Massachusetts
Health Data
Consortium

July 2022 Newsletter

When you are a mission-based, not-for-profit organization, as is MHDC, you can be forgiven for being passionate, altruistic, and optimistic about your ability to effect change, especially in an economy as vast and fragmented as health services. Making incremental progress in advancing health justice, accessibility, and value is what motivates organizations like ours to do the work we do.

We are motivated also by a vision of a person-centered health data economy where the “center of gravity” of an individual’s health information is the individual and not the enterprise. We know that without engaging the individual, the health system cannot understand each person’s health, social, and accessibility needs.

Mission and vision only go so far, however. Over just the last few weeks, we have seen dramatic, if not stunning, changes that defy a person’s ability to manage their health and their health data. The Supreme Court denied women the federal right to abortion (Dobbs vs. Jackson) and allowed employers to force employees with advanced kidney disease onto Medicare rather than pay dialysis providers (Marietta vs. DaVita). They also made several rulings around HHS payments (Becerra v. Empire Health Foundation, American Hospital Association vs Becerra) and also decided that state Medicaid agencies can seek reimbursement of funds from settlements made to patients for care costs (Gallardo vs Marstiller); all of these could affect cost and access to care for patients. Still pending at the time of this writing is a decision on whether physicians can be convicted of unlawful distribution even if they thought they were prescribing medication within their scope of practice (Ruan vs United States) which could affect patient ability to get appropriate medication. In addition to these monumental court cases, many other recent events affect patient care and data. Most notably, a significant proportion of the country’s leading health systems were caught sending patients’ health data to Facebook (we'll discuss this further in our feature article below).

In Massachusetts, we are fortunate to have a state known for its healthcare and its support for patient rights. We can be the “force for good” that health care needs to stay the course and keep patients center of mind and in control of their health data.

Denny Brennan, Executive Director

Follow Us

Be sure to follow us on Twitter and LinkedIn for live tweeting during industry webinars, insights on relevant news, and our take on interoperability, data, health equity, telehealth, APIs, and other topics of interest!

Upcoming MHDC Events & Webinars

July 6, 13, 20, 27, 11am-12:30pm
DGC Working Group (members only)

July 7, 9-10am
NEHEN Business Users Group (members only)

July 14, 8-10am
Board of Directors Meeting (members only)

July 14, 11am
What it Looks Like to be Done with Healthcare Transparency
Matt Parker and Keith LoMurray - HealthSparq
(free - open to the public)

July 26, 2-3pm
Spotlight User Group

July 28, 10am
Discernment in a Digital Health Gold Rush
Jessica Zeaske, PhD - Echo Health Ventures
(free - open to the public)

July 29, 8:30-10am
DGC Steering Committee (members only)

Missed any of our webinars in 2022? Click **HERE** to see what you've missed!

Interested in sponsoring a MHDC webinar or have an interesting topic you'd like to suggest? Contact us at webinars@mahealthdata.org

DGC Update

The Data Governance Collaborative (DGC) at MHDC is a collection of payers and providers throughout the region exploring ways to better exchange health-related data incorporating industry standards and automation as much as possible.

We recently held a deep dive on allergies, looking at the sometimes nebulous distinctions between allergies and intolerances (and, to a lesser degree, adverse events) and how much they matter as well as allergies in FHIR, USCDI, and US Core. We also explored some of the data currently collected, some of the current pain points of the reaction reporting process, and potential future interoperability routes we'd like to see. Watch this space for news of future deep dives.

Regulations and industry events are still a priority in our working group meetings. We have been reviewing the WEDI Spring Conference and will be reviewing last month's FHIR DevDays in the near future. We've also been exploring several special projects with our Steering Committee and lending our expertise to some external projects run by others - watch this space for more information as these projects progress.

Participation in the DGC is open to any payer or provider with business in Massachusetts - big or small, general or specialist, traditional or alternative. Want to know more? Email datagovernance@mahealthdata.org

Spotlight Analytics Update

Spotlight Business Analytics helps healthcare organizations run custom analytics on health data including market share, patient origin, disease prevalence, cost of care, and comparative costs and outcomes for acute care hospitals.

We are partnering with the Lown Institute to add civic and care leadership measures to Spotlight. Augmenting Spotlight's market share, disease prevalence, and demographic analyses with the Institute's equity, value, and outcomes measures will provide Spotlight subscribers with a more comprehensive, robust, and relevant view of health system performance.

Please join us at our next Spotlight User Group Meeting for updates and news about the progress of the Lown data as well as the current case-mix data. It is scheduled for Tues July 26 at 2pm and is open to the public. Click here to register (even if you're a regular attendee).

The current data status is:

Coming Soon:

- Massachusetts Hospital Inpatient Discharge Data FY21
- Massachusetts Emergency Department Visit Data FY21
- Massachusetts Observation Data FY21
- Rhode Island Hospital Inpatient Discharge Data FY21

Received & ready for use soon:

- Lown Institute measures

Future planned data:

- New Hampshire Facility Discharge Data Sets (Application pending)
- Maine Hospital Inpatient and Outpatient Data (Application pending)

Please feel free to visit our Spotlight Business Analytics page or email us with any questions or comments at spotlight@mahealthdata.org.

NEHEN Update

NEHEN reduces administrative burden through the adoption of standardized transactions. It is a cornerstone service for payer and provider trading partners wishing to exchange industry standard X12, HIPAA compliant transactions in a real-time, integrated manner using APIs. Because of our unique governance, non-profit status, and membership-based model, NEHEN is able to offer very competitive services relative to the market. Working with members and trading partners, NEHEN is also supporting a prototype electronic prior authorization (ePA) implementation that automates transactions using industry standard, open platform methods developed by the HL7 DaVinci Prior Authorization workgroup.

NEHEN has been closely tracking regulatory activity around transactions and data exchange and participating in related industry activity. Since the March 10th HITAC prior authorization recommendations to ONC, there have been multiple letters, listening sessions, and recommendations from industry groups interested in this and related areas (including but not limited to CAQH Core, WEDI, ONC, CMS, HL7, X12, and NCVHS). Of note, NCVHS (the National Committee on Vital and Health Statistics) conducted a day long listening session on June 9th on the role of information standardization in burden reduction focused on the convergence of clinical and administrative data and the increased collaboration efforts among federal agencies, particularly those within HHS.

In general, the level of engagement and consideration of industry in the development and advancement of standards and related regulations is at a high point. We anticipate this continuing in the near future and expect further impactful regulation soon from CMS and others. We are attending the HL7 CMS FHIR Connectathon in July and hope to learn more there.

All of this activity impacts both NEHEN and the work we are doing on electronic prior authorizations as the evolving standards include both EDI and API transactions for both administrative and clinical data and data exchange even as we and the rest of the industry remain bound by HIPAA and its required code sets. We remain hopeful that changes to HIPAA requirements for better alignment with newer standards is forthcoming.

For more information about NEHEN or ePA please contact us at nehen@mahealthdata.org.

Do You Know Where Your Health Data is Going? You Should

One of the biggest criticisms of the CMS mandated Patient Access APIs we heard was that it moves protected health data outside of the purview of HIPAA and thus patient privacy could be freely violated. Many want HIPAA or HIPAA-like protections extended to third parties handling health data. That argument might hold more weight if HIPAA was actually protecting the health information of patients at organizations who are bound by its rules. Sadly, that's not always the case.

In the past few weeks investigative reporters published three articles showing just how badly some of our healthcare organizations are violating patient privacy. These articles addressed data tracking and collection software placed on provider websites allowing online patient appointment scheduling, placed in patient portals, and placed in patient check-in software used by providers. They sent data to Facebook, to Google, to Amazon, to Oracle, and elsewhere (including to at least one data broker). Some of their websites included session trackers potentially recording every click made on those pages.

Two [1] [2] of the three articles were from The Markup, a non-profit newsroom doing data-driven reporting on how technology affects society. The third - a more narrow look specifically at one patient check-in application (Phreesia) - was by the Washington Post. The Markup articles, in particular, explain their investigative process and findings in detail, backing them up with data and evidence. They are compelling and horrifying at the same time.

Both of these scenarios involve the transfer and collection of PHI. In the case of Facebook, this is done without consent and entirely outside of the HIPAA framework. In the case of Phreesia (which typically signs Business Associate Agreements with its users to access the data), selling the data is ostensibly done with patient consent and under the guise of offering more personalized service to the patient. However, the consent is buried deep within a longer consent form that's part of the check-in process and, unless you are used to reading and absorbing every word of lengthy consent forms, likely to be dismissed as consenting to the visit.

The Markup research is particularly interesting. They looked at Newsweek's 100 Top Hospitals and found that 33 of them use Meta Pixel, tracking software that sends Facebook data whenever buttons are clicked where it's installed. Even if a user isn't logged in or hasn't provided their identity yet, the packet includes IP addresses which often are static and can be used to identify a patient or household.

The Markup contacted each of the 33 hospitals with the tracker and gave them the chance both to respond and to remove the tracker. These include many of the most well known and prestigious hospitals across the country including some here in Massachusetts. Only a few of the hospitals they contacted removed the software and even fewer responded to the request for comment (mostly with generic statements about taking patient privacy seriously).

When installed on pages used for online scheduling, the information shared typically included the text of the button clicked, the search term supplied or condition selected to generate the list of available appointments, and the name of the doctor selected for treatment. This is bad enough, but it is mainly inferred information rather than direct patient information (searching for a doctor to see about Alzheimer's doesn't necessarily mean the patient has Alzheimer's - but they almost certainly have some related symptoms). However, if follow up appointments are also made using this mechanism rather than just initial appointments attached to clinician discovery, the inference becomes a lot stronger. Knowledge of frequency of appointments can also be extremely useful in terms of knowing when a particular condition is bothering a patient, how severe their case is, or similar.

However, in addition to scheduling pages, 7 of the hospitals they examined also used Meta Pixel in their online patient portal. This was discovered using patient volunteers who consented to have information about Meta Pixel usage and the related data sent to The Markup in order to discover what's being collected. In these cases actual, direct patient health data was sent via the Meta Pixel tracker. This includes names of medications taken by patients, descriptions of the their allergic reactions, and details about upcoming scheduled appointments. 5 of the 7 removed the tracker from their patient portals after being contacted by The Markup.

The Markup bent over backwards to be fair to the hospitals in question. There are some limited circumstances where this type of data collection is legal without patient consent, but it nearly always requires explicit patient consent (see Phreesia comments above). They contacted all of the involved organizations to see if the types of contracts that would allow this type of data collection were in place. Neither Meta/Facebook nor any of the hospitals said these contracts existed. There was no evidence that consent was collected (even obscurely) from website or portal visitors, the other legal avenue to data collection. We wonder, though - even if a business agreement of some sort is in place to allow data transfer, does that absolve the companies for the need for separate consent to track user interactions with the system?

In their second article, The Markup did a deep dive of the tracking found at a large network of children's hospitals. In addition to Meta Pixel sending data to Facebook and also finding a Google analytics tracker, they found 25 ad trackers, 38 cookies, and signs of keystroke collection. A Meta spokesperson said that sending sensitive data via Meta Pixel is against policy and that health data is supposedly blocked from storage, but they did not comment on how they define health data or whether the data from this organization (or any of the others) was actually filtered out. Given that the only data being collected from either the scheduling sites or the patient portals is health information, it strains credulity to believe that none of it was retained or used.

These incidents are disturbing. While we all know people should be more vigilant about reading consent forms, that doesn't help when no consent forms exist. Further, if a patient needs care and is presented with a form to sign, most will sign it rather than walk away from an appointment. This is doubly true for people who have been waiting a long time for an appointment, have taken time off of work or arranged for childcare (or both), or who have otherwise spent time, energy, and money to make the appointment happen. Further, these forms are long, technical, written in the Legalese dialect of English, and require a lot of patience and experience for non-lawyers to understand. When presented amidst a slew of other forms, particularly other forms that seem more directly relevant to a visit such as health history or collection of current symptoms, and especially when under a time crunch to complete the annoying paperwork so you can get to the important parts of a visit, how many people are actually going to read and understand every clause and sentence of a consent?

That doesn't even get into other equity and accessibility issues. Will staff read a long and complex form to a patient who can't see it? Is someone even available to do this before a visit starts for a telehealth visit? Are consent forms available in other languages? Are non-technically savvy users able to understand the implications of what they're being asked to sign? And so on.

In the case of check-in software, the data isn't just collected to be sold (although it is). It's used to promote possibly relevant prescription drugs and similar products to patients right before they see a clinician for the conditions these products treat. Putting aside any questions about whether advertising prescription drugs should be allowed, this type of advertisement is disruptive to the care process. In this era of limited time for appointments, it invites patients to waste time by asking their clinicians about those products they were just told might help them. Furthermore, since that happened within the framework of their appointment, a patient might be forgiven for thinking that their medical providers approved of the advertisement and therefore were just reminding them to ask about something that has already been deemed appropriate for their care. Perhaps every so often the advertised product is a good fit for the patient, but that won't always be the case and it will be harder to convince the patient that they shouldn't get that product when they were just told - under the imprimatur of the hospital - that they should.

Even more disturbing is sending health-related data to Facebook without consent. This data gets used for everything - every part of a person's life in 21st Century America is affected by the way Facebook interconnects data. This is bad enough when permission is given or when a patient has some reasonable expectation that Facebook could see the data, but it is unconscionable when they have every reason to think the data is hidden from prying eyes. Knowing what types of medical appointments a patient is trying to make allows Facebook to infer a lot about the type of ads to show that patient or other places that might be interested in buying their data. Knowing the doctors the patient chooses to see could allow Facebook to infer information about the types of people the patient trusts, especially if there are demographic similarities between their various clinicians. Knowing the search terms they use allows Facebook to understand and analyze their specific word patterns and both identify them in other contexts and frame language it presents in an inherently more comfortable flow for that specific person (we don't know if this type of analysis is happening but it could).

The most disturbing case of all is the intrusion of these trackers into patient portals. One could argue that online appointment scheduling is happening in the open and thus a savvy person should assume it might be monitored (we reject this argument but it is something that some believe), but there is no one who could legitimately argue that information inside password protected software deliberately designed to hold PHI is appropriate to share with Facebook under these circumstances. In general, the data collected by appointment scheduling leads to inferences (sometimes strong inferences) but data from a patient portal is explicit, factual data about that patient. It is much more valuable and patients have a reasonable expectation that it's well protected. They have been told repeatedly that it's well protected. They have been told repeatedly that it's illegal for it not to be well protected. And yet, here we are.

Will an article in the Washington Post - as highly regarded and widely read as that outlet is - force check-in software to change its behavior? Even if it does, how many more companies with peripheral interactions with the healthcare system are doing similar things? We doubt it will land at all with Facebook or Meta, but will a fantastic, well researched, and well backed up report in the less widely read The Markup change the behavior of hospital systems across the country? Even if these particular trackers sharing data about these particular interactions are removed, who's to say there aren't others in place?

Consent forms are long and difficult to understand and problematic and need to be improved, but how do we deal with data sharing outside of consent? We've all heard and rely on security by obscurity, but this is lack of privacy by audacity. We shouldn't have to seek out and monitor every single interaction in every single system in every single provider or payer or other healthcare organization in the country to be confident that our health data isn't being shared without our consent. We shouldn't have to rely on volunteers who allow investigative journalists access to their private health information to prove privacy violations once we suspect they're happening. Limiting advertising of prescription drugs and prescription-only medical devices would help as they take away a major market for the data, but there are always venues that would find health data useful. We can always publicly shame companies, but that only goes so far if they're willing to be audacious - and memories fade. What else can we do? We'd love to hear your thoughts.

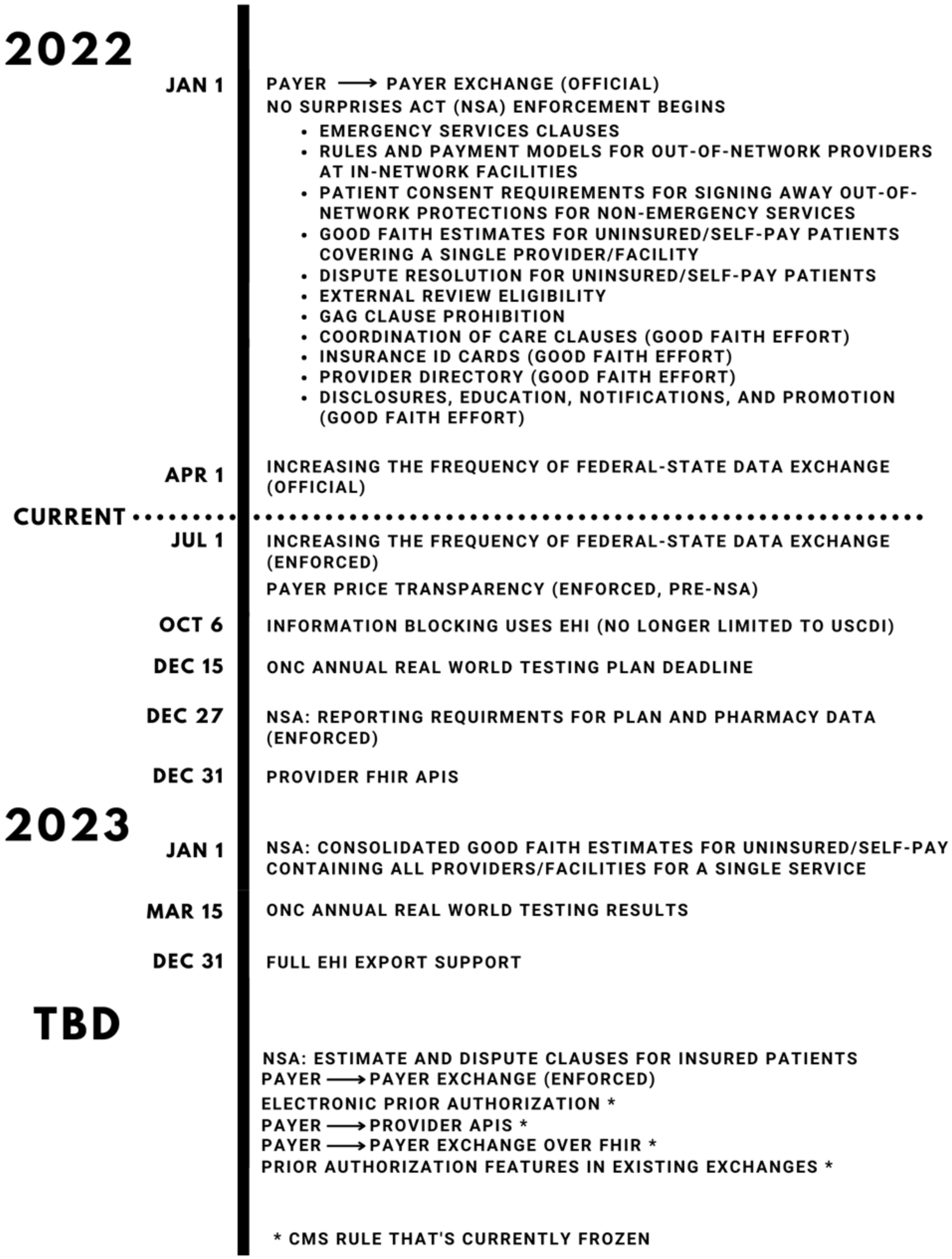
Industry Events

Webinars and online conferences we recommend (they're free unless otherwise noted):

- HIMSS: Is Your Health Data Stewardship Enhancing or Degrading Your Patient Experience and Trust?: Jul 11, 2pm
- WEDI: Virtual Spotlight on Value Based Care: Jul 12, 11am
- Beckers: Seeing the whole picture for whole-person health: Jul 12, 2pm
- Beckers: Consumerism is Calling: How Health Systems Can Provide the Digital Experience Patients Want: Jul 13, 1pm
- AHIP: Data-Driven Personalization: 3 Approaches to Accelerate Your Member Strategy: Jul 13, 1pm
- HL7: CMS FHIR Connectathon: Jul 19-21 (Today's the last day to register!)
- Beckers: How adding AI to your digital strategy can successfully strengthen your cardiology department: Jul 19, 12pm
- Beckers: Using technology to wrap digital arms around patients: Jul 20, 1pm
- EHI: Collecting Sensitive Data While Protecting Vulnerable Populations: Jul 27, 1pm
- AHIP: Get Back to Basics: CX Lessons from Members & Health Plans: Jul 28, 2pm
- Fierce: Dramatically Improve Care Management Using Embedded AI with Automated Rules Engines: Jul 28, 2pm

Regulatory Deadlines

Don't forget these health data exchange deadlines, including from ONC and CMS:



2022

JAN 1 PAYER ⟶ PAYER EXCHANGE (OFFICIAL)

NO SURPRISES ACT (NSA) ENFORCEMENT BEGINS

- EMERGENCY SERVICES CLAUSES
- RULES AND PAYMENT MODELS FOR OUT-OF-NETWORK PROVIDERS AT IN-NETWORK FACILITIES
- PATIENT CONSENT REQUIREMENTS FOR SIGNING AWAY OUT-OF-NETWORK PROTECTIONS FOR NON-EMERGENCY SERVICES
- GOOD FAITH ESTIMATES FOR UNINSURED/SELF-PAY PATIENTS COVERING A SINGLE PROVIDER/FACILITY
- DISPUTE RESOLUTION FOR UNINSURED/SELF-PAY PATIENTS
- EXTERNAL REVIEW ELIGIBILITY
- GAG CLAUSE PROHIBITION
- COORDINATION OF CARE CLAUSES (GOOD FAITH EFFORT)
- INSURANCE ID CARDS (GOOD FAITH EFFORT)
- PROVIDER DIRECTORY (GOOD FAITH EFFORT)
- DISCLOSURES, EDUCATION, NOTIFICATIONS, AND PROMOTION (GOOD FAITH EFFORT)

APR 1 INCREASING THE FREQUENCY OF FEDERAL-STATE DATA EXCHANGE (OFFICIAL)

CURRENT ••

JUL 1 INCREASING THE FREQUENCY OF FEDERAL-STATE DATA EXCHANGE (ENFORCED)

PAYER PRICE TRANSPARENCY (ENFORCED, PRE-NSA)

OCT 6 INFORMATION BLOCKING USES EHI (NO LONGER LIMITED TO USCDI)

DEC 15 ONC ANNUAL REAL WORLD TESTING PLAN DEADLINE

DEC 27 NSA: REPORTING REQUIRMENTS FOR PLAN AND PHARMACY DATA (ENFORCED)

DEC 31 PROVIDER FHIR APIS

2023

JAN 1 NSA: CONSOLIDATED GOOD FAITH ESTIMATES FOR UNINSURED/SELF-PAY CONTAINING ALL PROVIDERS/FACILITIES FOR A SINGLE SERVICE

MAR 15 ONC ANNUAL REAL WORLD TESTING RESULTS

DEC 31 FULL EHI EXPORT SUPPORT

TBD

NSA: ESTIMATE AND DISPUTE CLAUSES FOR INSURED PATIENTS
PAYER ⟶ PAYER EXCHANGE (ENFORCED)
ELECTRONIC PRIOR AUTHORIZATION *
PAYER ⟶ PROVIDER APIS *
PAYER ⟶ PAYER EXCHANGE OVER FHIR *
PRIOR AUTHORIZATION FEATURES IN EXISTING EXCHANGES *

* CMS RULE THAT'S CURRENTLY FROZEN

And that's it, folks. Loved it? Hated it? Have an idea for next time?

Send us feedback and suggestions at info@mahealthdata.org.

Confidentiality Notice: This email, including attachments, is for the sole use of the individual to whom it is addressed, and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you have received this email in error, please notify the sender by reply e-mail and destroy this message and its attachments.