next Steps

Connected content offers a way forward for healthcare payers to deliver better healthcare services and improve outcomes. Information from non-clinical and unstructured data sources can impact many aspects of payer operations, including experience, growth, efficiency, productivity, resiliency, security, and compliance.

1. Rally the C-suite, clinical, and operational leadership around an impetus to shift from data-rich to information-driven
2. Formulate a connected content mission as part of the broader vision and strategy for data-driven governance
3. Execute tactics and objectives to increase the organizational maturity on utilization of connected content enterprise-wide, such as through use of a content services platform
4. Identify silos that can be streamlined internally and ways to connect content externally from disparate systems
5. Adhere to protocols that proactively promote and ensure connected content consistency, quality, reliability, and integrity
6. Implement policies and training that meet connected content compliance and regulatory standards without compromise
7. Deploy privacy and security measures that ensure connected content is always secure, protected, and resilient
8. Advance continuous learning and improvement methods that drive connected content value and utilization over time

About the Analyst

Jeff Rivkin, M.Sc, PAHM, CHRS, CPEHR, CBIP, CCP, CDP
Research Director, IDC Health Insights

Jeff Rivkin is the Research Director of Payer IT Strategies for IDC Health Insights. He is responsible for research coverage on payer business and technology priorities, constituent and consumer engagement strategies, technology and business implications for consumer engagement, front, middle and back-office functions, value-based reimbursement, risk, and quality-based payment and incentive programs, among other trends and technologies important to the payer community.

More about Jeff Rivkin

Message from the Sponsor

Hyland Healthcare provides connected healthcare solutions that harness unstructured content from all corners of the payer organization and link it to core applications. Hyland Healthcare offers a full suite of content services solutions, bringing documents and other relevant data to the stakeholders that need it most. This comprehensive view of information along with workflow automation and low-code development tools help payers accelerate business processes, increase efficiency, reduce costs, and improve relationships with employers, providers and members.

For more information, visit www.hyland.com/healthcare

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC @idc @idc idc.com