Four Considerations Around Sensitive Data

Healthcare organizations carry as much responsibility in managing patient data, as they do in delivering care. They must continuously refine their data management system to protect sensitive information while ensuring it's accessible to the correct users.

The balance between full access and compliance

As healthcare becomes more integrated, providers need access to the patient's traditional medical records (PCP, hospital, etc.), dental, and behavioral health information. Viewing a patient's entire medical history helps ensure complete and accurate clinical decisions. However, access to this data must be balanced against complying with regulatory requirements, consent rules, and sensitive data protection.

One significant federal regulation is 42 CFR Part 2, which regulates the documentation and exchange of data from substance use treatment centers. "Part 2" has been revised to further facilitate better coordination of care in response to the opioid epidemic while maintaining its confidentiality protections against unauthorized disclosure and use. The improper handling or exchange of data according to "Part 2" carries substantial financial penalties for organizations that do not adequately protect the patient's data.

Ensure access to data when it's needed

Because of the nature of healthcare and interoperability requirements, it's not enough to just protect the data. It needs to be securely shared among medical organizations and providers. Collaboration and a robust framework ensure information is accessible to providers at the time it's needed—at the point of care.

As with many strategic imperatives, success begins with a plan of action. These recommendations will help you build a framework to manage sensitive data.

Four considerations

1 Determine the who, what, and where:

- Who will receive the sensitive data and the authorization needed?
- Where will the data end up?
- What classes of data are you sending and receiving? This could include:
  - Substance use disorder diagnosis or treatment information
  - Behavioral/mental health (notes, diagnosis codes, procedures, medications, etc.)
  - STI/STD/HIV
  - Minor patient information
  - VIP (celebrities, politicians, or other notable public figures)

Tip: Mirth® Health Data Hub *by NextGen Healthcare* enables you to build patient views which may include or exclude sensitive data—based on permissions, rules, user roles, and more.

nextgen® healthcare

2 Plan early and recruit allies:

- Start with your privacy and security team—it's essential for your technical, clinical, and regulatory teams to collaborate
- Identify the specific use case and value proposition of the exchange and retention of sensitive data—who are the specific users, who has access to the data, and how will they benefit from the data?
- Identify the "minimum necessary" data type and the values you need

3 Plan how you'll record, enforce, and exchange patient consent preferences:

- Will patients opt-in or opt-out of the data exchange?
- Will patients be able to set expiry dates for consent?
- Will patients be able to identify specific providers and/or organizations that can access their data?

4 Start small and test often:

- Ensure you have good requirements defined as you begin to build the interface and configurations that are required
- Test with your internal team and recruit actual end-users for testing and verification
- Write test cases that mirror common and uncommon scenarios in the real world **(edge-cases are everything)**

Exchange data securely

Beyond these considerations to meet ethical, legal, and clinical obligations, you need a scalable, integrated, and intelligent information exchange solution supported by a dedicated team of healthcare data exchange experts.

Mirth Health Data Hub is a central data repository that collects, organizes, and aggregates clinical data from many different sources. This data is used to produce a longitudinal record, which can be easily viewed from a web-based provider portal or accessed via an open application programming interface (API).

Protection features of Mirth Health Data Hub

Mirth Health Data Hub's Protected Data features allow you to meet 42 CRF Part 2 requirements and can support all local state guidelines for substance abuse disorder data segregation. The **Patient Groups** features will allow you to create cohorts of interest from various sources and formats, such as Patient Attribution Files (payer or practice), ACO Patient Rosters, Medicaid/Medicare Beneficiaries, and more.

These logical lists can be sent to Mirth Health Data Hub in multiple formats such as HL7 ADT, Claims Files, CSV/ Excel, among others. These logical patient lists can then be used as filters for other parts of the application, such as controlling the patients that a user has access to.

One of Mirth Health Data Hub's benefits is that these configurations and data protection settings only need to be set up one time. They can also be enforced regardless of the data exchange mechanism: API, User Portal, Document Generation, or HL7 interface.

Layered security approach

Healthcare organizations need a vendor that takes multiple security considerations into account. In addition to satisfying standard expectations, a well-architected framework supports good outcomes and enables a continuous-software-delivery pipeline. The result is a layered security approach—similar to that of an onion, where layers of security measures need to be peeled back before the data can be accessed.

BETTER STARTS HERE.

Contact us at **855-510-6398** or email **results@nextgen.com**.

1 Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule, July 13, 2020, https://www.hhs.gov/about/news/2020/07/13/fact-sheet-samhsa-42-cfr-part-2-revised-rule.html

CH_053023_SensitiveData