THE Download

A monthly webinar diving into the intersection of healthcare and technology

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

March 20, 2024

Copyright 2024

Katy Lewis

Director of Marketing Operations & External Communications

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

Copyright 2024

Michigan Health Information Network Shared Services (MiHIN)

MiHIN is a non-profit organization that provides technology and services to connect disparate sectors to securely, legally, technically and privately share health information.

An unbiased data trustee, MiHIN does not provide health care services or produce health care data.

Instead, we help convene to share vital health information to advance care, better outcomes and lower costs.

Copyright 2024

Navigating the Changing Health IT Landscape: *2024 Public Policy Updates*

Shreya Patel | Chief Policy & Privacy Officer
shreya.patel@mihin.org

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

Shreya Patel

Chief Policy & Privacy Officer

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

Copyright 2024

Meeting Agenda

42 CFR Part 2

- Align Part 2 with HIPAA and CARES Act

CMS Interoperability Rule

- Provider Access API
- Prior Authorization
- Payer to Payer Exchange

TEFCA Updates

- Common Agreement
- Standard Operating Procedures

Copyright 2024

42 CFR Part 2 Updates

Agencies Responsible for Proposed Rule

- Office of Civil Rights (OCR)
- Substance Abuse and Mental Health Services Administration (SAMHSA)
- Health and Human Services (HHS)

Copyright 2024

Purpose

When the HIPAA Privacy Rule was finalized in 2000, they did not contemplate a healthcare landscape in which HIPAA and Part 2 would apply simultaneously to an organization. This has clearly not been the case and has resulted in confusion, dual obligations, lack of care coordination, and siloed information

Copyright 2024

Consent Updates

- Consent Requirements
- Aligns Part 2 consent with HIPAA Authorization requirements:
    - The identity of the discloser
    - The recipient
        - Can be a class of persons
    - The description of the information to be disclosed
    - The right to revoke consent
        - Only for future disclosures
    - The expiration of consent
  - Can use a single consent for all future uses and disclosures until the patient revokes in writing
    - Written can mean electronic signature
    - A program *can* accept oral revocation (documented)
  - Change “disclosure” to “*use* or disclosure”
    - Use is largely seen as an internal function when Part 2 information is received
  - If consent is in place with Part 2, CE, or BA, that entity can use for healthcare operations during audits
  - Allows more granular consent, but does not require it

Copyright 2024

Rediscloure Requirements

Two permissions for redisclosures:

- Part 2, CE, or BA that receives records with a written consent for TPO can redisclose for any manner permitted by the Privacy Rule except for Legal proceedings

- Permits a lawful holder that is not Part 2, CE, or BA to redisclose for payment and healthcare operations to its contractors, subcontractors or legal representatives

Copyright 2024

Accounting of Disclosures

Accounting of Disclosures with Part 2 Consent:

- Maintain accounting and provide for three years prior to request

Copyright 2024

Permissions and Restrictions on Disclosures

- Cannot limit a patient from restricting use of their records for treatment, payment, and operations
- Cannot limit restrictions from patient on sharing with health plan if it is self pay
- Cannot limit a covered entity's choice to obtain consent to use or disclose records for TPO
- Can report Part 2 information to Public Health authorities so long as information is deidentified

Copyright 2024

Restrictions on Use of Disclosure in Civil, Criminal, Administrative & Legislative Proceedings Against Patient

- Information obtained through patient access may not be used for criminal charge or investigation against the patient
- Cannot submit testimony with Part 2 information on a patient absent a court order neither
- If the patient opens to door to use this information in a case or trial, it can be used
- Court order
  - Preventing serious bodily injury
  - To prosecute the patient for serious crime
  - In connection with litigations or administrative hearing when patient introduces the records themselves

Copyright 2024

Civil Monetary Penalties for Violations

- Investigative agencies (those investigating Part 2 facilities) that act with reasonable diligence when discovering Part 2 records through their normal course of work may not be subject to civil or criminal penalties
    - They must apply for a court order after discovering the information for use of it

Copyright 2024

Incorporate HIPAA into Part 2

- Align definitions and terminology
- Capacity
  - Add health plans to the list of entities to which a program may disclose records without consent when a patient lacks capacity
- Research deidentification is held to same standards as HIPAA
- When Part 2 information becomes part of a Designated Record Set, which is usually is, it is considered PHI and subject to HIPAA
- **Psychotherapy notes, which can be derived by Part 2 programs as well, are still entirely protected and require separate written authorization and consent by the PROVIDER**
  - Patient does not have a right of access here
- Security provisions to safeguard Part 2 records are aligned with HIPAA
  - They would like Part 2 to take on greater accountability
  - They would like Part to develop formal policies & procedures
  - Same notification requirements for breaches as HIPAA

Copyright 2024

Update Notice of Privacy Practices

- Written in plain language
- Header
- Summary
  - Summarize federal law that protects them
  - When Part 2 can share information
  - Violation of this is a crime
  - Statement on a patient's commission of a crime on the premises is not covered
  - Suspected child abuse and neglect is not protected
  - Cite to federal law
- Uses and Disclosures
  - TPO with consent
  - Must get consent before using for fundraising on behalf of program
  - References the restrictions on use and disclosure of Part 2 records in civil, criminal, administrative, and legislative proceedings against the individual
- Individual Rights
  - Can inspect and obtain copy for limited or free cost or send to third party
  - Can restrict TPO disclosures
  - Can restrict disclosure for self pay
  - Can request accounting of disclosures
  - Can obtain copy of notice upon request
  - Can discuss with contact person
  - NOT required to provide written consent or authorization in order to access their own records
- Duties of Part 2 Programs
  - Maintain privacy and security of systems
  - Responsibilities for breach
- How to File a Complaint
- How to Revoke Consent
- Contact and Effective Date
- Optional elements
  - Limited uses and disclosures e.g. required by law or emergency treatment
- Must redistribute when updated
- Be given as soon as possible after emergency treatment
- Posted in a clear prominent location
- Do NOT withhold notice from inmates

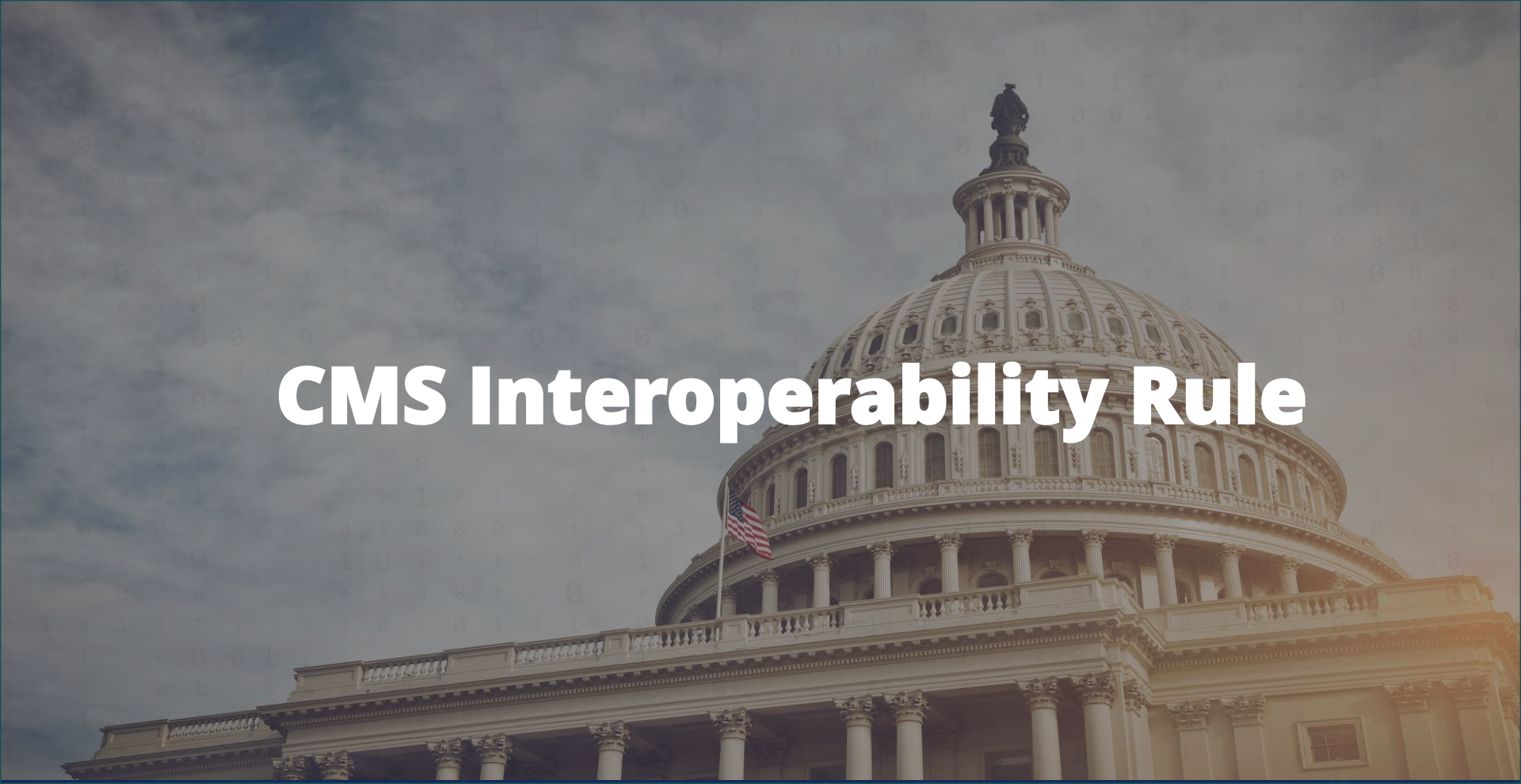
Copyright 2024

Other Areas the Proposed Rule Addresses

- Cannot take action against someone who files a compliant under Part 2
- Cannot ask patients to waive the right to file a complaint in exchange for treatment, enrollment, payment, or eligibility
- Business Associates can be considered Qualified Service Organizations if they receive records to work on behalf of Part 2 facilities
- Begin sharing Part 2 information with the Armed Forces and Veterans' Affairs
- Minor Patients: Differentiates that this is when a program is making an evaluation on a minor's capacity versus when a court is making a determination of a minor's capacity. This allows parents to be notified of the program's assessment and the minor's treatment
- Undercover agents and informants: Cannot employ an individual undercover and allow them to use Part 2 information in case unless under a court order
- Discontinued Programs- records do not need to be destroyed if transfer, retrocession, or reassumption occurs under ISDEAA (Indian Education Assistance Act)
- Program Audit or Evaluation
    - Federal, State, and Local audit permits Part 2 disclosure when mandated by law if deidentification would not be proper
    - May rely on a patient consent for TPO under healthcare operations but may not be feasible so allows for exception above
    - Medicare, Medicaid, and CHIP audits and evaluations included

Copyright 2024

CMS Interoperability Rule



Copyright 2024

Prior Authorization

Background: This new rule is seen as an expansion of the CMS Patient Access Rule, which was released in 2020, and required certain payers to provide individuals' own healthcare information to them via Fast Healthcare Interoperability Resources® (FHIR®) application programming interfaces (APIs).

Copyright 2024

Prior Authorization

What the New Rule Requires: Certain payers will be required to build on their FHIR infrastructure to implement and maintain FHIR APIs to streamline prior authorization processes. This will be done by requiring payers to have an API, which fully integrates into an existing EMR, and is able to select the appropriate pieces of information needed for a prior authorization request in an automated manner.

Copyright 2024

Prior Authorization

Why This Rule Was Proposed and Finalized: CMS is attempting to alleviate the administrative burden and workload surrounding prior authorizations. They are also trying to automate this process so the turnaround time on requests will not be as long as they are today

Copyright 2024

Prior Authorization

Which Payers are Required to Comply: Medicare Advantage (MA) organizations, state Medicaid and Children's Health Insurance Program (CHIP) Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally Facilitated Exchanges (FFEs), (collectively "impacted payers")

Copyright 2024

Payer Requirements for Prior Authorization

- Payers must be certain prior authorization information available via Patient Access API
  - All prior authorization requests and decisions for items and services (excluding drugs) for which the payer has data
  - Prior authorization status: whether the decision is still pending, active, denied, expired, or is in another status
  - Date the prior authorization was approved or denied
  - Date or circumstance under which the authorization ends
  - Items and services approved
  - Quantity used to date under the authorization
  - Any materials that the provider sends to the payer to support a decision
  - Specific reason for denial

Copyright 2024

Payer Requirements for Prior Authorization

- Payers must implement and maintain a FHIR Prior Authorization Requirements, Documentation, and Decision API (PARDD API)
- Payers must automate the process to determine whether a prior authorization is required for an item or service
- Payers must be able to allow providers to query the payer's prior authorization documentation requirements and make those requirements available within the provider's workflow
- Payers must support an automated approach to compiling the necessary data elements to populate the HIPAA-compliant prior authorization transactions and enable payers to compile specific responses regarding the status of the prior authorization, including information about the reason for a denial
- Payers must respond to prior authorization requests within 72 hours for expedited requests and seven calendar days for all others
- Payers must require impacted payers to publicly report certain metrics about their prior authorization processes for transparency (aggregated, deidentified)
  - The total number of unique patients whose data are transferred via the Patient Access API to a health app designated by the patient
  - The total number of unique patients whose data are transferred more than once via the Patient Access API to a health app designated by the patient

Copyright 2024

Prior Authorization Clarifications

- CMS proposed payers share the same information about prior authorization requests and decisions with a patient's provider via the Provider Access API and via the Payer-to-Payer API, and of course PARDD
- The prior authorization rule will NOT apply to drugs of any type that could be covered by an impacted payer, including, for example, outpatient drugs, drugs that may be prescribed, drugs that may be administered by a provider, or drugs that may be administered in a pharmacy or hospital
- PARDD information must be available in the Patient Access API as long as the authorization is active and at least 1 year after the last status change
- Relation to Right of Access – Privacy and Security of Apps
  - Covered entities and business associates would be free to offer advice to patients on the potential risks involved with requesting data transfers to an app or entity not covered by HIPAA, but such efforts generally must stop at education and awareness or advice related to a specific app
  - FTC enforces the FTC Health Breach Notification Rule, which covers most health apps and similar technologies that are not covered by HIPAA, and therefore, not subject to the HIPAA Breach Notification Rule
  - Payers will need to consider intersection of information blocking rule and patient access

Copyright 2024

Provider Access

What the New Rule Requires: This final rule would give providers access to the same information patients receive access to in the Patient Access API. This is inclusive of USCDIv1 and all Prior Authorizations decisions aforementioned. Payers will need to make this information available to them and it will be a requirement for payers.

Copyright 2024

Provider Access

Patient Attribution as a Key Component: This rule does emphasize that providers are not to receive information on a patient if they are not actively caring for that individual or otherwise a part of their active care team. CMS suggests utilizing existing provider- patient attribution frameworks. HIEs and HINs are pivotal in helping with this piece of compliance as they have comprehensive attribution processes.

Copyright 2024

Provider Access

Why This Rule Was Proposed and Finalized: Providers play a critical role in the prior authorization process as they are typically the individuals who are requesting certain treatments and services in addition to providing all background information to have these items approved by payers. Furthermore, they should have access to the same information patients do in their applications in order to provide comprehensive care, based on all pertinent information.

Copyright 2024

Provider Access Requirements

1. Payers must make available in the Provider Access API:
   a. Claims and encounter data
   b. All data classes and data elements included in a content standard adopted at 45 CFR 170.213 (USCDI v1) such as Immunizations, Procedures, and Assessment and Plan of Treatment
   c. All information, and only the information, the payer "maintains"
   d. Prior authorization information for 1 year prior
   e. There is not a provider remittance information requirement
2. Payers must make available educational materials for patients
   a. Provide the benefits of a Provider Access API
   b. Provide information on their opt out rights
   c. Provide instructions for opting out and opting in after opting out
   d. Provide information in non technical, easy to understand
   e. Provide information publicly, available at all times on website
3. Payers must make available educational materials for Providers
   a. Provide resources about Provider Access API
   b. Provide information on process for requesting patient data from payer using API
   c. Provide how to use attribution process to associate patients with the provider
   d. Provide information through payer website and other modes of communication

Copyright 2024

A Few Differences Between the Patient and Provider Access API:

- Patient requests through health application, provider requests through EHR practice management system or other technology solution for treatment purposes (eg HIE could function here)
- No provider remittances shared on Provider Access API
- No enrollee cost sharing shared on Provider Access API
- If a provider does not have a provider agreement or is not enrolled with a payer that holds their patient's data, the payer would not be required to provide patient data to this provider under this proposed rule
- HIPAA Interpretation- would this exchange be considered a healthcare transaction?
- Although the proposals would facilitate sharing claims data from payers to providers, the transmission would not be subject to HIPAA transaction standards because the purpose of the exchange would not be to request or issue a payment

Copyright 2024

Electronic Prior Authorization Measure for MIPS Eligible Clinicians and Eligible Hospitals and Critical Access Hospitals (CAHs)

Requirements: This will be an attestation measure, for which the MIPS eligible clinician, eligible hospital, or CAH reports a yes/no response or claims an applicable exclusion, rather than the proposed numerator/denominator.

If attesting "yes," they would be attesting yes to:

- Requesting a prior authorization electronically via a Prior Authorization API using data from certified electronic health record technology (CEHRT) for at least one medical item or service (excluding drugs) ordered during the CY 2027 performance period or (if applicable) report an exclusion.
- Requesting a prior authorization request electronically via a Prior Authorization API using data from CEHRT for at least one hospital discharge and medical item or service (excluding drugs) ordered during the 2027 EHR reporting period or (if applicable) report an exclusion.

Copyright 2024

Payer to Payer Exchange

What the New Rule Requires: This portion of the final rule requires existing payers to send a patient's information to a new payer for a certain number of years (likely five as CMS does not require information prior to five years to be shared) after they leave the plan via FHIR. It places the same requirement to provide to individuals with concurrent coverage.

Copyright 2024

Payer to Payer Exchange

Why This Rule Was Proposed and Finalized: This is meant to create a longitudinal record that follows the patient as they go from payer to payer. This is to increase coordination and prevent any delays or unintentional consequences when an individual switches plans.

Copyright 2024

Payer to Payer Requirements

- Payers must make available the same data classes as the Patient Access API
  - USCDI version 1
  - Adjudicated claims and encounter data (not including provider remittances and enrollee cost-sharing information)
  - Prior authorization decisions
    - While patient will be required to resubmit prior authorizations under a new payer, this will help will efficiency
  - Only required to share information within five (5) years of the date of the request
- Payers must use OpenID Connect authorization and authentication protocols to authenticate identity of payer requesting access
- Payers must use FHIR Bulk Data Access (Flat FHIR) used for exchanging multiple patients' data at one time

Copyright 2024

Payer to Payer Requirements

- Payers must allow patients to opt INTO payer to payer exchange (with previous and current payers) prior to start of coverage
  - Cannot be used as reason to delay an applicant's eligibility for start of coverage
  - Only can request enough information to identify and make successful request of previous or concurrent payers
  - Opt in is to identify the appropriate payers using the patient as the source of truth, it is not an opt in to share health information that is able to be shared without patient authorization
- Must require the requesting payer to include an attestation with the request for the data affirming the patient has enrolled with the payer and opted in to payer to payer exchange
- Information with Payer to Payer must be incorporated into the patient's record with the new payer

Copyright 2024

Payer to Payer Requirements

- For concurrent coverage, exchange patient's data available to each other every quarter at a minimum
- Payers must make patient education information available
  - Information must be non technical and simple
  - Must provide information on patients' ability to opt in or withdraw opt in and instructions
  - Education must be provided before requesting permission for payer to payer
  - Payers must only provide to those currently enrolled in plan- but available publicly on website (seems contradictory)
  - Information must be provided annually
- Payer to payer exchange is a one time share, not an ongoing share

Copyright 2024

Payer to Payer Requirements

- Patients can request subsequent data if they choose for other situations
- New payers must make request no later than 1 week after the start of the coverage
- There is a one (1) business day turnaround time if an impacted payer receives a request from another payer to make data available for former patients who have enrolled with the new payer or a current patient who has concurrent coverage
- This is if they have been authenticated and demonstrated opt in

Copyright 2024

TEFCA Updates

Copyright 2024

TEFCA Updates

- **Updates to Common Agreement 2.0 and Standard Operating Procedures:**
  - FHIR Exchange and Roadmap
  - Healthcare Operations
  - Public Health
  - Principal and Delegate designation
  - Terms of Participation
  - Connection to multiple QHINS

Copyright 2024

THANK YOU

LET'S CONNECT

mihin.org

@MiHIN

linkedin.com/company/mihin

Copyright 2024