b.well

June 16, 2025

Submitted via Regulations.gov

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-0042-NC
Mail Stop C4-26-05
7500 Security Boulevard
Baltimore, MD 21244-1850

Re: RFI | Health Technology Ecosystem

Dear CMS Team:

b.well Connected Health is on a mission to simplify healthcare for every American. We believe every person should have access to their health data—wherever they go, and wherever they are in their health journey. We believe every person deserves to be supported in their health journey - to make more informed choices, and to easily access information and services without added burden and toil. We share the Administration's observation that our health system indexes too much on "sick care", and that transparency supports more informed decision-making. Because of this mission and our shared alignment with the Administration's vision, we are honored to contribute to its efforts to create a generational opportunity for modernizing the health technology ecosystem, and finish the work of promoting innovation on open standards and pro-competitive principles.

I. About b.well and Our Longstanding Alignment With Administration Goals

For over a decade, b.well has worked across the industry—partnering with payers, health systems, global consumer health companies, and retail pharmacies—to unify fragmented data and services into seamless consumer-centric digital experiences. As active members of the CARIN Alliance and contributors to national regulatory efforts, we have worked to shape the regulatory landscape to support transparency, realize the promise of true interoperability, advance the goal of getting all beneficiaries into a risk based model by 2030, and catalyze innovation on open, pro-competitive principles.

Today, b.well powers the **largest connected, live health data network in the market—spanning 1.7 million providers, 300+ health plans, TEFCA, HIEs, national networks, and nearly every category of consumer health data.** Our Health Data Management Platform goes beyond simple data aggregation, delivering deep, bi-directional integration with both large and small EHRs through multiple technical methods and formats. Combined with connections to wearables, claims, and digital tools, this infrastructure fuels our real-time intelligence engine to deliver personalized, actionable experiences—enabling consumers to schedule care, access records, and take meaningful steps in their health journey.

Our response reflects not just our technology, but our track record. Our hands-on experience gives us unmatched insight into both the opportunities and challenges of operationalizing interoperability at scale. With deep regulatory expertise, a FHIR-based platform, and a national footprint, b.well is uniquely positioned to inform and accelerate the CMS Health Technology Ecosystem vision. We are not here to debate interoperability or FHIR—we're here to help offer suggestions for finishing the job, and then keep going with real-time price transparency, SMART insurance cards and even more ways to help consumers streamline their interactions with the health system.

II. Early Results of Progress

In 10 years, we've already accomplished a lot in regards to digital experiences focused on health, which offers a peek into how the Administration's transformational goals can be realized when the needs of patients and caregivers are at the center, and when data moves freely to support the apps and solutions that health care stakeholders want to build. Building solutions that support whole patient populations is critical if they are going to participate in the shift to value, including the Administration's determination to shift all Medicare beneficiaries into value-based arrangements by 2030.

Here is what's working:

- We have developed and launched digital consumer experiences that enable seamless health data interoperability and direct access to care and personalized health-related insights and recommendations across various healthcare settings. Our solutions focus on connecting patient data and care delivery pathways, ensuring that critical health information is accessible and actionable at the point of care.
- We have successfully established connections across all pathways that support nationwide interoperability, including the largest network of patient access API endpoints. This enables scalable patient-mediated health data access and exchange. We operate on national networks for provider treatment use cases and IAS. We are the only vendor currently live on TEFCA for IAS (with Epic and Athena, with more coming) via Commonwell, and we have direct gateways to HIEs. Additionally, we have secured proprietary access to data that is not yet widely shared under current information blocking regulations. We are also early adopters of Medicare BlueButton and the VA Lighthouse, and we currently connect with more than 300 payers and over 1.7 providers, leveraging the patient right of access.
- Through these endpoints, and through trusted exchange, it's now possible for 10s of millions of patients to manage a personal health record from the largest network of places where they receive care via the b.well FHIR platform.
- As an early adopter of the CARIN Alliance Code of Conduct, b.well also is the only developer to be an independently accredited adopter. The list of apps on myHealthApplication.com that have adopted the CARIN Code of Conduct illustrates that the app developer community chooses consumer-consented health data access, use and exchange on principles of privacy, transparency and choice. It demonstrates that app developers can be trusted partners in the health data exchange ecosystem.
- Our connected health platform enables customers to share proactive communications

with their end-users on prevention and condition management at a personalized level. We use evidence-based preventive medicine guidelines, data science-driven personalization and end-users' communication preferences (text vs. in-app notification vs. email) to surface and close care gaps and drive actions, which are far superior to industry benchmarks. We are also the early adopter of NCQA's digital content service where we are running NCQA certified CMS Quality measures on top of our FHIR server with proactive content going direct to the consumer.

- We launched digital identity proofing over three years ago in our customers' connected health experiences. We are the first Individual Access Service Provider to demonstrate federated digital identity on TEFCA, first with Epic and then with Athena, through our CLEAR integration and QHIN partner Commonwell Alliance. Our experience shows that patients can securely authenticate themselves to access their health information, with less friction than remembering their patient portal login.
- We incorporate a consent management framework into our platform. It supports privacy rights, like the right to be forgotten. It also empowers patients and families to make informed medical decisions as a household and for loved ones. Our consent management frameworks allow consumers to opt in to using their data for any purpose they choose - having agency in how their data is used.

All these efforts lay the foundation for a complete vision for empowered patients and families - allowing us to shape the future of health care so that it becomes patient-centered.

We have demonstrated how technology, innovation-minded partners and interoperability mandates work together for the good of patients and caregivers, leveraging personal health data to anticipate health needs, share timely and relevant insights and recommendations, and encourage more towards health and prevention, instead of just reacting with "sick care". We've only begun, and we've already made substantial progress; but there is still much more we can do.

III. A Call To Action

If we are faithful to the Cures Act interoperability mandates, we should be thinking expansively to finish the work on full, complete data access, exchange and sharing for essential purposes – especially patient access, treatment, care coordination, and population health – by reinforcing expectations of bi-directional data sharing on open standards that minimize special effort and don't involve added costs or use restrictions, and down involve trade-offs with system performance. We need to finish this work, largely by enforcing the rules that already exist. At the same time, we should declare success with meaningful use of certified EHR technologies. We need to move certification off of the EHR workflows and onto the inputs and outputs to core systems of record for all stakeholders that play a role in health outcomes, and specify appropriate data access APIs, with a goal of making these edge cases secure and frictionless. In this way, we can build the interconnected and interactive foundation for a modern health tech ecosystem.

IV. If The Administration Does Nothing Else, Do These Four Things

A. Enforce the Principle of Data Extraction from EHRs via Bulk (Backend) FHIR APIs

Our HIPAA-covered customers manage large patient populations (in the magnitude of 100,000s). It's critical for them to access, use and exchange data from their EHR systems easily and without special effort, added cost, degraded performance or use restrictions. In order to effectively manage the health of any population, and to leverage advanced technologies like large language models (LLMs), they must be able to access data from all core systems of record.

Bulk (or "backend") data access APIs based on open standards, transparency and pro-competitive principles are intended to accommodate requests on whole populations. Unfortunately, right now these APIs have become a limiting factor. In some cases, our customers can only retrieve data from their own EHR in increments of 1,000 patient records. This may be due to the legacy nature of how EHR systems were built. Minimally, these APIs should be expected to be fully conformant to standard, and capable of scaling to whole populations, with real time data. But if the standard needs to be enhanced, we believe EHR vendors should be held to standards for meeting these performance expectations, consistent with these open, transparent and pro-competitive principles.

Instead, many of our customers are steered into proprietary APIs that perform better, but which cost more and have use restrictions attached. Sometimes, these use restrictions remove independent decision-making from EHR customers, when the data they want to extract is from their own EHRs (with limited carve-outs for home-grown solutions). Stated differently, EHR customers are sometimes prevented by their EHR vendors from allowing any of their other tech vendors from establishing direct connections with these proprietary APIs. Or, these customers are steered towards other products of their EHR vendors via price-tying and product-tying strategies.

As a result, many of our HIPAA customers face challenges in accessing the data and point-of-care information they need for entire populations without incurring additional effort, costs, or losing the autonomy to make technology decisions that align with their transformation goals. Their progress is often tied to the timelines set by their EHR vendors, which can hinder their ability to innovate and compete effectively in the marketplace. These restrictions could also make it difficult for EHR customers to be ready to manage all Medicare beneficiaries in risk-bearing arrangements by 2030.

Interoperability mandates establish open standards as a baseline, but they should also foster a "race to the top" in innovation. Interpretive guidance when the Information Blocking Rule was finalized in 2020 states that when customers or users are dependent on an actor's technology or services, "any practice by an actor that could impede the use of the interoperability elements - or that could unnecessarily increase the cost or other burden of using the elements - would almost always implicate the information blocking provision." In other words, it doesn't matter whether the existing specification for (g)(10) APIs is faulty or not, Developers of Certified HIT Modules must support interoperability.

Recommendation. For this reason, CMS in conjunction with the ASTP/ONC and HHS (including the OIG) should use existing authorities to investigate whether practices we've described

implicate information blocking, and take appropriate regulatory or enforcement action to ensure EHR vendors have unrestricted ability to extract data from their own systems without special effort, additional fees or burdensome use restrictions that prevent them from building capabilities outside of competing products or services offered by their EHR vendor.

B. Enforce Data Sharing by Health Care Providers and HIEs

The Cures Act sets an expectation for data sharing. Unfortunately, due to lack of enforcement and regulatory guidance, many information blocking actors are not supporting interoperability through standard patient access APIs data.

Recommendations: That's why we recommend an enforcement priority reset, aimed at vigorous enforcement of information blocking mandates towards health care providers, not just for providers that must be offered certified (g)(10) APIs by their EHR vendors. The objective is to set a similar "race to the top" for nationwide coverage of clinical data through patient access APIs, so patients can actually locate and connect all their data through their choice of application. We also recommend expansion of the promoting interoperability certification program so that it specifies data access APIs for all health care providers, starting with labs and pharmacies. To complement these updates, CMS' four-year policy roadmap should include updates to its Conditions of Participation, effectively mandating adoption and use of certified APIs offered to them by Developers of Certified Health IT Modules.

Why It Matters: For the Administration to achieve its transformation goals - centered around whole person, proactive health care, instead of sick care - we need every health care provider to participate in interoperability mandates. That means enforcing the laws we have now, while expanding the coverage of the certification program and corresponding payment adjustments.

Discussion: To illustrate why these recommendations are needed, we offer labs as the first example. The largest nationwide clinical laboratories only support a small handful of hand-picked consumer-facing applications, while claiming the "infeasibility exception" under the Information Blocking Rule for why they won't enable access for similarly situated applications serving similar organizations and consumer populations. While some of their laboratory data may be accessible through patient access APIs of ordering physicians, the only lab data released is for labs ordered by those physicians. Meantime, through private data sharing arrangements that labs have with different EHRs, these same practitioners see all of a patient's lab information inside the EHR. Patients can't be empowered with only a fraction of their lab data.

The second example is with pharmacies. Because pharmacies are not named in information blocking enforcement priorities, patients cannot connect to pull in their filled prescription data. For patients and caregivers, this is a critical gap with risks to patient health and safety. It's hard to know what medications a patient is really taking, to understand treatment adherence, address coverage gaps, or perform an accurate medication reconciliation. But even though pharmacies are subject to info blocking mandates, they claim it is infeasible to support patient access.

As with labs, private data sharing arrangements between pharmacies and EHR vendors might give a practitioner a more complete medication history, or even a more complete vaccination history when vaccines are administered in pharmacy settings. But pharmacies won't allow that vaccination history to be shared with a patient through that practitioner's patient access API. This gatekeeping of critical clinical information perpetuates poor clinical decisionmaking. If an EHR can show pharmacy data to a provider, it should also be shown to the patient by whichever source has access to this vital information, and we think that access should include data from the source: the pharmacies.

Meantime, other info blocking actors are not supporting individual access. Many HIEs claim that their agreements with participants restrict them from doing so. LTPAC providers, imaging centers, and dentists aren't complying either, citing the lack of standards-based patient access APIs and their lack of participation in Medicare payment programs that incentivize participation.

All these stakeholders contribute to health outcomes, but they're not participating in interoperability. That's why CMS should also adjust its payment policies, starting with Conditions of Participation, setting an expectation that all health care providers that receive payments from government programs must support patient access.

C. Cure Portalitis: It's An Affliction We Can Eradicate

b.well was an early adopter of integrated digital ID solutions, because we aim for empowered patients. This means helping patients participate meaningfully in their health journey. But the current standards for consumer-directed health data access, leveraging patient portal credentials, comes with a lot of friction. That friction has a name, and it's called "portalitis", it's the overwhelming burden we place on patients and caregivers to:

- Manage multiple patient portal credentials
- Navigate complex multi-factor authentication workflows
- Re-authenticate to an endpoint multiple times because of expired refresh and access tokens
- Maintain access to fragmented health information
- Securing portal accounts for providers no longer seen can be difficult, as it's often needed for data access. For instance, young adults moving from pediatric to adult care can't access their data without an appointment, but can't make an appointment without a portal account.

In the three years since launching digital ID capabilities in digital front door solutions for HIPAA customers, we've given patients a way to easily access their health data from our customers' EHR systems, without concerns for compromised security. As noted above, we've also demonstrated two approaches for consumer-mediated data access with federated identity proofing through trusted exchange, which inform key learnings:

1. In our experience, the single biggest drop off point for users wanting access to their full medical record is the portal credential step in the process. In some cases, that drop off rate approaches 75% of users, after they've located the data source they want to

connect.

2. Federated identity must be supported end-to-end for trusted exchange. Hybrid approaches that force patients to enter patient portal credentials does not increase security, especially when Individual Access Service Providers are held to the same standards as others through their acceptance of HIPAA security rule, HIPAA breach notification rule and most HIPAA privacy rule protections.
3. End-to-end support for federated identity allows for more complete medical record payloads to be shared, eliminating friction points. It also allows app developers to leverage large language models to rapidly convert and standardize information and make it available to patients.
4. However, for patient access APIs to support patients, other friction points need to be addressed and eradicated too. Short-lived refresh tokens, tokens that break, consumer education that introduces hesitancy or scare tactics in patient-directed access, and redirects into the patient portal login workflow are friction points that all contribute to drop off by patients who are interested in accessing their own records.

With these learnings, we need to scale adoption and use of digital ID through trusted data exchange. In addition, we need an OIDC credential leveraging an IAL2 token to be incorporated into the standards for the patient access APIs of health care providers and plans as mandated under the information blocking and interoperability rules.

D. Move Certification Off EHRs, and Onto APIs

Data Access Should Be Table Stakes. To Drive Change, Let's Talk About Access To Care

The interoperability mandates are rightfully centered on data access, but we now need to focus on expanding API mandates for use cases at the boundary edge to EHR systems. In other words, adding new conditions of certification that promote the adoption of APIs that support bi-directional exchange between EHRs and other applications to support real-time scheduling, in-basket messaging for prescription refills, requests to correct medical record errors, real-time price transparency tools, filling out forms and completing verification of eligibility and coverage. We also need APIs that support CDS hooks, subscriptions and "since" parameters (so app developers have the option of only pulling down new information from a specified date and after).

Some of the larger EHRs are already equipped to provide these APIs and functional capabilities. However, due to their proprietary nature, third party app developers are not allowed to access them, and in many situations, even the EHR customer is prevented from authorizing access for use by their non-EHR vendor partners. Or, they may be priced in a manner that prevents their affordability for use.

These practices prevent the broader health tech ecosystem from innovating with solutions that most populations need - to streamline their efforts as they navigate the health system, when they have a care need. These are reasons why we ask the Administration to move Meaningful Use certification requirements off the EHR workflows and on to the APIs that surround the EHR, opening up guaranteed innovation advancement if the mandate comes with the following

stipulations:

1) That all core APIs surrounding data access (individual and Bulk) and service access APIs that cover all actions performed at the point of care (ex: scheduling, messaging, RX Refill, etc.) are mandated with penalties and are required to be published transparently.
2) That third parties get the same API/hardware access as the EHRs own apps.
3) The APIs must be free (covered by the EHR software license) and effective (not degraded), with no exclusive features for first-party (EHR) apps.

V. Responses to a Selected Questions from the CMS RFI

PC-1 What health management or care navigation apps would help you understand and manage your (or your loved ones) health needs, as well as the actions you should take?

The app developer community holds untapped potential to provide innovative features and digital experiences that resonate with patients and caregivers, offering crucial support for health management and care navigation. From our vantage point, working with customers across employers, payers, systems, pharmacies, and big tech, we have a front-row seat to the impressive innovation each entity is striving to deliver, which aligns with the administration's goals. However, significant blockers hinder the realization of these well-curated roadmaps. We need regulatory assistance to address these obstacles, which frustrate permitted data access and use, throttle interoperability infrastructure performance, and undermine competitive principles through price-tying or product-tying strategies. As mentioned earlier, this can be achieved by enforcing existing interoperability mandates, shifting certification from core EHR functionality to the meaningful use of APIs that provide access to EHR features, and integrating a federated digital ID trust framework to enhance system security while reducing the friction of managing multiple patient portal credentials.

At the same time, we need to: (i) finish the work of enabling real-time, consumer-consented high fidelity data computability on open standards while (ii) accelerate the adoption of standards based APIs at the edge of core systems of record, to include read- and/or write- APIs that facilitate one-way or bidirectional exchange of relevant information for:

- scheduling and completing forms
- cost transparency
- real time eligibility check
- real time benefit check
- in-basket messaging to request medical records, medical record corrections, medication refills
- sharing comprehensive immunization records, medical histories, medication histories, lists of allergies and side effects and active medication lists

By centering on these interoperability priorities, we will get even more app developers with hands on keyboards to offer innovative consumer-centered connected health experiences that drive real value, not only in terms of health outcomes but in terms of reduced administrative burden. This will create a race to the top and spur innovation!

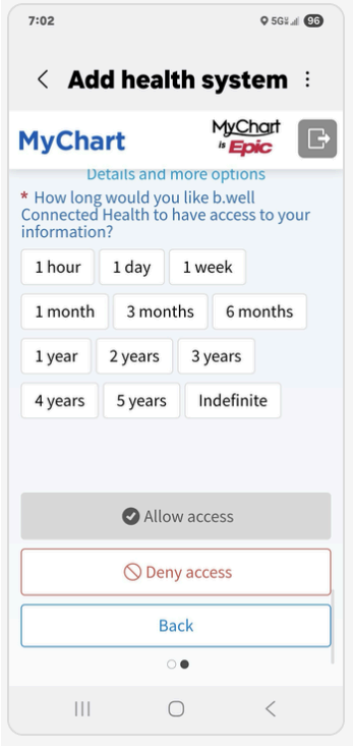
PC-2 Do you have easy access to your own and all your loved ones' health information in one location (for example, in a single patient portal or another software system)?

Because our U.S. health system is fragmented by design, very few patients have all their health data in one location. That is why it's critical for patients to be able to access and unify all their health data in one place, using an app that they like. We are encouraged by the number of healthcare incumbents and new entrants who are leveraging the new patient facing APIs as a path to provide patients access to all of their health information in one place.

However, it's important for patients to be able to access and authorize health data connections via any application of their choosing with as little friction as possible, so they don't become frustrated and abandon their efforts. However, reducing unwarranted friction involves a multi-pronged regulatory effort, illustrated below:

Practices of Certified API Developers

- **Token Practices.** refresh tokens are not supported, are short-lived, or break. Without a choice to set long-lived or even indefinite connections, consumers must actively re-authenticate and re-authorize connections, which they may decide not to do if it happens frequently enough. We note that CMS-9115F and CMS-0057F do not incorporate any token refresh minimum requirements, which is why refresh practices tend to be worse with patient access APIs of CMS-regulated payers. **Solution:** An example of a good solution is where patients are given a range of different amounts of time they want to authorize an app's connection (including 1 year, up to 5 years, and even indefinitely), as shown in the below screen. Many EHRs don't offer patients and token length options and default to expiring tokens every week or every month. This prevents app developers from providing value on top of a patient's data and instead forces them to engage users to simply "log back in."



By standardizing the interoperability rules to require long-lived refresh token, patients can set data connections based on their personal preferences;

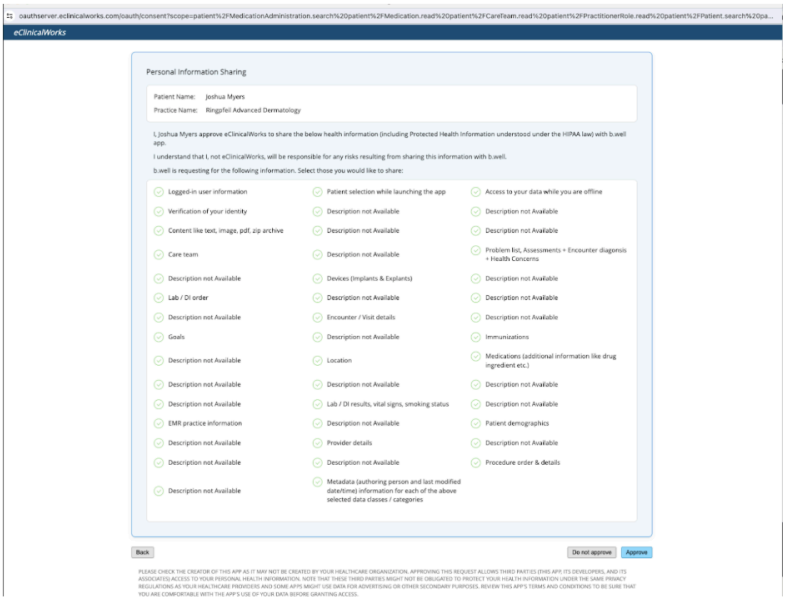
- **Consumer Education:** the OAuth workflow presents "consumer education" that misstates privacy risks and uses design colors and elements that are likely to make consumers unfairly hesitant about connecting their data through third party apps, as illustrated in the image below. We note that CMS-9115F applies a different standard on consumer education than the guidance provided by the ASTP/ONC when it first published the Information Blocking Rule in 2020 **Solution:** Regulators should harmonize its guidance on consumer education, and limit it to guidance of a general nature in neutral terms that reminds consumers about their personal responsibility to understand the privacy, security and data practices of the app they use to connect their data, and sharing resources about how to submit a complaint with the FTC or OCR if they feel that their privacy rights have been violated.

- **Poor UX design within OAuth workflows.** Some Certified API Developers have invested little design effort to support patient selection of the data they want to authorize for connections to their chosen application. Poor design elements contribute to patient burden, and may lead to higher-than-expected abandonment rates. Example: To illustrate, below is a screen shot and analysis of the screen in eCW's OAuth workflow where users select the resources they want released to the app developer. There are better practices for making this consumer friendly, as indicated in the accompanying analysis. **One Solution:** Publish regulatory guidance that the expectation of supporting data access "without special effort" extends to the consumer-facing workflows that shift unreasonable burdens on patients to authorize data connections.

eClinical Works OAuth workflow

❌ Requires each resource to be selected individually; too many actions
❌ Many resources read “Description Not Available”
❌ Per Web Content Accessibility Guidelines, v2.2, missing widely recognized best practices to improve end user experience,

- ✖ Grouping resources into classes with understandable relationships
- ✖ Use of color
- ✖ Use graphics (icons) to reinforce comprehension
- ✖ Use plain language at a 4th grade reading level
- ✖ Many clicks required



- **Federated Identity, IAL2 and Patient Matching (The Case for Functional Parity).** It’s important to acknowledge that many Certified API Developers compete in the product segment of unifying health care experiences for consumers to market. For this reason, they know as well as others that getting patients to connect their data introduces friction, and that it’s important to minimize the burden on patients. In this video, Epic federates identity across its Epic Community Members, allowing patients to **link accounts** so all their data from linked accounts can be displayed in both customer instances. Authorization is completed with low-levels of identity proofing. All the user needs to do is know the user name, email address or phone number associated with the account.

  The contrast with policy concerns for enabling individual access in trusted exchange is stark. The policy arguments center on concerns with patient matching being imperfect in legacy EMR systems, and the resulting risk of reportable breaches if the wrong records are transmitted. And yet, as the above video demonstrates, patient matching is working, with federated identity being accepted within the Epic Community ecosystem.

  b.well has successfully demonstrated use of a federated digital ID solution with two EHR

vendors, Epic and Athena to streamline patient retrieval of their health information through trusted exchange.[1] **This video** illustrates how federated digital ID coupled with device native FIDO-supported biometrics (like a facial or fingerprint scan) dramatically alleviates the patient burden on patient access. And yet, when we tested this with Epic, it only supported federated identity to locate organizations that may have records, but patients must still go to the API endpoints for each of these organizations, and login. The reason given is to manage risk of breach, and patient matching isn't good enough.

One may argue that the risk of breach is different, but b.well and other Individual Access Service Providers on TEFCA accept obligations to adhere to the HIPAA Security Rule and the HIPAA Breach Notification Rule, as well as select provisions of the HIPAA Privacy Rule. Inside a community network or out, the low risk of compromise analysis applies, and IASPs have even higher obligations to notify the FTC and others under its Health Breach Notification Rule.

One Solution: As Amy Gleason declared at the June 3, 2025 In-Person Listening Session, it is time to finish the work on interoperability. It's time to go live with individual access on trusted exchange, and get OCR to weigh in with appropriate guidance, as instructed by Congress in Section 4006 of the Cures Act.[2] It's also time to scale up federated digital identity, ensure functional parity so that consumers using untethered applications are not subject to more points of friction than the applications of Information Blocking Actors that control the "essential interoperability elements"[3].

- **Other Practices of Certified API Developers.** Another reason patients can't always connect to the providers that they want ties back to practices of certified API developers who deliberately implement processes that require their provider customers to decide whether to activate their patient access APIs, and refuse to intervene when advised that multiple end users are trying to connect to these users. Instead, we are told to cold call their customers. Not only is contact info for their customer base not provided but when we contact these provider offices their front office staff have no idea what we are talking about and direct us back to the EHR. A similar, and equally vexing, practice is when certified API developers require their customers to authorize individual app developers, in direct conflict with explicit guidance in the 2020 regulatory preamble for the Cures Act Certification Program updates.[4] **One Solution:** Use regulator guidance to strongly

[1] https://www.commonwellalliance.org/wp-content/uploads/2025/03/CW-IAS-White-Paper-3.pdf and https://www.hcinnovationgroup.com/interoperability-hie/trusted-exchange-framework-and-common-agreement-tefca/article/55275890/partners-demo-individual-access-to-health-records-via-tefca-whats-next.

[2] https://www.congress.gov/bill/114th-congress/house-bill/34#:~:text=4006)%20HHS%20must%3A%20(1,4)%20promote%20policies%20to%20facilitate

[3] 85 Fed Reg 25624 at 25810 (May 1, 2020).

[4] 85 Fed Register 25642, 25813 (May 1, 2020), accessible at https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification. ("[F]or a patient to be able to use an application of their

recommend that certified API developers "ship" patient-facing APIs with "default on", to help them shift the risk of noncompliance with the Information Blocking Rule to their customers. From a regulatory burden perspective as well, this guidance will ease the burden on overworked office staff to understand their compliance mandates.

Now, onto some real world observations:

- One EHR vendor with nearly 15,000 customers told b.well that two-thirds (2/3s) of its customers hadn't activated their patient access APIs as of late summer/early fall 2024.
- Another EHR vendor told us most of their customers with on-premises deployments hadn't activated – and likely would not activate – their patient access APIs.
- Some of our efforts to connect to individual API endpoints have lasted years, well beyond the expected turnaround time for completion of onboarding to production access stated in the 45 170.404 (10 business days to verify an app's authenticity, followed by 5 business days to complete onboarding). We are happy to provide access to our tracking system on the true burden to app developers to get these connections turned on.

These and other observations have been catalogued exhaustively by the CARIN Alliance's app developer community, and are published as resources on the CARIN Alliance webpage.[5]

Not all certified API developers follow these practices Many activate the (g)(10) APIs by default, and we think this is smart business and good for consumers. In effect, it shifts the risk of noncompliance with information blocking to their customers.

When consumers can't find their providers, they tend to see less value in connecting all their health data, and abandon a PHR feature. We must do more to help consumers easily access data from all their data sources. **One Solution:** Use the OIG's enforcement authority to investigate these and the other practices detailed by the app developer community to determine if they introduce unreasonable special effort that discourages interoperability, and work with the ASTP/ONC to issue regulatory guidance on these practices. And vigorously investigate complaints that reveal patterns of practices that introduce unreasonable special effort and implicate the information blocking rule

choice with certified API technology, the software application will need to be "registered." In that regard, [ ] an actor's refusal to register a software application that enables a patient to access their EHI [electronic health information] would effectively prevent its use given that registration is a technical prerequisite for software applications to be able to connect to certified API technology. As a result, such refusals in the context of patient access unless otherwise addressed in this rule would be highly suspect and likely to implicate information blocking.")

[5] See "Patient Access APIs in the Wild: Challenges with Scaling User Choice Without Special Effort", "Endpoint Discovery", "Registration and Onboarding", "FHIR Standard APIs with Related Support and Enablement Services" and "Patient Experience" (forthcoming)

Practices of Health Care Providers

Another reason patients cannot access all their own health information in one place involves widespread noncompliance among health care providers with the Information Blocking (data sharing) mandates.

To add color on why this is a problem, we've created a composite patient story based on things we commonly hear from our user base:

Patient Story: As a patient, I can't connect data from many of my providers' health records through my choice of application. Most of my doctors have a patient portal, but no one in their office knows how to help me when I explain I want my health data in the mobile app I like to use. I also can't find data or retrieve images from my emergency department visit when I was on vacation. This limits my ability to create and manage a complete picture of my health history, or share critical information with my regular doctor for a follow-up after my emergency illness.

One type of data I'd really like to track are my labs. A lot of my doctors draw labs in their office. I'd like my app to see all of my labs in one place, to view trends. But even though most of my doctors ship my lab samples to Quest or Labcorp, I can't just connect my lab test results from Quest and Labcorp directly into my app.

Another type of data I like to track are my prescribed vs. filled medications. This is super important for managing my diabetes. But I can't just connect to the pharmacies I commonly use. I have to piece it together through my claims. That's a pain because I get my coverage through my employer, and we keep changing health plans. Even if I have a member portal login, I can't get my claims data from them in my app.

- As indicated above, many health care providers have not activated certified (g)(10) patient access APIs even if they've been offered to them by their EHR vendor.
- But for other critical health care providers - especially labs and pharmacies - they resist efforts to authorize connections with patient access APIs, except for a small handful of handpicked mobile applications, contradicting pro-competitive principles in the Information Blocking Content and Manner Exception.
- Labs, pharmacies and other health care providers claim that their failure to support patient access is excused by the infeasibility exception under the Information Blocking Rule. In so doing, they ignore their obligations to support legitimate requests with at least two alternative manners, at least one of which must be through a manner that uses "content and transport standards specified by the requestor and published by the Federal Government" 45 CFR 171.301(b)(1)(ii)."

We offer many solutions, organized under concepts of what regulators can do "Now" under existing authorities, "Next" under annual rulemaking processes and "Later" for more comprehensive change.

Now:

- Publish interpretive guidance on what's allowable vs potential information blocking, based on observations shared with you in this comment letter and others. This helps application developers to have something to point to when encountering push back from providers or payers to break down blockers.
- Enforce the Information Blocking Rule towards Certified API Developers that throttle timely registration and onboarding with excessive manual processes for API connectors, introducing *de facto* special effort that is presumptive information blocking.

- Begin investigations of information blocking actors that claim their obligations to support patient access through standardized APIs is excused by the infeasibility exception.
- Also investigate information blocking actors that violate the principles of openness and pro-competitive principles in the Content and Manner Exception, by authorizing patient access API connections to a small handful of hand-picked consumer-facing applications rather than publishing to all.
- Publish interpretive regulatory guidance, explaining how health care providers can meet their data sharing responsibilities for patient access through APIs that conform to 45 CFR 170.315(g)(10), without having to support exchange for USCDI data classes and elements that they do not routinely maintain in their core systems of record.

Next:

- Publish regulatory guidance that failure of health care providers that are offered (g)(10) APIs but which fail to activate these APIs is presumptive information blocking.
- Update CMS Conditions of Participation to require activation of patient access API endpoints for the entire contract year
- As well, require MAOs to add requirements in the network contracts for their in-network providers to maintain active patient access APIs throughout the contract term
- Strengthen the Promoting Interoperability Performance Category, in particular the measure for Provider to Patient Exchange (PI_PEA_1) and the surrounding payment adjustments. As currently designed, they are not doing enough to incentivize covered practitioners and medical groups to activate patient access APIs. Instead, adjust the category and assign an automatic 0 score for the entire category if the reporting practitioner or medical practice fails to maintain active (g)(10) APIs throughout the reporting period.
- Broaden information blocking disincentives so they apply to all health care providers.
- Enhance the disincentives for not supporting patient access through FHIR-standard APIs.
- Publicly report the absolute number and percentage of Medicare-eligible clinicians and hospitals that have active patient access API endpoints. This can be an objective and key result tied to CMS' initiative to establish a national healthcare directory (which we also strongly endorse, to improve endpoint discovery.

Later:

- Update the Certification Program to include standard APIs for pharmacies, labs,

diagnostic imaging, and LTPAC providers

- As part of the specification for APIs for these health care providers specify the USCDI standards that are appropriate for the data these health care providers are expected to manage. We understand this recommendation is being made by the Electronic Health Record Association, and perhaps others.
- As you may have seen in the Patient Story, most consumers can't access their adjudicated claims. About 54% of the U.S. population gets their health coverage through their employment[6], but under existing laws, most can't connect their adjudicated claims because FHIR API mandates don't apply to commercial lines of business.[7] For this reason, we recommend that HHS work with Congress to expand Information Blocking and the Certification Program so they include health plans, including commercial lines of business, and put patient access APIs on the same regulatory framework.
    - One of the benefits of creating a unified regulatory framework is that it will also close an enforcement gap with CMS 9115F and CMS 0057F. CMS doesn't have a formal intake process for interoperability complaints. By moving to the Certification Program, CMS can leverage the formal Health IT Complaint Portal and other infrastructure, and add Information Blocking penalties for noncompliance.

PC-5 What can CMS and its partners do to encourage patient and caregiver interest in these digital health products?

Consumer education, done right, invites individual participation and informed decision making, free of bias or steering influences. We like the approach mandated in CMS 9115F, but it's not being enforced.

NOW

- CMS can also lead the way by demonstrating on Medicare.gov how good consumer education and functionality can be presented
- CMS can develop more educational resources under its Medicare Learning Network geared towards different Medicare participating providers and health care organizations about their responsibilities for promoting interoperability

NEXT

- CMS can update Medicare Advantage Conditions of Participation by requiring MAOs to include consumer education in their STAR rating profile, include post a link to a gallery of apps that are already connected to their patient access API endpoint(s), and explain how beneficiaries can learn more if they want to connect their data through another app.

---

6 https://www.kff.org/report-section/ehbs-2024-summary-of-findings/#:~:text=AVAILABILITY%20OF%20EMPLOYER%2DSPONSORED%20COVERAGE,53%25).

7 California (https://www.dhcs.ca.gov/provgovpart/Pages/interoperability.aspx) and Tennessee (https://tn.amhealthplans.com/docs/current/member/1/member-interoperability-information.pdf) are the only states that currently require federal parity with CMS-9115F for health plans licensed in their states.

- As well, require MAOs to add requirements in the network contracts for their in-network providers to maintain accurate listings of their connected apps gallery, and maintain active patient access APIs throughout the contract term
- Update the CAHPS Survey with questions to beneficiaries to see if they are aware of their rights to connect their health data through their choice of application, both with their health plan and their in-network providers. Apply a strong weighting on this measure.
- CMS can also encourage state medical licensing boards to include Continuing Education Units on the same topics, to promote a culture shift and awareness about these compliance expectations

Similarly, the ASTP/ONC could update its Conditions and Maintenance of Certification with a requirement that Certified API Developers offer similar education in its customer-facing portals and through annual programming, to earn CEU credits.

PR-7 What strategies can CMS implement to support providers in making high-quality, timely, and comprehensive healthcare data available for interoperability in the digital product ecosystem? How can the burden of increasing data availability and sharing be mitigated for providers? Are there ways that workflows or metrics that providers are already motivated to optimize for that could be reused for, or combined with, efforts needed to support interoperability?

Some voices in the health tech community complain that data from FHIR APIs is not good enough to drink or swim in. Others say they can leverage AI to extract the data they need more easily from the documents exchanged over trusted networks or through Model Context Protocols.

To these statements, we offer the following considerations:

- **We should expect, but not wait for FHIR APIs to deliver high-fidelity streamable data.** Numerous downstream developers and stakeholders have AI-enabled and other technical capabilities and motivation to improve data quality, and should be encouraged to improve the quality of data so that it's fit for use for a wide range of use cases, including digital quality measure reporting, population health analytics and reporting, risk adjustment and digital health tools for patients and their caregivers.
- **Patients have an equally legitimate interest in high quality data.** High quality data is as important for patient access APIs as it is for other use cases. Health management and care navigation apps powered in real-time by high-fidelity streamable data is how to drive personalization off patients' consolidated longitudinal health summaries.

With these considerations in mind, b.well makes the following policy recommendations, each of which we believe CMS in conjunction with HHS and the ASTP/ONC can implement NOW, NEXT or LATER

NOW,:

1. **Add Data Quality to Certification Standards.** Hold Certified API Developers accountable

if they pollute or degrade the data stream.[8]

2. **Data Quality Ratings.** Lead an initiative whose objective is a standardized data quality tiered (gold, silver, bronze) rating framework, for increasing transparency of data quality conformance at individual API endpoints.
3. **Crowdsourced Reporting of Data Quality Issues.** Add an open Jira-like ticketing system to the ASTP/ONC's Inferno testbed. This would allow API connectors to report data quality issues at individual API endpoints as "bugs" and "feedback" to certified API developers, in a transparent way that encourages "upvoting" when others observe similar issues vendors. By adopting this common agile strategy for reporting data quality errors, upstream and downstream developers can work collectively and cooperatively to refine data for a high-performance rapid data transit system, without overburdening the formal regulatory complaint process
4. **Provenance.** Make data provenance an essential data class. There's no way to fix data quality at source, if you can't investigate the source of pollution or non-conformance.

NEXT,

5. **Open APIs for Reference Sets.** Either remove ICD-10 codes as reference data sets or obtain agreement from the AMA that their codes and underlying descriptions will be made accessible through open APIs.

LATER,

- **Updated API Conditions & Maintenance of Certification.** Add a data quality reporting requirement in the API Conditions & Maintenance of Certification as part of the technical documentation that Certified API Developers must publish and maintain, and service level expectations for acknowledging, responding and resolving data quality and other API

[8] Two examples illustrate when Certified API Developers contribute to bad data quality

Example 1 illustrates **pollution** in clinical data we see for patients like Kristen's daughter Bailey. Some of the EHR vendors with her medical records send her health data over patient access APIs with proprietary codes, instead of ICD-10 or preferred SNOMED codes required by the (g)(10) API specification. Without a data dictionary to map these proprietary codes to open standards, her patient data from these sources can't be incorporated without special effort into her longitudinal health record. An important negative risk of not using standard codes to help unify a longitudinal record is that it increases the risk of treatment errors and unnecessary repeated tests. AI certainly helps alleviate that effort, but not in real time in ways that are immediately evident in real-time computable data streams. This kind of conduct is a form of pollution, and we should be holding polluters accountable under our existing regulatory framework.

Example 2 illustrates **particulates** that make data **"turbid"** or **"muddy"**, requiring additional processing to make it swimmable or drinkable in longitudinal health records, for use in downstream apps and solutions . Most mammography-related data from certified APIs in the real world is coming through as Diagnostic Reports or Procedures. The way digital quality measures currently work, we would expect this data to be broken down between (i) Encounter resources for when a patient gets her mammogram, and (ii) Observation resources for the diagnostic report completed by her radiologist. Downstream developers can and do leverage AI and other tools to correct for these inaccuracies, but not necessarily in real-time. Meanwhile, what's happening is that stakeholders downstream have a confidence problem with using FHIR if we don't fix data quality issues now, so we're not seeing the high adoption of FHIR. It's not for lack of demand, but for lack of quality (and as we explain in the immediately following section, reliable performance).

performance issues

Secretary Kennedy spoke on June 3 at the In-Person Listening Session about the sanitizing effect of transparency. Building a collaborative, cooperative and continuous improvement feedback loop for data quality aligns with this principle, without always having to use regulatory enforcement as a threat or cudgel. By allowing downstream developers to innovate in data quality enrichment, this approach also aligns with the centering objectives in Executive Order 13813, signed on October 12, 2017, which affirms that government rules affecting the United States health care system should "re-inject competition into health care markets by lowering barriers to entry and preventing abuses of market power."

* * *

We look forward to continuing the work of advancing data exchange and empowering consumers together.

Please do not hesitate to contact us if you have any questions.

Kristen Valdes

Kristen Valdes

CEO and Founder

Jill DeGraff

Jill DeGraff

SVP Privacy, Regulatory Affairs & Compliance