mro™

Fast Focus

Payer Direct Access to Provider EHRs

Managing EHR Access to Protect Patient Data

Health system leaders face a conundrum of issues regarding the clinical exchange of their patient data. CMS regulations require a broader exchange of information across the healthcare ecosystem while recent massive breach events heighten privacy and security concerns. Furthermore, third-party payers' requests for clinical data (and denials) are on the rise.

Yes, payers' requests for information are authorized for treatment, payment or operations (TPO), but HIPAA's minimal necessary rules still apply. To address these demands, healthcare provider organizations (HCOs) are seeking new, efficient ways to exchange information in a digitized age.

Enter the emerging practice of granting payers direct access to providers' EHRs.

Granting payers direct access to the EHR is positioned to relieve administrative burdens, reduce operational costs, minimize payer-provider friction, and provide a quick win during managed care contract negotiations. However, not all health systems that grant payers access to their EHR data realize these promises and may, in fact, experience unintended consequences such as higher denial rates or unauthorized access to protected health information (PHI).

This Fast Focus Brief explores the pros, cons and real-world experiences associated with exchanging clinical data with payers. In partnership with the *College of Health Information Executives (CHIME)* and *Healthcare Financial Management Association (HFMA)*, MRO shares the following insights for revenue cycle management, finance, IT, compliance, and health information management (HIM) leaders to maintain control over payers' access to patient data.

CHIME Survey Reveals Five Insights About Payer Access to Provider EHRs

A survey of 181 qualified respondents was conducted by CHIME and MRO in early 2024. Respondents included IT, health information management (HIM), finance and revenue cycle leaders. *Full results were published by CHIME in July 2024.*[1]

Here are five key insights to know.

- Most HCOs exchange clinical data with payers via third-party solutions or modules within the EHR.
- Payers are commonly granted access to EHRs for care management, quality submissions, claims adjudication, claims appeal, payment integrity audits, prior authorization, and *risk adjustment*.
- Direct payer access to EHRs could be a good practice, but it must be done right.
- It is unclear who owns responsibility for payer access to the EHR and four specific departments are burdened with the aftermath of these decisions: IT, business office, HIM, and payer/managed care directors.
- These same departments often experience operational challenges and privacy concerns when payers are granted access to the organization's EHR.

[1] https://mrocorp.com/case-studies/navigating-the-complexities-of-clinical-data-exchange-a-survey-based-analysis-by-mro/

> "HIPAA's minimum necessary rule still applies, and HCOs remain responsible to protect patient information, even when exchanging data with payers as part of treatment, payment, and operations."
>
> **Anthony Murray** | Chief Interoperability Officer

Payer Requests for Your EHR Data: Unpacking the Who, What and Where

Now is the time for health system leaders to re-evaluate their organization's policies related to granting payers direct access to their EHR data. New checks, balances, and guardrails are indicated. Proper monitoring means knowing who is reviewing the record, what data they are reviewing and the reason for the review.

For example, specific data elements and templates for each use case are not always defined. And in some EHRs, direct access is an "all or nothing" proposition; systems lack the ability to limit access by use case.

Finally, since direct payer access technology is frequently misunderstood, there are gaps in ensuring compliance with HIPAA's minimum necessary rule.

Here are seven questions to ask about the who, what and where of payers' direct access to your EHR data.

- What is the reason (use case) for the payer's review?
- Who at the payer location is accessing your EHR data and reviewing the records?
- What specific data elements and use cases are accessible to the payer?
- What information are they viewing versus what information they need for each use case?
- What is the outcome of the review?
- If payers have direct access, is the volume of requests for information from payers subsiding and the operational costs to fulfill these requests reduced?
- Where is the payer storing your EHR information after they complete each specific task?

Three potential misuses of payers' direct access to your EHR data.

- Payers could take advantage of open EHR access to download more information than what was intended by the HCO.
- Payers could use unapproved use cases to see encounter data outside of the current episode or specific task.
- Other third parties might inadvertently obtain access protected patient information (PHI) intended exclusively for TPO.

> "If I'm negotiating with a payer and providing additional access, I should never receive an 835 denial that's requesting data because the payer has access to [the data]. If I'm going to do all this work to make sure the payer has all the information just so they can deny the claim, what's the point?"
>
> **Sheldon Pink, MBA, FHFMA, LSSBB** | Methodist Health System

HFMA Roundtable Shares Real-World Insights and Experiences

MRO convened the aforementioned group of nine hospital and health system leaders to discuss clinical data exchange with payers. Attendees shared valuable insights regarding the pros, cons, and lessons learned with granting payers' access to their EHRs.

Here is what they had to say.

"We opted to reduce our employees' manual labor by granting EHR access to our value-based care payers. **Without this access,** we are required to provide supplemental data, which we used to submit manually. **It is a time-consuming and tedious process.** It was our corporate decision to grant payers access to pull the data they required for submission to CMS. All payers with EHR access are **restricted to accessing their own member population only.**"

Juliet Santos, MSN, APRN, FNP-BC | AdventHealth Mid-America

"We are pushing for payers to come to the table and have greater accountability. We want to see the **true value** of allowing EHR access, which is **still unclear** at the moment."

Christopher Ballesteros | Peterson Health

"Our main focus in this evaluation [of payer direct access] is **safeguarding patient information.**"

Brittany Roth, CHFP, CRCR, CSMC | Phelps Health

"**We are not providing direct EHR access to payers.** Our question is, 'Will there be any benefit to us?' The payers are going to have to come to the table and **offer something that makes it mutually beneficial,** such as reducing denials and helping our staff be more efficient."

Amy Hayes, MBA, CCS, CCS-P | Great Plains Health

"Claims adjudication was a manual process, but now they [UnitedHealthcare] should be able to relieve our burden by pulling the information they need themselves. **Hopefully, it will save us money, but it's too soon to know** if we've achieved any reduction in administrative burden."

Dolores Perez | Inova Health System

"It is **difficult to correlate** whether overall increases in denials are **due to payer access.** You have to look at the denials, because you could get a denial for missing a modifier. If you update the modifier, then the payer might request medical records. Even after the pandemic, Blue Cross Blue Shield of Nebraska would pay a clean claim within five days, but that's unheard of anymore. It's like denials are used as delay tactics."

Sheila Augustine, FHFMA, MHA, CRCL | Nebraska Medicine

"For our value-based organization, we receive payment upfront, but for us, the **concern was security.** There is a substantial amount of sensitive information, so we've figured out other ways to provide the data."

David Lombardi | Emcara Health

Finding a More Efficient Path to Clinical Data Exchange with Payers

Interoperability in healthcare is the new standard, however, compliance, patient privacy and information security must still be maintained. These are three primary concerns related to payer access to providers' EHRs.

Prevention begins by establishing data sharing guardrails to protect patient privacy while also enabling data exchange and interoperability in healthcare. MRO is a proven company with best practices to achieve this balance.

The use of third-party partners like MRO to facilitate information exchange with payers provides a safer path to achieving the goals first mentioned in this Fast Focus Brief:

- ✓ Relieve administrative burdens
- ✓ Reduce operational costs
- ✓ Minimize payer-provider friction
- ✓ Protect patient data
- ✓ Minimum necessary data sharing

MRO works with HCOs to promote the safe sharing of clinical data while also building strong guardrails to protect patient information and ensure compliance with HIPAA's minimum necessary rules.

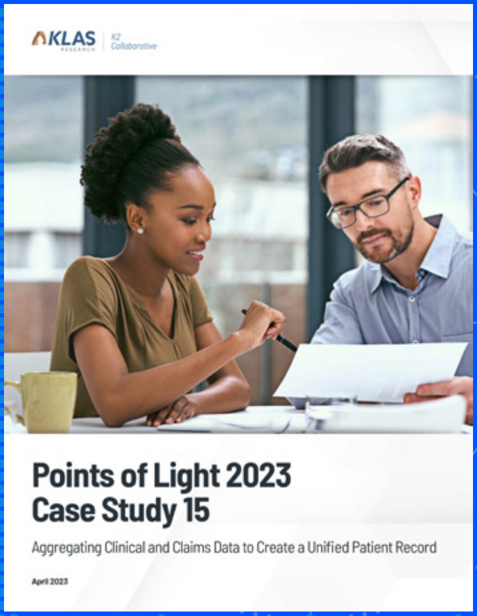
We are champions of patient privacy and relentless advocates for good, thoughtful information exchange.

mro™ Accelerating Clinical Data Exchange™

Interested in learning how MRO partners with both providers and payers to accelerate the exchange of clinical data?

Read the Points of Light 2023 Case Study, completed in partnership with KLAS.

https://mrocorp.com/white-papers/points-of-light-2023-case-study/



KLAS RESEARCH | K2 Collaborative

Points of Light 2023
Case Study 15

Aggregating Clinical and Claims Data to Create a Unified Patient Record

April 2023

MRO CONFIDENTIAL AND PROPRIETARY INFORMATION. This document and its contents are a confidential communication to, and solely for the use of, the intended recipient. No part of this document may be disclosed to any third party, in any manner, without the prior written consent of MRO.