Simplifying Data Access for Better Patient Experience:

Best Practices and Implementation Toolkit for Providers

Interoperability MATTERS

Consumer Engagement Workgroup

the sequoia project

Table of Contents

Forward

If you're reading this, you care about patient experience. Whether it's based on personal frustrations, professional interests, or some combination of the two, making life easier for the patients in your care matters to you. You want to get it right. Positive patient experiences translate into better patient outcomes, improved patient safety, increased patient loyalty, and a stronger reputation in the marketplace.

Each encounter patients have with their providers, clinics, or the vendors that support them provides an opportunity to build trust and loyalty – or diminish it. From the treatment in the clinic and the website's look and feel, to the hospital's participation in community events, providers' choices build or break credibility. Health system and provider executives know this. They invest heavily in improving patient care and projecting a positive image. Little things matter. It's essential to get it right.

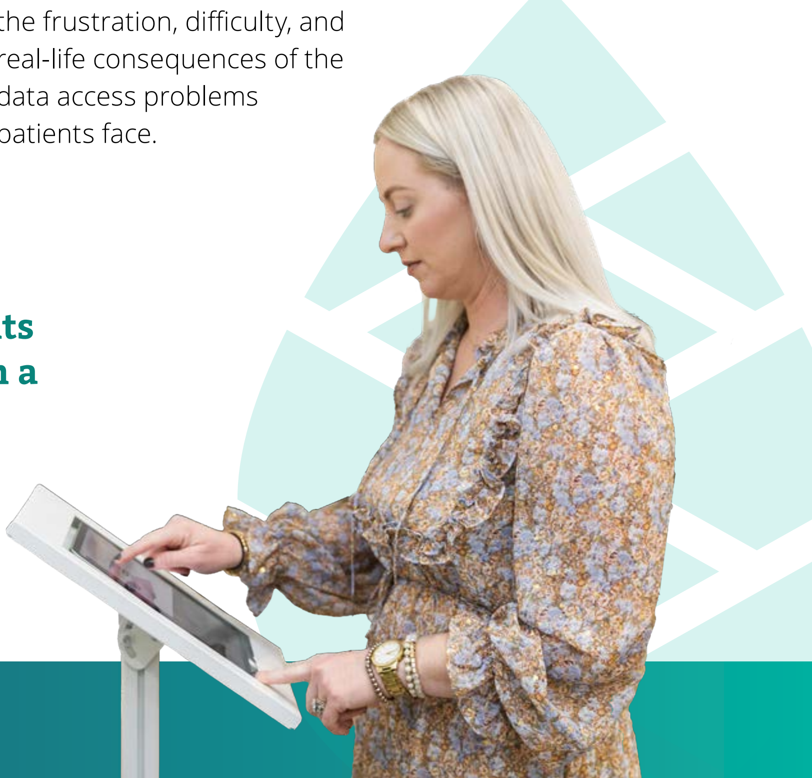
All this understanding and emphasis on patient service sometimes gets lost when it comes to patient data access. That part of the patient's experience can feel, at times, like an afterthought. Providers may think about patient data access through the lens of legal requirements and regulatory compliance. They seem to see it as separate from patient experience. The thing is, it isn't. In the eyes of the patient, it's all part of the continuum of care.

The Sequoia Project launched the Consumer Engagement Workgroup with a singular mission: making it easier for people to access and use their own health data. If your initial reaction when you read this mission statement is, "Haven't we done that already?", you're not alone.

Our Workgroup's Mission – *Make it easier for people to access and use their health data.*

We have policies that grant patients a definitive right to access their data in a timely manner without undue burden. At both the federal and state levels, the intent of the laws and regulations to support patients and caregivers is clear. Yet, the realization of this intent is far from the reality many patients experience. We began our work with a year-long convening of a patient forum to explore and understand real-life experiences of patients when they try to access their health data. The patients we worked with varied in age, ethnicity, socioeconomic status, education levels, and health conditions. They spoke candidly and in depth about their experiences interacting with their providers to gain access to their health data. The findings not only documented myriad data access barriers, but also captured the frustration, difficulty, and real-life consequences of the data access problems patients face.

We now have policies that grant patients a definitive right to access their data in a timely manner without undue burden. The intent of the law is clear. Yet...the realization of this intent is far from reality for many patients.



Patients experience difficult-to-understand, cumbersome, and often unnecessary procedural and administrative barriers to accessing their own data. These barriers require time, resources, problem-solving skills, and often, technical savvy to overcome. For many patients, they're first confronted with these labyrinthine tasks when they're dealing with a new health crisis or diagnosis. They're trying to understand their diagnosis and get the data they need to access care while keeping up with work, family, and life obligations that can't be put on hold. Precisely at the time their energy is the lowest, their fear and uncertainty are highest, and time is most precious, patients face administrative challenges that feel antiquated, unnecessary, and impossible to solve on their own.

For providers, the administrative processes they've established for accessing health data exist for a reason. The way they are executed made perfect sense at the time they were established. But since then, things have moved on. HHS has bolstered HIPAA with the Information Blocking Rule. Other industries that deal with sensitive data have found ways to make it easier and more secure for people to manage things like finances on their smartphones. These industries have enabled screen-based tools that manage identity, consent, and access to sensitive data, making the process easier to navigate while (mostly) maintaining security.

Meanwhile, many healthcare providers still rely on printing, signing, and faxing forms and receiving paper checks before releasing data on CDs. For people already stressed with illness and struggling to get access to their health data, this doesn't make sense. They try to understand why it's so complicated to get their own health data. They question their provider's motives. They wonder if it's just incompetence or if, for some reason, it's designed to be difficult. Is their provider neglectful or malevolent? That may seem extreme, but these are the things that go through the minds of frightened, frustrated patients. A patient's experience accessing their data can help make or break provider credibility.

The good news is, fixing these issues isn't difficult. You're already close! You're down to the "last mile" for patient data access, and it's likely you already have the team and skills on staff to make it happen. This best-practices guide and toolkit, shaped by patient voices and informed by experts, outlines what you can do to remove the final data access barriers.

We hope you'll join us, not only to enhance the patient experience, but also to improve patients' lives. The team at The Sequoia Project and our dedicated workgroup members want to help. Let us know what you think, what you need, and how we can all make this better.

Thank you for your commitment to making life better for patients and improving health, care, and data access experiences for all of us.

InteropMatters@SequoiaProject.org.

Introduction

Solving the "Last-Mile Problem" for Patient Data Access

We have come a long way in providing patients with access to their health data, but many patients still struggle to get the data they need when they need it.

In some ways, the administrative burdens associated with accessing data are baffling. More than 20 years after the establishment of the Department of Health and Human Services' Office of the National Coordinator for Health IT, recently renamed the Office of the Assistant Secretary for Technology Policy (ASTP), and nearly 30 years since the passage of the Health Insurance Portability and Accountability Act (HIPAA), we have very clear policy in place that requires providers to ensure that patients have access to their data without undue burden. There are a few policy tweaks that would make things work more smoothly, but the right to access data in a timely manner is firmly established. The technological infrastructure is there. Since 2009, we have invested an estimated $36 billion in tax dollars to fund the creation of a digital health infrastructure. We can and will continue to make improvements, but the proverbial pipes have been laid.

Meanwhile, other sectors that handle highly sensitive personal and financial data have implemented tools that enable secure, readily accessible management of personal information and assets on smartphones. The same patient who struggles to get access to the data they need for an upcoming specialist visit or surgery does so knowing that the previous day they simultaneously streamed Netflix, ordered a pizza, checked their bank account, and adjusted their 401 (k) all through their smartphone.

So why is patient data access still so challenging?

When it comes to providing patients with timely access to their data, the healthcare industry has a "last-mile problem." Many of the big problems have been solved. What remains is the frontline implementation needed to smoothly deliver health data to patients when and how they need it. The remaining problems don't require complex engineering or significant investments in new infrastructure. **What we need to solve these problems is a new perspective on how we communicate about and facilitate access to data.**

In short, providers need to think about patient health data needs from a patient's perspective. Solving the last-mile problem for patient data access must begin with user experience design.

This toolkit is not a textbook for user experience design. Instead, we've used the perspective of user experience to inform the development of a set of best practices and a toolkit focused on solving the last-mile problem for patient data access. We aim to help shape providers' approach to serving patients' data needs, making it easier for them to adopt a user-centered design for the operational and process tasks associated with patient data access.

Begin with the User in Mind

Imagine you're a patient. Except for seasonal colds, flu, and a couple of broken bones from that skiing accident in college, you've lived a healthy life. You see your doctor once a year for a physical. Every year, you get a clean bill of health, wish your doctor well and say, "See you next year." But during one of these routine visits, the doctor notices something concerning: your blood work is strangely out of range. Or maybe there's a lump that you've missed or a misshapen mole on your back.

Or maybe it's your son. Your seemingly healthy baby misses their developmental milestones or has a seizure.

Regardless of the details, the circumstances change. The conversation with the doctor shifts. It's imbued with confusion, fear, and urgency. You're referred to a specialist who orders additional tests. Those tests suggest you need a consultation with a new specialist who practices at a different hospital in a different city. Meanwhile, your best friend from college is a doctor who knows a lot about your new diagnosis and wants to help.

Your head is spinning. You're frightened.

You Google symptoms and procedures, desperate to understand your new condition. *What will you tell your family? Your boss? Should you cancel the vacation you have planned for next month? What do you need to do to get the best care you can when your week is already packed with pressure and deadlines?*

But first, you need to get your test results and doctor's reports so you can send them to the specialist in another city. This process should be easy. You work with spreadsheets for work, and you manage your 401 (k) from your iPhone.

You start by going to the referring doctor's website on your phone, but it's confusing, so you switch to your computer.

To get the data, you need to sign up for a patient portal. That requires getting a code from your doctor, but it's now past 4 pm on a Friday, and the doctor is out of the office. *Should you call the on-call doctor? Will they think this is an urgent request?*

Finally, Monday rolls around. You call the doctor and listen to a long list of pre-recorded prompts. You're not sure which extension to choose, so you pick one. Nobody picks up, so you leave a message. Then you wait.

You have a meeting and put your phone on "Do not disturb." After the meeting, you notice you have a message from the doctor's assistant about the code you need to get a portal account. You call back, listen to the list of possible extensions, choose one, and leave another voicemail.

We aim to help shape providers' approach to serving the data needs of patients, making it easier for them to adopt a user-centered design of the operational and process tasks associated with patient data access.

Finally, they call back when you can answer. You get the code you need to set up the portal. The portal requires you to set up multi-factor authentication, which involves annoying texts and more codes. You do all of that.

By now, four days have passed, but you finally get into your patient portal at this one doctor's office. You find some of the data, but not all of it. You download your labs and diagnostic codes in a PDF, but you can't find the images you need. You search through all the tabs and menus on the portal. Eventually, you see a report that includes four sentences in medical jargon describing the image, *but where is the actual image?*

Finally, you give up and call the doctor's office. Again, you get the phone tree. Again, you leave a message. By now, it's 4 pm, and the staff no longer answers the phone. You're forced to wait until the next day.

The next day, you speak with the doctor's administrator who explains the process for getting your images. The doctor can send the images directly to the new specialist, but that requires a form. The form needs to be printed and signed, and either mailed, hand-delivered, or faxed. Faxed? Your office doesn't use fax, so you start thinking about who you know who might have a fax machine. But you still want the image to send to your friend. The administrator explains that the file can't be sent by email. She instructs you to call the medical records department. You make the call. Another phone tree. Another voice mail. After several attempts, you connect with a human and are informed that the image can be mailed to you, but first, you need to mail a personal check to the medical records office.

Once the check has cleared, they will send you the image file by mail within 30 days. *A check? 30 days? Do you even have a checkbook anymore? Or stamps?* You need the image now, so that you can get your friend's advice!

You look at the clock and realize you're 20 minutes late to an important meeting. You scramble to get your stuff together, run to the meeting, and sit there half-listening while your mind races with fear, anxiety, and a long list of new problems to solve.

This is the process patients face when they want to access their data. Each step is there for a reason. Each of them, when examined separately, doesn't seem like that big of a deal. However, taken as a whole, each of them adds up to a lot of little but often consequential barriers. In a world shaped by technology designed to capture and cater to the needs of users, the need to print, sign, fax, and write checks to access your own data feels like a cruel prank being played when you're at your most vulnerable. It can be bewildering and infuriating. This frustration may be no one's intent, but it is the reality patients confront.

The experience of this fictional patient is based on many stories of real patients – real people who, at their most vulnerable moments, are suddenly thrust into a world of processes and requirements that seem mind-bogglingly antiquated and out of sync. It is the experience of these patients that has shaped our workgroup's approach to developing our best practices and the tools we have created to support providers who want to implement them.

> In a world shaped by technology designed to capture and cater to the needs of users, **the need to print, sign, fax, and write checks to access your own data feels like a cruel prank being played when you're at your most vulnerable.** It can be bewildering and infuriating.

Simplifying Data Access for Better Patient Experience:
Best Practices and Implementation Toolkit for Providers

Best Practices

Best Practices

Improving Patient Data Access Experience

Providers need to develop easy-to-follow processes and tools to facilitate timely access to electronic health information for patients. These processes and tools should be readily accessible and easy to locate, understand, and execute for any patient who needs timely access to their data.

The following list of “best practices” outlines important elements and factors to consider and implement to ensure patients can access what they need to facilitate timely, high-quality care. The recommendations are grouped into six categories:

Simplicity

Making it easy to find where and how to access personal health data.

Information Needs

Providing essential information about health data access, rights, and use.

Process & Integration

Reconfiguring operational processes and tools to focus on patient needs.

Design Guidance

Using web and graphic design tools to make it easier to find and act on critical information related to health data.

Training

Empowering staff to ensure they can succeed in meeting patient needs.

Updates & Maintenance

Establishing a process for keeping information about patient data and data access resources updated and working.

Simplicity

Providers need to strive to reduce and eliminate any points of friction for patients who need access to their data.

Patient Data Resource Center (PDRC) – Consolidate all personal data-related information in a central, web-accessible "resource center," which includes data access guidance, along with information about data policies and privacy. The resource center should be designed to prioritize attention to how to access data, ensuring that patients with limited time and high stress can quickly and easily find what they need without having to sort through dense pages of information.

PDRC Elements:

- **Data Access Process** – Specific elements that should be included are listed in the informational best practices below.
- **Data Privacy Policies** – Bulleted overview and full text of the provider's data privacy policies.
- **Health Information Exchange** – Information about how patient data is shared through HIEs, TEFCA™, and other private exchanges.
- **Portal Access** – What to expect from the patient portal and how to access the portal.
- **Mobile Access** – Information on any mobile apps or mobile device tools that the provider has developed, recommends, or enables connection through or with the patient portal or other provider data tools.
- **Patient Consent** – Patient consent or constraint of data access, including general opt-in/out policies and specific controls or opt-out rights for certain sensitive information.

Information Needs

Providers should provide patients with written guidance on how to access data available to patients in two formats:

1. **Provider Website** – Viewable on any major web browser or mobile device.
2. **Printed or Printable Handouts** – In a format that providers and/or their staff can easily print in response to patient questions about how to access data.

These materials should include the following types of information.

Patient Right to Information – A clear articulation of the patient's right to their electronic health information as dictated in federal law and policy. The overview of rights does not need to and should refrain from providing a detailed description of the laws and regulations that enumerate the right to data access.

However, it should succinctly state the data access rights derived from relevant policy, including:

- 21st Century Cures Act (2016)
- Cures Act Final Rule, specifically the Information Blocking Rule (2020)
- HTI-1 Final Rule (Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (2023) (specifically Individual Access Services through TEFCA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent rules supporting the patient's right of access.

Types of EHI – A list and brief description of the various kinds of electronic health information (EHI) that are generated by that provider's practice and/or that institution, as well as instructions for gaining access to that information.

Fees – A clear articulation of any fees that will be charged to patients to facilitate access to their electronic health information.

Format Options – Options for the formats in which the information can be provided, which will enable the patient to request the information in the form they need. (i.e., on a CD, thumb drive, portal link, printout, PDF, etc.).

Timing for Information Retrieval – Projected timing for receiving information types, based on the type of data requested.

Needed Forms – Easy, immediately accessible access to any forms that need to be completed, along with specific instructions for how to submit the forms. Ideally, forms should be able to be submitted through a web-based tool that does not require printing, wet signatures, scanning, faxing, or mailing.

Proxy Authorization – Clear instructions for how to enable proxy authorization and access, as well as any requirements or guidance for accessing adolescent data.

Data Options – An overview of the type of data that can be accessed via the patient portal, as well as instructions for how to download and/or transmit data through the portal.

Historical Data Access – Overview of the types of historical data that are generally available in a patient's data archive, how to access that data through medical records, along with information about fees, timing, required forms, etc.

Correcting Data Errors – Clear instructions on how patients can notify providers of errors in their medical records and request corrections

Process & Integration

Providers should consider each of the types of patient health data and information produced by and exchanged with them. Providers should also consider how to provide that information in the most patient-centric way. Considerations should include:

1. **Format** – Providers should think through in advance what needs to be in place for data to be provided to the patient in both printed/viewable formats, as well as machine-readable formats, such as those that can be downloaded directly through the portal or through another form.
2. **Manner** – Providers should ensure that they can provide copies of the data in a format that will be usable by the patient, as well as another provider. Given that most patients no longer have disc drives, alternative tools for data sharing should be provided, such as USB drives (including USB-A and USB-C) or a link to the structured data file.
3. **Required Forms** – Providers should strive to remove any friction points and unnecessary steps that they currently require to provide patients with their data. Before requiring patients to complete a particular form to access their data, providers should evaluate if that form is legally necessary. If the form is legally required, it should be able to be completed in an electronic format that does not require printing, faxing, notarization, or mailing.
4. **Payment** – If providers choose to charge a fee for providing the data, and the law allows a fee to be charged, the provider should allow patients to pay that fee using any of the methods that can be used for payment for services, such as credit cards, debit cards, or mobile device-enabled electronic wallets. In addition, the provider should ensure that payment for data access can be made using a method that is at least as frictionless as payments for treatments. (i.e., if the provider takes payment for services through the website, they should also accept payment for fees associated with accessing data through their website).
5. **Proxy Access** – Providers should have a clearly defined process for enabling patients to assign proxy access to caregivers. The process should be easily understood and executed by the patient.
6. **Adolescent Data Access** – Access to data for adolescents and parents of adolescents needs to have an easy-to-understand overview of their policies and processes for patient and parent access. The variability and complexity of these issues can be challenging and vary among states, but for both adolescent patients and their parents, providing clarity and enabling agency are essential.
7. **Urgent Access Process** – Providers need to have a process for patients to request, access, and/or send copies of their data for urgent needs, such as an urgent health issue requiring immediate attention in critical care or a second opinion from a specialist at a different health system. This process should include:
   - Direct Communication – The ability to speak with and/or directly contact someone who can facilitate timely access.
   - Clear Steps – The ability to set expectations based on understanding how the process works.
8. **Internal Tools** – There should be mechanisms for staff to support/facilitate patient data requests at the departmental level without having to send them on to other parts of the organization (so a patient could call their usual contact point and get a resolution directly).

Design Guidance

Providers should utilize established user experience/user interface design methods to refine their web-accessible services and develop printable materials that facilitate low-friction access to guidance on how and where to access electronic health information.

1. **Readability** – Language should be written to be readable at an eighth-grade level.
2. **Accessibility** – Providers should ensure that the design of the Patient Data Resource Center and the various elements within it are accessible for patients with visual impairment.
3. **Terminology** – Providers should use consistent wording or phrases to refer to patient health data or medical records. We recommend:
    - Patient data
    - Patient health information
    - Electronic health record
4. **Placement** – Providers should include readily visible links or call-out buttons on their web-accessible service/website to make it easy to find how to access their data. This section should include one or more of the following:
    - Inclusion in the site's top navigation menu.
    - Inclusion in the site's footer as a key category in a readily legible font size.
    - Utilizing "call-to-action" buttons or graphic icons that will take patients directly to a page with the data access process and overview.
5. **Search Terms** – Website design should include back-end tools to link likely search terms used by consumers to describe patient data to results that direct patients to the correct page. The following is a list of suggested search terms
    - Data access rights
    - Rights to data access
    - Medical records
    - Health records
    - My medical records
    - My health records
    - My medical history
    - My health history
    - My medical file
    - Medical records access
    - Medical records update
    - Health records access
    - Health records update
    - Share my data
    - Sharing my data
    - Download my data
    - Download my records
    - Export my data
    - Export my records
    - Release of medical information
    - Release of health information
    - Health Records Department
    - Health Information Office
    - Clinic records department
    - Hospital records department
    - HIM
    - Health summary
    - Medical summary
    - Patient portal
    - Request medical records

Annual Updates – Provider practices and institutions should ensure their web team, communication team, and compliance officers regularly review their website and patient handouts to ensure they are accurate, up-to-date, and functional, verifying that the content is still valid, the links still work, and that processes/payments are in place.

Issue Reporting – The data access overview page should include a method for reporting issues and errors, along with a support contact number. The person or department responsible for monitoring those requests or reports must be held accountable for responding to any notifications or support requests.

Training

To ensure they comply with federal law and provide patient-centered care and support, providers should take steps to ensure that their staff, consultants, and information management vendors are fully trained on how they can best facilitate timely access to patient data.

- As part of their regular staff training, providers should ensure their medical and administrative staff are aware of data access rights, tools, processes, and protocols.
- As part of their contracts with EHR vendors and information management companies, providers need to include requirements that ensure their EHR and information vendors best facilitate patient data access in a manner consistent with the law and in support of patient needs. Specifically, these contracts should include:
    - Requiring that vendors' employees be trained and annually tested on current federal policy and requirements, including the 21st Century Cures Act Final Rule and the Information Blocking Rule, as well as HIPAA.
    - Facilitating electronic access to patients' data for patients who need it quickly and urgently, without the need to call, print, fax, or mail any documentation to the records facility.
    - Enabling electronic submission of any forms required to access data, including the importance of understanding that patients have limited access to printers, faxes, and paper check writing.
    - Accepting electronic payment for fees through a web- or mobile-enabled payment system that works with major credit/debit cards.
    - Requiring health information management vendors to conduct user testing across a sampling of provider patients to ensure patients can readily access their data in a timely manner.

Updates & Maintenance

Providers should create and maintain a systematic process for reviewing, updating, and validating all information related to patient data access that appears on their websites, patient portals, and printed or printable materials. This ensures that patients, caregivers, and staff always have access to the most current and accurate information about their rights, processes, and tools for accessing health data.

The update process should include the following core elements:

Establish a Review Schedule – Providers should adopt a formal update schedule—at least annually, and ideally semi-annually—to review all materials related to patient health data access. This review should include web pages, PDRC content, downloadable forms, portal instructions, and printed handouts.

Assign Ownership and Accountability – A designated data access oversight team (or equivalent cross-functional group) should be responsible for coordinating these reviews. The team should include representatives from compliance, communications, IT/web services, and patient relations. One individual should be clearly identified as accountable to ensure updates are completed on schedule.

Monitor for Policy and Technology Changes – The update process should include monitoring for:

- New or revised federal or state regulations (e.g., ASTP/ONC, CMS, HIPAA, Cures Act, TEFCA updates).
- Changes to EHR vendor capabilities that affect data access.
- Internal process or staffing changes that alter how patients obtain their data.
- Broken links, outdated forms, or inaccessible web content.

Document and Track Revisions – Providers should maintain a change log recording the date, description, and responsible party for each update. This log supports accountability, quality improvement, and compliance verification during audits or policy reviews.

Communicate Updates Internally – Once updates are published, all relevant staff should be notified and trained on any changes to patient data access procedures or resources. This includes front-desk staff, medical records personnel, and compliance teams.

Ensure Consistency Across Channels – Updates made online should be reflected immediately in all printable or distributed materials such as brochures, discharge packets, or portal instructions. Consistency minimizes confusion and ensures patients receive the same information regardless of format or contact point.

Patient Feedback Loop – Providers should offer an easy way for patients to report errors, broken links, or outdated information on the website or printed materials, and ensure those reports are routed directly to the oversight team for timely correction.

Simplifying Data Access for Better Patient Experience: Best Practices and Implementation Toolkit for Providers

Implementation Toolkit

Implementation Toolkit

How to Use this Toolkit

The toolkit is divided into seven sections, which are aligned with the key elements of the Best Practices. These include:

- Simplicity
- Information Needs
- Process & Integration
- Design Guidance
- Training
- Updates & Maintenance
- Implementation Checklist

In addition, we have included two sections that provide informational resources and implementation tools to help facilitate your team's adoption of the best practices.

Each section includes several categories of informational, process, and design needs, all of which align with the recommended best practices. Within each section and category, you'll find two consistent components:

Guidance for Implementors – This component provides context and background for those implementing the recommended best practices. By providing this background, we hope to help implementers understand the legal framework and requirements, as well as the importance of this information for patients seeking to access the data they need.

Recommendations for Implementers – This component provides brief, bulleted recommendations for implementers responsible for creating a Patient Data Resource Center (PDRC).

Implementation Toolkit:

Simplicity

Simplicity

Guidance for Implementors

When you step back and think about health data from the patient's perspective, most providers' websites can be confusing to navigate. Our workgroup conducted an extensive audit of provider websites to get a baseline understanding of how providers of different types and sizes approached patient data. While some were better organized than others, nearly all of them had aspects of policies and processes related to patient health data scattered throughout the website. Privacy policies are in one place. Patient rights are in another. Portal information has its own section. Medical records often require some digging to locate. Information about data exchange, if available, was typically minimal.

Through the patient's lens, none of this makes sense. When you're trying to find what you need, particularly if you're frightened, stressed, or pressed for time, it can feel like it's deliberately confusing. Things seem hidden. It's as if the provider web team sat down and conspired to make it as challenging as possible.

If you change your lens and view the same website from the provider's perspective, it begins to make sense. It's easy to understand how this disjointed approach to patient data emerged across the industry. Especially for large healthcare systems, each of these issues is managed by a different department with distinct reporting structures. Each of these data-related elements no doubt emerged on its own timeline in response to a new legal or regulatory requirement. In response, somebody rightfully decided it needed a place on the website. It wasn't meant to be intentionally confusing. That's just the way it evolved. It wasn't designed that way – the problem stems from the fact that it was never designed at all.

When you consider the needs of a patient who is ill, stressed, and pressed for time, what they want and need is for everything to be simple. They need to access their data, understand how it is used, enable access to family or loved ones, and know what they need to do to take action in real-time. Patients do this daily for apps and platforms that have highly sensitive personal and financial data. They expect – and deserve – to be able to do the same when it comes to their health.

Empathetic and effective design begins with the patient's perspective, centering on their needs and organizing health data so it's easy for patients to use.

The cornerstone of our best practices is the creation of a *Patient Data Resource Center.* The resource center should include all information related to patient data in one central location on the provider's website.

Patient Data Resource Center – Consolidate all personal data-related information in a central, web-accessible "resource center" that includes guidance and tools for data access, along with information on data policies, data exchange, and privacy. The resource center should be designed to prioritize data access, ensuring that stressed patients with reduced problem-solving capacity don't have to dig for what they need on a dense page of information.

Patient Data Resource Center Elements:

- ☑ **Data Access Rights and Process** – Specific elements that should be included are listed in the informational best practices in this toolkit.
- ☑ **Data Privacy Policies** – Bulleted overview and full text of the institution's data privacy policies.
- ☑ **Health Information Exchange** – Information about how patient data is shared through HIEs, TEFCA, and other private exchanges.
- ☑ **Portal Access** – What to expect from the patient portal and how to access the portal.
- ☑ **Mobile Access** – Information on any mobile apps or mobile device tools that the institution has developed or recommends.
- ☑ **Patient Consent** – Patient consent or constraint of data access, and general opt-in/ out policies, and specific controls or opt-out rights for certain sensitive information.

Recommendations for Implementors

- **Begin by understanding the patient's** data access and information needs, and design your data-related site elements to meet them.
- **Focus on patient user experience,** rather than institutional or departmental organization.
- **Consolidate all patient health data in a central** "hub" on your website.
- **Make it easy and obvious for patients** to find the PDRC by prominently placing links or action buttons on the home page.

Implementation Toolkit:

Information Needs

This section provides an overview of the information that patients need to understand how to access their health data successfully. Providing this information to patients in one easy-to-find place not only makes it easier for patients, but also reduces the administrative burden on staff who would otherwise have to respond to requests.

Patient Data Rights

Guidance for Implementors

Federal law gives patients the right to access all their health information. If you have data in any format that was generated by, through, or on behalf of a patient, that patient is legally entitled to be able to access that data to use in any way they choose.

Through the 21st Century Cures Act and the Information Blocking Rule, the federal government specifically requires you to make any electronic or digital data available to patients in a timely manner. This need is especially true in situations where urgent or timely access is essential for that patient's care.

While some of the critical data that patients need is available through the patient portal, some of it is not. As a provider or company that works on behalf of providers, it is your responsibility to facilitate access to any and all data generated by that patient, including data stored in systems outside of the patient portal and EHR, such as images, EEGs, ECGs, and other types of data.

Why is it important for you to help patients know their data rights?

For those who work in provider offices, health data companies, and healthcare institutions, the idea of data access and use is well understood. However, for many patients who need to access their data, knowledge of what data is available and how to access it is often limited.

By making it clear to patients and caregivers what they have a right to access, you can help patients understand what to expect and how to engage with you to obtain the data they need.

Below is a list of the key federal laws and regulations that have been enacted over the past 30 years that collectively created patient data access rights and describe what is required of providers to remain compliant with federal law:

- ☑ **Health Insurance Portability and Accountability Act of 1996** and subsequent rules supporting the patient's right of access.
- ☑ **21st Century Cures Act Final Rule (2020)** specifically the Information Blocking Rule component of the Final Rule.
- ☑ **HTI-1 Final Rule** (Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (2023).
- ☑ **HTI-2 Final Rule** (Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (2024) (codifies individual access through TEFCA).

Recommendations for Implementors

- **In a prominent location within the PDRC,** provide a brief overview of patients' legal rights regarding data access. This helps clarify for patients what they can and cannot access and sets expectations for both patients and staff about what is required by law.

- **Keep the overview relatively brief and straightforward**, focusing on communicating the rights to data access rather than on detailed descriptions of the laws and policies that underpin them.

- **Provide a link to the laws and regulations** as a footnote to this section of your written or web communications..

- To help you get started on this section of your PDRC, we have provided sample text for you to adopt or adapt for use on your website or in written communications to patients. See ***Appendix B***.

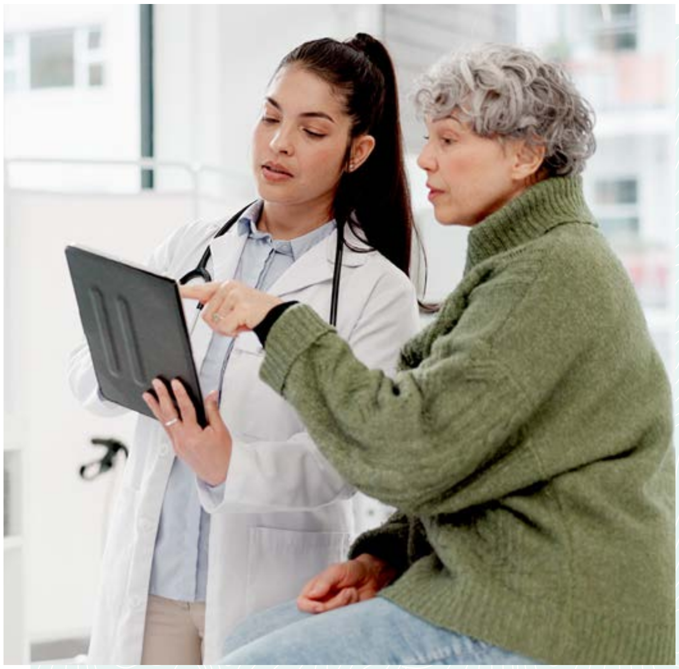
Data Types and Access

Guidance for Implementors

Patients have a right to access any and all data that is generated about them in the course of their medical treatment at your institution or practice. If you have data about that patient's health, treatment, or care, you are required by law to make it available to them. If the data is in a digital form of any kind, you are required by the Information Blocking Rule to make it available to them electronically in a timely manner.

While portals provide access to some of the data to which patients are entitled, they do not include all the data. We recommend that providers clearly inform patients about the types of data accessible and the steps required to access them.

Federal law requires that patients have access to any electronic health information generated by your practice about that patient's health or care. The type of data you might have about a patient will depend mainly on the type of practice or institution and the patient's needs and health history. We have developed a list of the types of electronic health information that are likely to be generated about a patient. We recommend using this list as a checklist for your institution, selecting the information relevant to the type of care you provide.



It's essential to keep in mind that patients may not fully comprehend all the data generated during their care. For individuals with complex illnesses who need all their data for personal records or to use with a provider in a new location, seeing the list of available data types will make it easier for them to request the necessary data with fewer support requirements from practice staff.

Recommendations for Implementors

- **Make it easy for patients to readily view** a list of all the electronic health information your practice or institution collects.
- **For each data class listed, provide** specific guidance on how they can access that data. For web-based communications, provide a link to more information on how they can access that data.
- **Use the checklist on the next page** for your practice. Work with your health data team to determine which data classes are generated at your institution or practice, and list those elements in your informational handouts and website.

Clinical Data Types

1. Clinical Notes
Documentation created during patient visits, including progress notes, discharge summaries, and procedure notes.

2. Health Conditions List
A list of a patient's current and past health conditions that impact care decisions.

3. Medication List
A record of current and past medications, including dosages and prescription history.

4. Allergies and Adverse Reactions
Information on known allergies and reported side effects to medications or other triggers.

5. Laboratory Results
Results from blood tests, urine tests, tests for bacteria or viruses, genetic tests, and other diagnostic labs.

6. Imaging and Diagnostic Reports
Radiology images, such as X-rays, MRI/CT scan results, eye images, and related reports detailing any findings from the imaging.

7. Procedures
Records of any surgeries or other medical procedures performed on the patient.

8. Vital Signs
Data on heart rate, blood pressure, temperature, respiratory rate, functional assessments, and other essential indicators.

9. Immunization Records
Documentation of vaccinations received.

10. Care Plans
Treatment plans detailing goals, interventions, and outcomes for managing a patient's health.

11. Encounters
Records of healthcare visits, including dates, providers, and purpose.

Behavioral and Social Health Data

1. Behavioral Health and Substance Use Data
Mental health records, substance use treatment plans and therapy notes. Exceptions may apply.

2. Social Determinants of Health (SDOH)
Documented social and environmental factors, such as housing instability or transportation needs.

Advanced and Emerging Data Types

1. Genomic and Molecular Data
Results from genetic testing and other types of molecular profiling.

2. Device-Generated Data
Data from medical devices, such as glucose monitors, heart monitors, or CPAP machines, used during treatment.

3. Longitudinal and Patient-Reported Data
Results from genetic testing and other types of molecular profiling.

4. Palliative and End-of-Life Care Details
Advance directives, hospice care plans, and other end-of-life preferences documented in the medical record.

5. Advanced Vital Signs and Continuous Monitoring Data
Measures such as oxygen saturation trends or data from continuous monitoring devices incorporated into the record.

Administrative Data

1. Demographics
Basic identifying information such as name, address, date of birth, and sex.

2. Billing and Claims Data
Records of services provided and claims submitted to insurers.

3. Care Team Information
Details of healthcare providers involved in a patient's care.

4. Legal and Administrative Documents
Medical power of attorney, consent forms, and other legal documents related to care.

5. Nutrition and Dietary Data
Dietary assessments and nutritional recommendations are documented in the record.

6. Environmental and Occupational Health Data
Records of workplace exposures or environmental factors affecting health.

Data Access Fees

Guidance for Implementors

Legally, providers may charge reasonable fees to patients for providing access to certain types of health information. However, the law requires certain records to be accessible free of charge and limits the fees providers can charge for access to other records.

Record Types and Fees

Patient Portal Data – Under the federal Information Blocking Rule and HIPAA, providers are prohibited from charging patients for accessing their medical records through the provider's patient portal. That access must be free.

Other Records – For records not accessed through the patient portal, providers may charge fees to cover some of the labor costs associated with providing them. For example, suppose the records are provided in hard copy, or the information is being emailed, faxed, or downloaded to a data storage device, such as a thumb drive or disc. In that case, HIPAA permits providers and health plans to charge a "*reasonable, cost-based fee*" for the labor associated with printing and compiling the medical records, while making it clear that providers are prohibited from charging for costs associated with the search and retrieval of the records. Providers are also allowed to charge patients for the cost of any office or device storage supplies required to produce the copies in the requested format. HIPAA does not permit patients to be charged "*search and retrieval*" fees.

In other words, providers are not allowed to charge patients for labor associated with searching for and retrieving patient records.

However, if it takes an hour for a staff member to copy a patient's records or download data or images to a storage device, providers can charge reasonable fees to cover the labor costs for that time, plus the costs of the paper, or thumb/disc drive to transfer the data, along with any postage or shipping fees.

State-Sanctioned Fees – While federal law defines the types of costs providers may charge, states have established maximum limits on what providers may charge anyone who lawfully requests records. Every state in the U.S. has laws that set the maximum amount that can be charged to individuals for obtaining copies of medical records. In many states, costs are defined by "per page" charges that the state deems permissible.

However, even if the requested records are paper records, providers and health plans cannot charge the state-defined fees if the total cost would exceed what HIPAA defines as "reasonable." *As federal law, HIPAA preempts or overrides state laws that provide fewer patient rights.*

Final note: Many healthcare providers and health plans offer patients access to their records at no cost. Currently, one state, Kentucky, mandates that providers provide patients with one free copy of their health records per year. Providers are required to provide patients with their data in the format chosen by the patient. However, as a matter of practice, we recommend that providers seek to provide patients with their data in electronic form whenever possible. Whether the data is structured or in PDF form, electronically provided data is often easier for patients to view, store, and access when needed. It also makes it easier to share data with other providers, patient data registries, and/or utilize new forms of health data guidance platforms, such as large language models (LLMs) and patient-facing artificial intelligence tools. If providers are providing printed copies, we recommend providing one free copy of records per patient per year, which helps keep requests to a minimum and prevents financial barriers from blocking patient access to data.

Fee Guidance for Providers That Maintain Electronic Records

Flat Fee for Electronic Copies of PHI Maintained Electronically – Under the HIPAA Right of Access, healthcare providers may charge patients a flat fee of up to $6.50 for electronic copies of their health records stored electronically. This fee must include all labor, supplies (such as a CD or USB), and any postage. No additional charges are allowed.

Choosing the flat fee is a convenient option for providers who want to avoid calculating actual or average costs for each request. However, whether using a flat fee or another method, any charges must comply with HIPAA rules—not just state law. ***HIPAA only allows reasonable, cost-based fees that cover limited labor, supply, and postage costs. Providers cannot charge for activities such as searching for or retrieving records, even if state law permits it, since these costs are not covered under HIPAA.***

Using Average Costs for Record Requests – Instead of calculating the labor cost for every request, healthcare providers can establish a standard cost based on the average time it takes to handle common types of requests. This process is allowed as long as providers include only the types of labor costs that HIPAA rules allow – such as time spent copying records, but not searching for them – and the fees are reasonable. Providers can also add the cost of supplies (such as paper, a CD, or a USB drive) and any applicable postage.

A per-page fee can only be charged in two circumstances.

1. If the records are on paper and the patient wants a paper copy.
2. If the paper records are being scanned into an electronic format.

HIPAA only allows reasonable, cost-based fees that cover limited labor, supply, and postage costs. Providers cannot charge for activities such as searching for or retrieving records, even if state law permits it, since these costs are not covered under HIPAA.

Providers cannot charge per-page fees for records that are already stored electronically.If a patient requests electronic copies of their records, the provider can charge only for the actual labor costs of creating and sending the copies.

Please note: ***In situations where the state law provides individuals with greater rights*** of access to their health information than those outlined in the HIPAA Privacy Rule, ***the state law takes precedence (see 45 CFR 160.202 and 160.203).*** Therefore, if your state prohibits charging fees to individuals who request copies of their health information or sets fees lower than those required by the HIPAA Right of Access rule, providers must follow the state law. If, for any reason, state law permits higher fees than those outlined by HIPAA or restricts access in other ways, the provisions in the HIPAA right of access rule take precedence.

A detailed table is available in ***Appendix A***, listing all current state laws related to patient access fees, along with links to the corresponding laws. These laws and associated fees are accurate as of July 2025. However, state laws change frequently. Statute links change frequently. If the link is broken, you may search for the provided code number.

Recommendations or Implementors

- **Try Not to Charge Fees** – When possible, refrain from charging fees for patient data access. The data is generated by and about the patient. If they want to access it, it's a sign that they want to be actively engaged in their care. Supporting this engagement helps build trust between the patient and your practice/institution.
- **Make One Copy of Data Available for Free Yearly** – If you do decide to charge fees, consider adopting the practice of making one copy of data available for free for each patient per year. This will keep costs from discouraging patients from getting the data they need for their care while keeping requests for difficult-to-access data in check.
- **Make Fees Clear in Advance** – If you charge fees, in your PDRC, clearly and succinctly state what, if any, fees are associated with accessing different types of data.
- **Explain Why Fees are Needed** – Keep in mind that patients may not fully understand the complexities of accessing their data. It may be helpful to note that the fees cover administrative time and costs.
- **Make Payment of Fees Easy** – Enable patients to pay for data access fees on the website with credit or debit cards. In short, if you accept payment for co-pays, make it possible to use the same payment methods for data access fees.

Required Forms

Guidance for Implementors

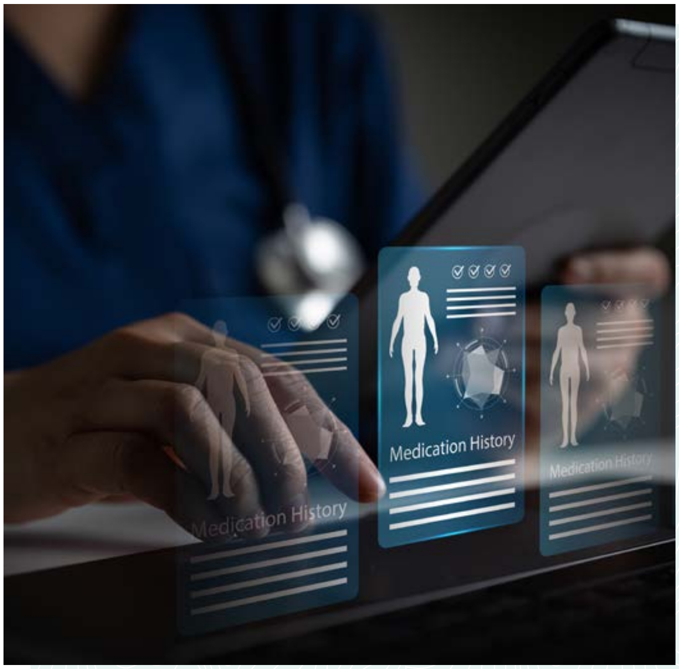
Federal Law

Healthcare providers should strive to eliminate any friction points and unnecessary steps that hinder patients' access to their data. Before requiring patients to complete a form, providers should evaluate whether it is truly necessary.

Federal law allows providers and health plans to require patients or their proxies to submit a written request for their health information. It is common for providers and health plans to have their own forms for making these requests.

The specific elements of this form will depend on the requirements of your practice. However, we recommend keeping it simple. Only require information that is necessary to complete the data access request.

Keep in mind that patients who are seeking their data may be stressed or overwhelmed. Make any requirements for submitting the form easy for them to fulfill, or consider accepting any written requests from patients that meet applicable legal requirements. Whenever possible, we highly recommend using digital tools to enable web-based form submission. Many people lack access to printers. Requiring patients to print a form, sign it, scan it, and then upload, email, or fax it creates substantial logistical challenges and administrative burdens for some patients. The fewer process burdens you create with form submission, the easier it will be for your patients to submit the form to you without needing to call staff for assistance.



Similarly, if fees are associated with the data for which the form is required, make it possible to pay those fees at the time of the form submission. A variety of web and mobile-based payment tools can be incorporated into the form submission process. Requiring a separate process for fee payment creates additional work for both patients and your staff.

The American Medical Association has developed a set of forms for providers to use to facilitate patient information requests. A copy of that form is provided in ***Appendix A***.

Recommendations for Implementors

- **Keep Forms Simple** – Only collect the required information. Consider accepting a patient-submitted written request for records, even if it isn't submitted through your institution's form.

- **Make Form Submission Easy** – Allow digital submission of the forms through a web- or patient portal-based form tool that enables written fields to be completed digitally and facilitates digital signatures.

- **Reuse Available Forms** – Use the forms developed by professional groups, such as the American Medical Association. These forms have been vetted and are available for you to use and repurpose at no cost.

- **Digital Payment Options** – Consider using a digital payment tool to allow patients to pay any fees at the time of form submission. Ensure that fees can be paid using credit and debit cards. In short, if you can submit payment for services by a credit card or through an online payment platform, you should also accept the same forms of payment for any fees for record access. This change will reduce the burden and workload for both patients and decrease demand on your administrative staff.

Proxy Access

Guidance for Implementors

Under the HIPAA Right of Access, patients have the right to designate a third party—**a personal representative or proxy**—to access their health information. For many patients, proxy access is essential to timely, informed decision-making. This process is especially vital for those managing chronic illness, navigating disability, or coordinating care for dependents.

Within the Patient Data Resource Center, providers should have a clearly defined process for enabling patients to assign proxy access to parents, caregivers, and chosen representatives. While the process requires thoughtful development of policies based on legal considerations, providers need to make the process as simple as possible. The easier it is for patients and their proxies to understand and follow, the less likely it is that legal or administrative challenges will arise.

Providers must ensure that proxy access is supported by internal policies, workflows, and digital systems that are not only compliant, but also practical, patient-friendly, and inclusive of real-world caregiving dynamics. Where state law imposes additional requirements, institutions must harmonize them with HIPAA, taking care to ensure that any state standards do not impede the rights granted by HIPAA. As noted in previous sections, any right granted by federal laws takes precedence over state law. States can pass laws that strengthen a patient's rights beyond those granted by HIPAA, but they cannot lessen any rights granted by HIPAA or other federal data access rules.

Importantly, while the right to proxy access was first guaranteed through HIPAA, it also falls squarely within the scope of the **Information Blocking Rule** under the 21st Century Cures Act.

Covered entities must ensure their policies and systems do not delay, limit, or restrict proxy access in ways that would be considered information blocking. More specifically:

- Under **HIPAA's Right of Access** (45 CFR § 164.524), individuals may authorize others to receive or access their protected health information (PHI).
- Under the **Information Blocking Rule** (45 CFR Part 171), healthcare providers may not engage in practices that are likely to interfere with access, exchange, or use of electronic health information (EHI)—including by legally authorized proxies—unless a documented exception applies.

These rules mean that failure to **provide timely, reasonable access to a patient-designated proxy could constitute information blocking,** even if unintentional.

Access Limitations

In some cases, proxy access may be limited, depending on the patient's needs, expressed preferences, and legal requirements. These limitations may be based on different data classes, different time periods, or legal restrictions. Certain types of data, such as that related to mental health, substance abuse, and reproductive health, may have additional legal protections and requirements. Please ensure that your compliance officer clearly reviews your policy to ensure it is consistent with applicable state and federal law.

Key Provider Responsibilities

To comply with HIPAA and avoid information blocking, healthcare providers must:

1. **Honor Valid Proxy Requests with the Same Rights as Those for Patients** – Covered entities are required to provide individuals with access to their PHI or to direct access to a designated third party, including proxies or personal representatives.
2. **Avoid Unnecessary Barriers** – Do not require in-person requests, notarized forms, or proprietary processes, unless legally required. Accept electronic authorization (e.g., via email or portal). If the information is in electronic form, ensure your processes enable access in a timely manner. For printed or written records, process requests within the standard 30-day timeframe outlined by HIPAA.
3. **Ensure That Proxy Access Reflects the Same Scope as Patient Access** – Unless a patient specifies limitations, proxy access should include all available information, including electronic data via the patient portal or APIs.
4. **Provide Clear Workflows for Revocation** – Patients must have the ability to revoke proxy access at any time. Revocation processes should be clear, accessible, and ideally available through the same channels as the original request. Providers cannot charge per-page fees for records that are already stored electronically. If a patient requests electronic copies of their records, the provider can charge only for the actual labor costs of creating and sending the copies.

Please note: ***In situations where the state law provides individuals with greater rights*** of access to their health information than those outlined in the HIPAA Privacy Rule, ***the state law takes precedence.*** *(See 45 CFR 160.202 and 160.203).* Therefore, if your state prohibits charging fees to individuals who request copies of their health information, or if it sets fees lower than those required by the HIPAA Right of Access rule, providers must follow the state law. If, for any reason, state law permits higher fees than those outlined by HIPAA or restricts access in other ways, the provisions in the HIPAA Right of Access rule take precedence.

A detailed table is available in ***Appendix A***, listing all current state laws related to patient access fees and links to the corresponding laws. These laws and associated fees are accurate as of July 2025. However, state laws change frequently.Statute links change frequently. If the link is broken, you may search for the provided code number.

Recommendations for Implementors

- **Proxy Access Policy** – Include a proxy access policy in your Patient Data Resource Center that clearly explains the policy and distinguishes legal access rights from optional designations.
- **Proxy Authorization Form** – Provide a simple proxy authorization form that supports both written and electronic submission. While written submission should be an option, ensure that the proxy form can be submitted electronically through your website or directly through the patient portal, without the need for printing, faxing, notarizing, or any other potentially cumbersome process, unless required by law.
- **Role-Based Proxy Access** – When possible, configure EHR systems and portals to grant appropriate role-based access for proxies through the patient portal or an easily accessible web-based tool (e.g., parent vs. adult child).
- **Easy of Granting Proxy Access** – Make it easy for patients to grant proxy access. Use electronic forms or electronic methods for form submission and avoid cumbersome requirements for printing, signing, faxing, or notarizing forms.

Adolescent Health Data Access

Guidance for Implementors

One of the most complex areas of health information policy is navigating access to adolescent health data. While HIPAA establishes a national baseline, state laws often determine when and how parents or guardians can access an adolescent's health information—and when adolescents can limit that access. These variations affect what data can be shared through patient portals, what must be segmented, and how proxy access is configured.

In general, the medical records of a minor child under 12 can be accessed by the child's parent or legal guardian as the child's personal representative. The specific age at which parental access is limited can vary, with some states establishing different age cutoffs and creating exceptions for records related to mental health care, deferring to the adolescent and doctor's oversight.

Parental access is typically terminated once the patient reaches 18 years of age. When a child turns 18, the account is rolled over to an adult account. At that time, if the patient wishes to include their parent/guardian in their care, they will need to complete forms granting their parent proxy access to their data.

There are important considerations around parental access to an adolescent's medical records. A provider may exercise professional judgment in evaluating requests for access. Additionally, depending on the family's structure, a parent may be legally barred from accessing the adolescent's data.

How HIPAA Affects Access for Adolescents

Under HIPAA, a parent is typically considered the personal representative of a minor child and thus has the right to access their child's health information. However, HIPAA defers to state law in three important exceptions:

1. When state law allows minors to consent to their own care (e.g., reproductive health, mental health, or substance use services), and the minor has not requested the parent's involvement.
2. When the court or another law authorizes someone other than the parent to make healthcare decisions on behalf of a minor.
3. When a provider determines **that it is not in the best interest of the minor** to treat the parent as the personal representative, consistent with professional judgment and applicable law.

In practice, these laws can create significant implementation challenges for healthcare organizations—particularly when enabling portal-based or API access. Many EHRs are not configured to automatically **segregate sensitive adolescent data** (such as visit notes, lab results, or prescriptions) from general information. As a result, some providers either shut off proxy access altogether at a certain age (commonly 12–17) or restrict all adolescent portal access, both of which risk undermining care, trust, and legal rights.

To support access appropriately, healthcare organizations must:

1. Understand the **specific state laws** that apply to adolescent consent and confidentiality.
2. Align **policies, forms, and EHR configurations** with those legal requirements.
3. Train staff on how to **process proxy requests** for adolescents and how to navigate requests to restrict access.
4. Create mechanisms to **limit access to sensitive data elements** where required or requested.
5. Ensure that **compliance officers or legal counsel** review and approve final policies and procedures.

Recommendations for Implementors

- **Review state laws** on adolescent consent, confidentiality, and parental access, especially for services like reproductive health, mental health, and substance use.
- **Configure your EHR or portal system** to restrict proxy access to sensitive data for adolescents where required by law or upon adolescent request.
- **Develop clear internal policies** for adolescent access, proxy access, and situations where access must be limited based on state law or provider judgment.
- **Train frontline staff** and portal administrators on how to handle requests for access or restriction appropriately.
- **Provide adolescents with a way to request confidential care or restricted access,** including documentation that is secure, private, and accessible.
- **Work closely with your compliance officer or legal team** to ensure that your access policies are consistent with both HIPAA and applicable state law.
- **Clearly communicate your policy to patients and parents,** using language that is accessible and easy to understand in all relevant portals, forms, and web materials.

Patient Portal Access

Guidance for Implementors

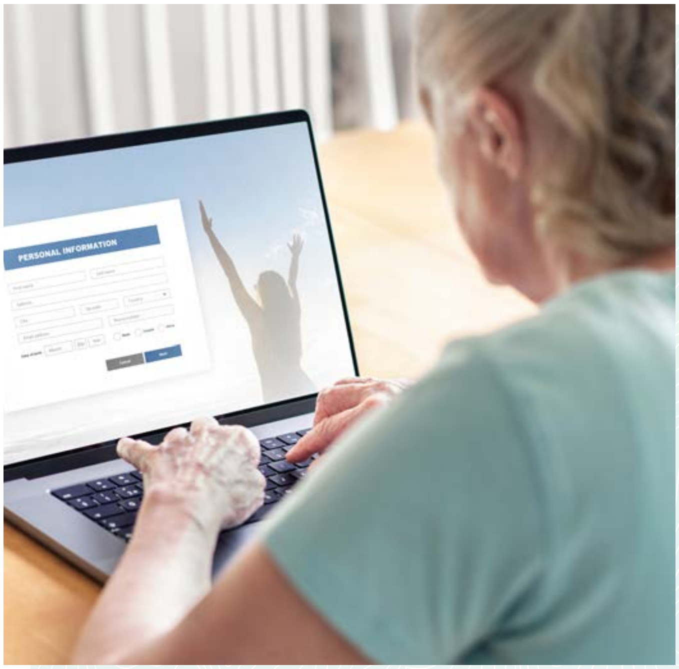
While patient portals are not required by any federal or state laws or regulations, patient portals have become the primary mechanism through which providers enable patients to access their electronic health data. Broadly speaking, most portals are developed and maintained by electronic health record companies. EHR vendors typically provide a patient portal system as part of their EHR implementation. Over time, the amount of data available through the portal has increased. Today, much of the data patients need is accessible through their patient portal.

Simplify Establishing a Portal Account

The easier it is for patients to readily access their portal, the better the data access process is, and the fewer demands are placed on providers' staff. While it's essential to verify that the person accessing the records is, in fact, the patient, it's equally important to ensure that accessing the portal is simple. The less administrative burden that providers create for patients to establish a portal account, the fewer demands that will be placed on providers' administrative staff. Additionally, patients often search for their data and attempt to access it after business hours when administrative support may be limited.

Clearly Define What Type of Data is Accessible Via the Portal

Even for patients accustomed to using portals or web-based tools, understanding which data is accessible via the portal can take some searching. What may seem obvious to those who design portal sites or practice administrators may seem complex to patients, especially when a patient is stressed, frightened, or overwhelmed.



Finding different classes of data, such as clinical notes and lab results, can be challenging, especially under stress. Therefore, your Patient Data Resource Center should clearly list the types of data accessible via the portal and either link to or direct patients to where that data can be found. For larger institutions, we recommend collaborating with your EHR vendor to help ensure the portal layout is easy to follow, allowing users to readily find the needed data.

Clearly Communicate the Date Range for Data that is Accessible in the Patient Portal

Most portals include only data generated after the provider implemented electronic health records. While most patients will only need access to their most recent medical records, in some cases, they will want to access all the data and records that your practice or institution has collected about them. These requests may encompass records generated before the widespread adoption of electronic health records. Knowing what is and is not accessible via the portal is important..

Recommendations for Implementors

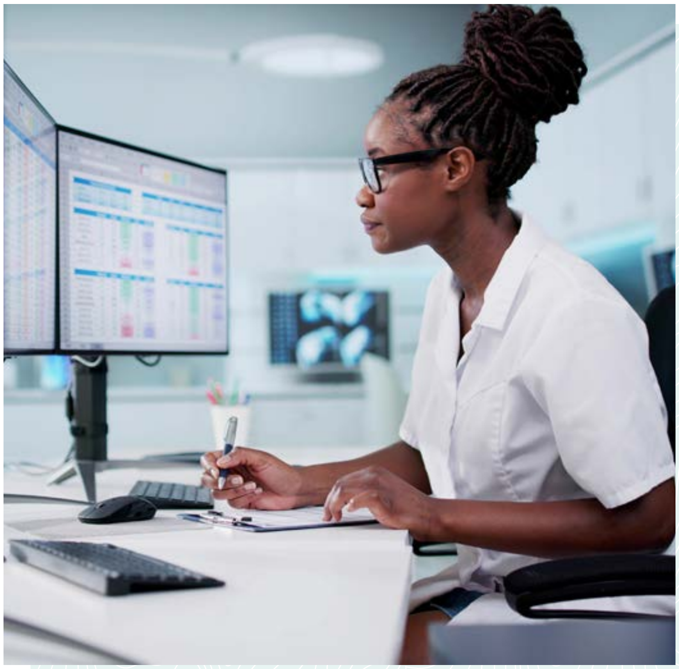
- **UX Design** – Use user experience design and testing methods to ensure patients can easily navigate your portal, accounting for limited functioning and problem-solving capacity when they need the data most urgently.
- **State Expected Time Frames** – Clearly state the time frame for data that is accessible via the patient portal.
- **Ease of Portal Setup** – Make it easy for patients to set up a portal account without needing to call or contact your office staff.
- **Data Accessibility List** – Clearly list the types of data accessible via the portal and indicate where that data can be found.

Historical Data Access

Guidance for Implementors

The number of years providers must maintain patient records varies by state. Many states dictate how long providers must keep patient records, specifying different time periods for different types of data. For data that is not electronic and is older than ten years, accessing it can be more complicated for both the patient and the provider. Please consult with your compliance officer to determine the specific requirements in the states where you operate and tailor your policy accordingly.

The specifics of your policy will be set by your compliance team. To ensure ease of understanding for patients, it's essential for providers to clearly state the policy and process and list any fees associated with accessing records that are not in the portal.



Fees for Access

The specific requirements and recommendations regarding fees are provided in the Data Fees section of this toolkit. However, some key points from that section are worth restating.

1. **Rationale** – If your organization chooses to charge fees, it's important to clearly explain the rationale and process for charging any fees for data access.
2. **Payment** – Ensure that fees for data access can be paid through an electronic method that accepts major credit and debit cards. Increasingly, consumers no longer write paper checks. Requiring patients to send in a paper check or cashier's check to get access to their records is cumbersome and adds to the patient's administrative burden. Electronic payments simplify the process.

Recommendations for Implementors

- **Clearly state the time range** for which records can be accessed electronically via the patient portal.
- For data that is not accessible via the portal, **clearly articulate the steps** to request historical data and records.
- **Provide a clear timeline for when patients can** expect to receive their data.
- **Clearly list any fees** associated with accessing historical data.
- Keep the process for requesting access to historical data **as simple as possible**, utilizing web-based request forms and digital payment methods. This simplicity decreases workload for both patients and provider staff.
- For patients who have difficulty submitting the request via online tools, **ensure that telephone support is available.**
- Consider offering an **urgent documentation process**, in case there is a rush need for records.

Medical Record Error Correction

Guidance for Implementors

Under the HIPAA Privacy Rule (45 CFR § 164.526), patients have the legal right to request an amendment to their medical records if they believe the information is inaccurate or incomplete. Healthcare providers (and other covered entities) must respond to such requests within 60 days, with a one-time extension of up to 30 days allowed if necessary. If the request is accepted, the provider must amend the record and make reasonable efforts to inform relevant parties of the correction.

What if the request is denied because the information wasn't created by the provider, is not part of the designated record set, or is deemed inaccurate and incomplete? In this case, the provider must send a timely written denial explaining the reason and informing the patient of their right to submit a statement of disagreement or request that their amendment request be included in future disclosures. All actions and communications related to amendment requests must be documented and retained for a minimum of six years.

Despite the clarity of the HIPAA rule, medical record errors remain a common source of frustration for patients when they receive their data. The reasons for this are many, but commonly include:

1. The complexity of the data.
2. The myriad processes through which data is entered.
3. The various purposes for which events and treatments are included.
4. The broad array of individuals who can enter and access patient data.

Errors are inevitable. The prevalence of errors has been well documented in numerous peer-reviewed, published studies. The number of patients who reported finding errors in their medical records varies across studies, but the most comprehensive research indicates that the rate of noticed errors is between 25 and 45 percent. In an era when data is exchanged between providers without the knowledge of the patient or the ability to confirm record details, it's easy to see how a simple data entry error could create a very real problem. Patients may be given inappropriate care or denied coverage due to a mistake.

Studies have shown that the majority of patients who discover errors want to report them, but few who attempt to do so actually succeed in getting the error corrected or noted on their record. When probed, patients cited confusion about how to report the errors and a lack of clarity about whether their request had been received and the status of the correction.

Given the prevalence of medical record errors and the potential for serious consequences for patients whose records contain inaccurate information, providers need to ensure that the process through which patients request corrections or additions to their records is straightforward and requires as little additional effort as possible. The most logical way to enable patient reporting of errors is through the patient portal. The patient should be able to flag the error through the portal and receive updates on the process there.

Recommendations for Implementors

- **Make it easy** for patients to report medical record errors by adding error-reporting functionality to the patient portal.
- Add a clearly visible **'Report an Error' button** to all sections of the patient portal that display medical records.
- Ensure the forms for submitting requests for correction can be completed **through the portal or the institutional website.** Avoid requiring patients to print, sign and submit the errors manually through fax or mail.
- Allow patients to **upload supporting documentation or comments** with their request.
- Design the correction request form to be **intuitive and straightforward,** with options to specify the error type, location in the record, and reason for correction.
- **Automatically confirm receipt of the request** with a timestamped message in the portal.
- **Provide updates on the status of the error review** through the patient portal, allowing patients to confirm the error was corrected or appended without additional effort or the need to contact administrative staff or medical records.

Implementation Toolkit:

Process & Integration

Making data accessible requires thinking through a range of complex processes in advance. Much of the work is conducted by the information management team, EHR vendors, and/or the information management vendors. However, some types of specialty and imaging data may be stored separately, requiring patient data access to fall within the responsibility of individual providers or their support staff.

Because responsibility for accessing different types of specialty data likely lies with various hospital offices, navigating the process for patients can be challenging, especially during times of stress and limited functional capacity. It's essential for providers and their vendors to consider the full range of processes in advance and envision the experience from the patient's perspective.

This section of the toolkit aims to help implementers proactively think through these processes. We will consider the context of all actions patients will be required to take to access their data.

Data Formats

Guidance for Implementors

Much of the data generated by patients is stored in standardized formats prescribed by regulators and/or adapted by informatics vendors. However, specialized datasets from medical devices, diagnostics, and imaging often use non-standard data formats or structures, requiring specialized software to read them.

In instances when data is stored in non-standard formats, it's essential for providers to consider potential uses patients might have and proactively address these issues in their communications.

For example, a patient who needs access to their imaging data may want the data for different uses. They may want to view the images on their computer or smartphone or upload the photos to a large language model (LLM) for analysis. That would require the data to be capable of being read or viewed by software that is native to those personal-use devices or readily available for download. In addition, some image and data types may not be viewable on standard software. However, a growing number of open-source, free, or low-cost tools are available for patients who want to view their image files. Providers may want to provide a list of tools patients can use to view the files, ensuring options that work on both PCs and Macs. If not, providers should provide patients with information on the specific type of file they are providing, so that patients can search for a tool with the appropriate capabilities.

The same patient may also want the images shared with another physician who has specialized software. In that case, it will be essential for that physician to have access to the original file structure, which contains the full data captured by the imaging software.

It's essential for providers and their vendors to consider the full range of processes in advance and envision the experience from the patient's perspective.

Because responsibility for accessing different types of specialty data likely lies with various hospital offices, navigating the process for patients can **be challenging.**

Recommendations for Implementors

Audit Your Devices — Conduct an audit of the various types of devices that your institution uses. Note the type of data that is generated by those devices. Identify how that data can be shared most effectively with the patient.

Develop Support Prompts — When patients request data from a specialty device, such as imaging or EEG, develop prompts to help them and staff determine the anticipated use of the data, so the data are shared in a format most likely to meet that patient's needs.

Create a Resource List — Consider developing a list of resources available for patients to view/read data in formats not readable by most home computers or smartphones/tablets.

Train Your Staff — Ensure that the staff most likely to interact with patients seeking specialty data are trained on the types of data available. In addition, help staff understand the questions they need to ask to provide patients with the necessary tools and information they need to access and use their data successfully.

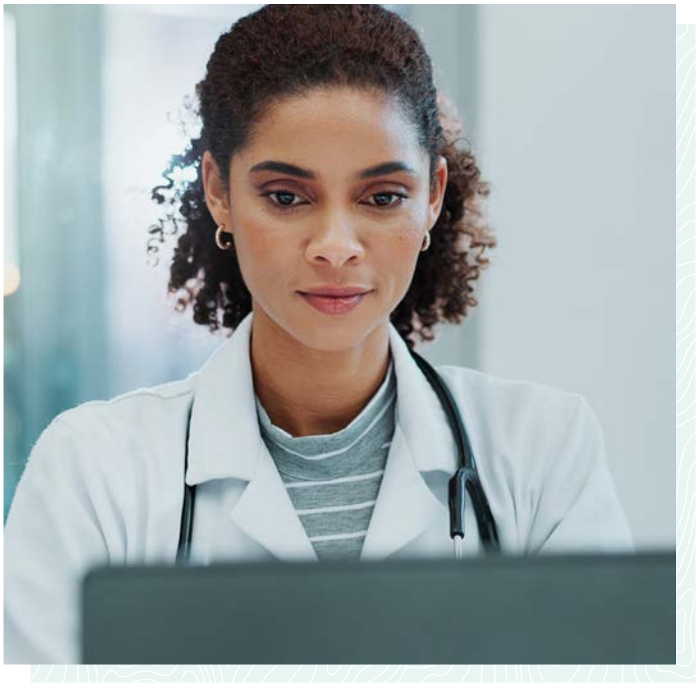
It's essential for providers and their vendors to consider the full range of processes in advance and envision the experience from the patient's perspective.

Data Transfer Options

Guidance for Implementors

In addition to thinking through the data format, it is important to consider the method of data transfer. Keep in mind that the patient wants the data presented in the most friction-free way possible.

Portal-Based Access – Although not yet required as part of ASTP's certification standards, EHR vendors increasingly are facilitating access to more complex forms of data, such as images, through patient portals. These portal-based image files can be viewed, downloaded, and then forwarded to physicians or members of the patient's care team. Since patients are increasingly accustomed to accessing data through their portal, sharing images through a known "workflow" would make it relatively easy for patients to access images on their own, without the need to contact the provider office staff or medical records to get access to their critical data. Adopting a portal-based image and data-sharing system would help alleviate the administrative burden and logistical challenges of accessing images and non-standard data. This process would reduce the workload for patients and staff.



Emailing Personal Health Information – In some cases, patients may prefer to receive their data through email. Under HIPAA, patients have the right to request that their data be provided by email, and providers must comply with this request as long as they ensure patients are aware of the privacy risks associated with sharing personal health information through unencrypted email. HIPAA makes no distinction regarding the types of data that can be emailed and imposes no requirements for additional written consent. However, providers who are federally supported substance use disorder treatment facilities have specific restrictions for emailing data related to substance use disorders. Additionally, some states have imposed restrictions on emailing certain types of data, such as data related to reproductive health, adolescent health, HIV/AIDS status, and genetics. While we discourage requiring a written consent form for email data transfer, providers must ensure patients are aware of the risks. We recommend that providers work with compliance officers to identify any data types the state restricts from email sharing.

Cloud-Based Image Sharing Platforms – A growing number of companies have emerged that specialize in providing cloud-based access to medical images. These services can provide low-friction methods for ensuring patients have access to their images when needed. Specific features vary among different service providers, but many offer options that would enable patients to access and view their data on their home computer, tablet, or smartphone. If choosing one of these options, ensure it is deployed in a way that does not create additional burden for patients, such as requiring them to download an app or create a new account. Also, ensure that the company's data use agreement is consistent with your practice or institution's data use practices. If the company's data use agreement is different, ensure that patients are properly informed and consent to any secondary data use in advance.

Document Sharing Platforms – Major document sharing platforms, such as Box, Dropbox, and others offered by Google and Microsoft, can serve as a secure method for sharing large data files that are not accessible via the patient portal. Most major commercial platforms offer HIPAA-compliant versions that providers can use to securely share data with patients. If providers choose this method, it's important to ensure that the log-in process does not introduce new, burdensome steps or requirements for patients, which could delay their access to their data. Not only would this increase patient frustration, but it could also result in a violation of the Information Blocking Rule.

Portable Storage Device – Large data files, such as image files, are often shared via portable storage devices, such as CDs or thumb drives. Increasingly, sharing data this way can be problematic for patients. Many modern computing devices lack a disc drive, so patients may not have the hardware to read data from a CD. Furthermore, thumb drives that use traditional USB-A ports are increasingly obsolete, since many computers now incorporate only USB-C ports. It's important to keep these and other trends in computer design in mind when determining the most effective way to present the data to your patients. Otherwise, you will inadvertently create an additional hurdle for patients who want to access and use their data.

In addition, if you choose to share data via a portable storage device, it's essential to consider where the device comes from. Providers would be wise to avoid connecting a patient-provided thumb drive or compact disc to their computer network. Instead, providers should consider purchasing an inventory of portable storage devices to provide patients with the data. That would ensure the device is clean and does not introduce any malware onto your computer network.

If choosing to provide the device, please ensure that any costs to the patient for the device are minimal and based on the device cost without any price markup or "convenience fees." Important considerations include:

1. Does your EHR vendor have the capability to add portal-based sharing of images and other non-standard forms of data? If so, does your practice/institution have access to that capability?
2. Can the data be emailed? HIPAA allows providers to email protected health information to patients if the patient requests it and is aware of limitations on secure emailing.
3. If you are emailing the data to the patient, is the file size likely to exceed the data limit of most email programs?
4. Could the data be shared via a cloud-based file-sharing system, such as Dropbox, Box, or other secure file-sharing sites?
5. Does the data need to be downloaded onto a portable storage device? If so, keep in mind that many home computers no longer have disc drives. Additionally, computers are increasingly using USB-C connections, rather than USB-A ports.
6. Who provides the portable storage device? Patient-provided devices may introduce security risks. How will this be handled? Providers may want to purchase the storage devices in advance and offer them to patients for a nominal fee to cover their costs. This process ensures that providers have control over potential security risks and makes it easier for patients who would likely need to purchase a portable storage device to access their data.
7. If the provider provides the storage device and charges the patient for the device's price, how will payment be collected and when?

Recommendations for Implementors

- Think through the data transfer process in advance, considering both the patient's needs and the limitations and demands on staff.
- Explore and adopt portal-based data access options for data types, including image files and other non-standard formats. Transferring data through well-established patient data access platforms decreases the need for additional problem-solving processes for both patients and staff.
- Consider purchasing a supply of data transfer devices, such as USB storage drives in USB-A/B and USB-C formats, and providing those to patients for a fee (if necessary), rather than asking patients to provide their own. This solution reduces patient workload and ensures the provider's computer system is not inadvertently exposed to viruses or malware.
- Ensure the cost of the data transfer/storage device is minimal and does not include any price markup. Clearly list the device cost in the Patient Data Resource Center section, along with any fee notifications for data access.
- Make it easy for patients to pay any fees for the data storage device via credit card or debit card through a web- or mobile-based interface.
- Explore using file-sharing platforms to share large files, taking care to ensure you select a platform that offers HIPAA-compliant capabilities.
- If using a file-sharing platform, ensure that the platform's use does not introduce any additional requirements for downloads, apps, or IDs that would make accessing the data more cumbersome for patients.
- Ensure staff most likely to interact with patients seeking specialty care are trained on data transfer options and processes. Additionally, help staff understand the questions they need to ask to ensure they provide patients with the necessary tools and information.
- Whenever possible, opt for data transfer processes that can be performed electronically by the patient outside standard business hours. The easier it is for patients to successfully navigate the process without contacting staff, the less burden is placed on staff who are already busy dealing with other urgent care matters.

Urgent Access Assistance

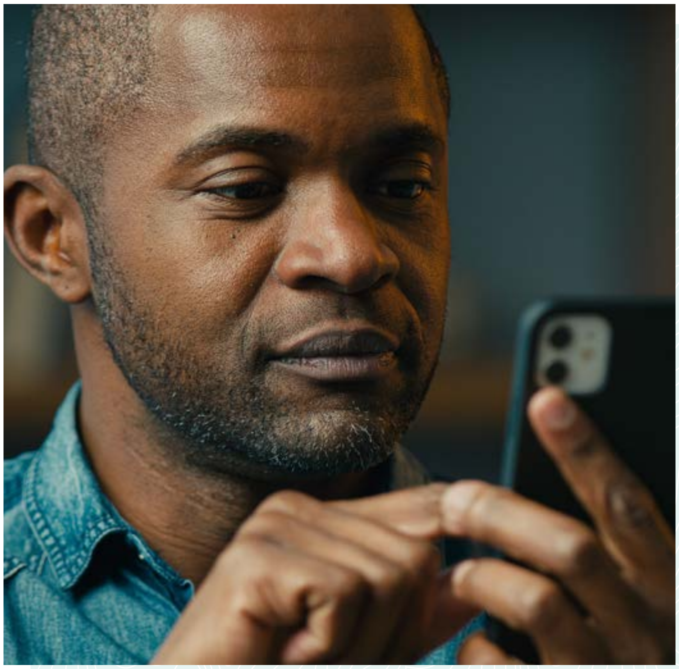
Guidance for Implementors

The 21st Century Cures Act and the Information Blocking Rule require providers to give patients timely access to any data stored in electronic format, especially when the need for the data is urgent or time-sensitive. Providers need a system that can assist patients facing a crisis, for which immediate access to their data is essential.

The best way to ensure patients in a crisis have access to their data in a timely manner is to make it possible for everything about data access to be “self-serve” – easy to understand and simple to execute at any time of day. Creating a comprehensive PDRC should help increase patient agency and decrease the need for patients to contact staff with questions. In most cases, that will be the easiest option for both patients and staff. However, in some cases, patients may be unable to complete the process online, either due to personal limitations or technical glitches. In such instances, it’s essential for providers to have a method in place for patients to receive urgent assistance with their data requests.

The volume and nature of urgent data needs and requests will vary considerably, depending on the type and volume of care that you provide. Therefore, the amount of resources available to support urgent requests will also vary.

Keep in mind that urgent health situations often occur after normal business hours, and for some patients, these issues may require access to their data. For providers with call centers, information hotlines, or nurse triage call centers, provide guidance to staff on how to handle and effectively support truly urgent patient data needs. Ensure staff are familiar with the tools available in the PDRC.



If your practice doesn’t have hotlines or triage centers, ensure that staff are trained to act quickly on urgent requests for data access when they receive them via voicemail or email contact. Regardless of your staffing level or resources, set clear expectations for when patients should expect an in-person call with assistance.

Recommendations for Implementors

- Ensure your Patient Data Resource Center provides “self-serve” access to patients who need their data urgently. Enable web-based methods for accessing data, signing any required forms, and making payments for fees (if any). The easier it is for patients to access their data without contacting your staff, the better it will be for both patients and your staff.
- Once established, conduct monthly checks of the Patient Data Resource Center to ensure all links and processes function smoothly.
- Collaborate with your team to identify the most effective process for providing phone-based support for facilitating truly urgent patient data access needs.
- Create data access scripts and guidance for call center or nurse triage staff who take patient calls after hours, providing the necessary tools they need to facilitate patient data access and answer any questions.
- Train staff to respond promptly to any voicemails or emails related to urgent data requests.
- Clearly set expectations for when patients requesting urgent data can expect a callback to support their request.

Implementation Toolkit:

Design Guidance

This section provides an overview of the information that patients need to understand how to access their health data successfully. Providing this information to patients in one, easy-to-find place not only makes it easier for patients, but also reduces the administrative burden on staff who would otherwise have to respond to requests.

Design Guidance

Guidance for Implementors

All good design begins with focusing on the user's needs and desires. For providers, the primary users of the Patient Data Resource Center (PDRC) will be your patients, their families, and loved ones. The technical sophistication, proficiency, and patient needs vary widely. However, even the most sophisticated users prefer a design that makes it easy to find and understand the information they need through easy-to-use interactions and tools. Keep in mind that the person seeking access to their health data is likely doing so amid a health issue or crisis for themselves or a loved one. Sorting through complex text, processes, or fine print will increase cognitive load and further frustrate them. With good design tools and a focus on user experience, your team can make it easier for patients who are stressed to get better care for themselves or their families.

Our primary goal is to ensure that patients can quickly and easily find and access their health data in the way that best suits them.

When designing the PDRC, keep these patient-centric principles in mind and ensure the following:

1. **Easy to Use:** Simple for everyone, no matter their technology skills or urgent needs.
2. **Clear Language:** Use everyday words, not medical jargon. Make it easy to understand.
3. **Accessible:** Ensure that the PDRC works for all users, including those with disabilities.
4. **Fast:** Help patients get information quickly, especially in emergencies.
5. **All-in-One Place:** Create a single place for all patient health information.

Every organization will have its own style guide and design for its web pages. The design of your Patient Data Resource Center should be aligned with your overall style and branding guidelines. This section provides guidance on using design tricks and tools to enable patients to quickly find the information they need and act in real time to access the necessary data.

To inform our guidance, members of The Sequoia Project Consumer Engagement Workgroup evaluated common home pages for healthcare organizations and identified the design elements that facilitate user success. Our workgroup members developed sample mockups for how these could be adapted and deployed by providers.

Recommendations for Implementors

Design Principles – Key Points

1. **Begin with the User in Mind** – All good user experience design begins with "user stories." Develop user stories based on the profiles of the patients who receive care at your practice or institution, and design the PDRC and each of its elements with those users' needs in mind.

2. **Stay Consistent** – Keep the same look and feel as your existing brand, ensuring the PDRC, while distinct, feels like a natural part of your website. Design consistency helps build and reinforce trust while reducing cognitive load for users trying to grasp complex information and navigate unfamiliar processes.

3. **Keep It Simple** – Important information should be clearly visible. The layout should be easy to understand, regardless of the user's experience, knowledge, language skills, or current concentration level.

4. **Make it Obvious** – People should be able to find information easily and always know their current position in the process. Buttons and menus should have clear labels so people know what they're doing.

5. **Be Forgiving** – Allow people to explore and interact with the site without fear of making a mistake. If someone makes a mistake, make it easy to correct or provide them with a clear way to back out.

6. **Provide Feedback** – Give visual cues to indicate where users are in the process and inform them of the next steps resulting from their actions. Give users enough time for their tasks and ensure they don't lose their work if time runs out or if they step away from their screen or navigate to a different page.

7. **Use Simple Language** – Make it easy to read and understand. Use words people know. Avoid acronyms or abbreviations when possible. Spell out the full names of departments or tools that have acronyms or abbreviations when used for the first time in written text.

8. **Make It Efficient** – Keep the number of words and steps to a minimum. Let people use the keyboard or mouse for interaction. Make it accessible to everyone, regardless of ability or background.

9. **Use Color Effectively** – Use colors consistently and deploy them to convey meaning and guide action, such as red for caution, green for success, and blue for progress, etc.

10. **Make It Readable** – Use white space to convey calmness and focus attention on critical elements. Make the font at least 12 point and ensure there is sufficient contrast between the text and the background to accommodate different color rendering among devices and to ensure users with decreased vision are able to read it. (Refer to WCAG 2.1 Success Criteria 1.4.3 Contrast (Minimum))

11. **Avoid Flashing or Moving Content** – If content moves or flashes, provide a readily apparent way for people to turn it off.

12. **Lighten the Cognitive Load** – Make instructions easy to find and follow. Try to prevent the need for users to ask, "How do I…?" or "Where is…?" Make help easy to search and use.

Note: For sample designs and examples of how to use visual design to feature your PDRC on your website's homepage, see ***Appendix A***.

Implementation Toolkit:

Training

This section provides an overview of the information that patients need to understand how to access their health data successfully. Providing this information to patients in one easy-to-find place not only makes it easier for patients but also reduces the administrative burden on staff who would otherwise have to respond to requests.

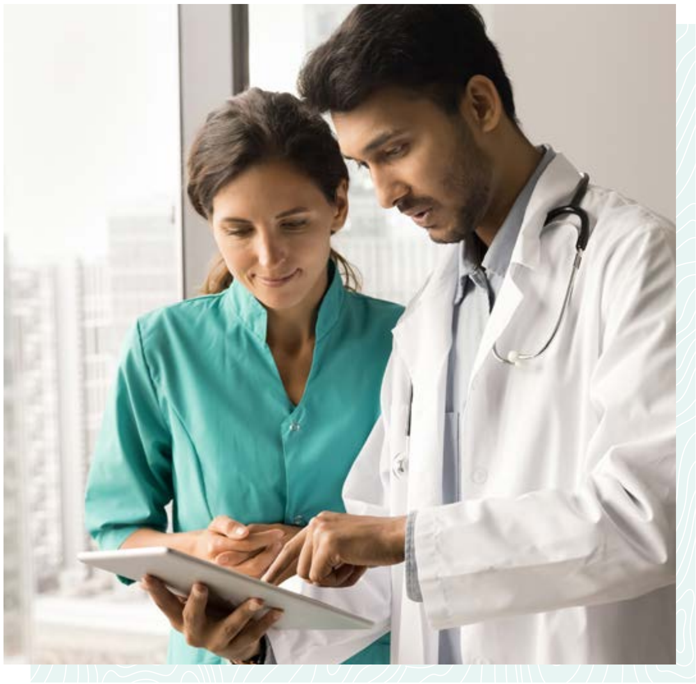
Staff Training

Guidance for Implementors

The rules and requirements for providing patients with timely access to their data are complex. Understanding which federal or state requirement takes precedence can be challenging for experts. For front-line and administrative staff at providers' offices, data access is one of many issues they must juggle, understand, and manage, all while serving the needs of their patients, supporting the providers in their practice, and maintaining the business of health. Taking the time to understand and sort through data access issues for a patient can be a time-consuming process if the systems aren't well designed and the office staff aren't informed about how to best support and troubleshoot any issues.

Ideally, by implementing a comprehensive, cohesive, and complete Patient Data Resource Center (PDRC), patients will be able to access their data directly, eliminating the need to engage with providers or their administrative staff. The more autonomy that you can deliver to patients to do "self-serve" data access, the better it will be for them, as well as your staff. This toolkit offers recommendations for how to approach and design processes to enhance efficiency for both patients and providers.

1. **Patient Data Access Rights** – Many healthcare workers and providers are aware of HIPAA. However, more recent and updated requirements, such as those established in the Information Blocking Rule, are not fully understood by many providers and their staff. While HIPAA data access rules require providers 30 days to provide patients with access to their data, the standard for the Information Blocking Rule is significantly different. Given that the Office of the Assistant Secretary for Technology Policy (ASTP) has announced an increase in enforcement of the Information Blocking Rule, training staff on its requirements will be critical – not only to support the needs of patients, but also to ensure compliance with the law.



2. **PDRC** – Once developed, it will be important for staff to consider the PDRC as the best "source of truth" for patients regarding all aspects of health data collection, use, and access. The more comprehensive and robust the PDRC, the easier it will be for patients to understand their rights, understand how their data is used, and access their data for personal use. Having said that, some patients will still need assistance from your staff. Ensuring your staff is familiar with the elements and capabilities of your PDRC is crucial.

3. **Portal Access Training** – As more data becomes available through patient portals, it's critical that all staff are aware of what is and is not available for patients to access through their portal. Ideally, signing up for, logging into, and navigating the portal should be simple, and the process should be facilitated through the PDRC. Your staff will need a basic understanding of the process and the tools available.

4. **Troubleshooting** – Even the best-designed website with self-serve form submission and payment will occasionally not work as needed. Staff will need to know where to refer patients in the event of any issues.
5. **Recognizing and Responding to Urgent Access Needs** – Training should instill a deep understanding that patients may urgently require their data. This goes beyond knowing how to process electronic requests; it involves recognizing the critical nature of a patient's need for their information. Training should cover how to prioritize and expedite data access for urgent requests, aligning the process with patient-centered care. This approach ensures that facilitating quick access to patient data is driven by empathy, moving beyond the technical steps to embrace the underlying reasons behind the urgency.

Requirements for Vendor Contracts

Guidance for Implementors

Through the Information Blocking Rule and its subsequent guidance, ASTP/ONC has been clear: any process that prevents or delays a patient's timely access to his/her electronic health information will be considered a violation of the Information Blocking Rule. To ensure compliance with the rule, it will be important for providers to incorporate training and other requirements into their contracts with information management vendors or EHR companies.

As listed in the Best Practices portion of this document, specific recommendations for contracts include:

1. Stipulating that vendors' employees must be trained and annually tested on current federal policies and requirements. This training should include the 21st Century Cures Act Final Rule, the Information Blocking Rule, and HIPAA.
2. Facilitating electronic access to patients' data for those who need it quickly and urgently, eliminating the need to call, print, fax, or mail any documentation to the records facility.
3. Enabling electronic submission of any forms required to access data, with consideration that patients have limited access to printers, faxes, and paper check writing.
4. Accepting electronic payment for fees through a web- or mobile-enabled payment system that works with major credit/debit cards.
5. Requiring health information management vendors to conduct user testing across a sampling of provider patients to ensure patients can readily access their data in a timely manner.

Empathy-Driven Communication and Proactive Support

Staff and vendor training should reflect understanding and empathy for patients needing quick access to their data. Building on the knowledge that patients often have limited access to printers, faxes, and paper check writing, training should focus on developing empathetic communication skills to proactively guide patients through electronic access.

This training should recommend providing clear, supportive, and patient-friendly instructions for utilizing electronic submission of any forms required to access data. This training should also recommend enabling the ability to accept electronic payment for fees through a web- or mobile-enabled payment system. Staff and vendors should be trained to anticipate and address potential difficulties patients might encounter with digital processes, ensuring that electronic access is as seamless and supportive of patient needs as possible. This approach aligns with the goal of ensuring patients "can readily access their data in a timely manner," as supported by the recommendation for user testing.

Implementation Toolkit:

Updates & Maintenance

This section provides guidance on establishing and maintaining a regular process to review, update, and validate all information related to patient data access that appears on provider websites, patient portals, and printed or printable materials. Having a consistent process ensures that patients always receive accurate, current, and complete information about their rights and the steps required to access their health data. It also helps providers remain compliant with evolving federal and state regulations while reducing confusion and administrative rework.

Maintaining Your PDRC

Guidance for Implementors

Providers must adopt a structured and recurring process for reviewing all patient-facing materials related to data access. This includes information published online, such as the Patient Data Resource Center (PDRC) and portal instructions, as well as printed materials distributed in offices or through discharge packets.

Regular reviews and updates are essential to maintaining compliance with federal policy and ensuring that staff and patients have accurate, up-to-date information. To maintain accuracy and trust, these materials should be reviewed on a routine schedule.

Providers should assign clear ownership for overseeing the review process. This responsibility can rest with a Data Access Oversight Team, which includes representatives from compliance, communications, IT/web services, and patient relations. A single individual should be designated as the accountable lead to ensure that updates are completed on schedule.

During each review cycle, providers should evaluate whether:

- Any federal or state laws affecting patient data access have changed (e.g., ASTP/ONC, CMS, HIPAA, Cures Act, TEFCA).
- Any technology or EHR vendor updates have altered the way patients access their data.
- Any internal workflows or staffing changes have affected the processes described in public-facing materials.
- Any links, forms, or downloadable content are outdated or non-functional.

Providers should document each update in a change log that records the date, description, and responsible party for the revision. This documentation ensures accountability and serves as a reference during compliance audits.

Finally, providers should ensure that any updates are communicated internally to staff and that online and printed materials are updated simultaneously to prevent inconsistencies. Patients should have access to the same information regardless of whether they view it online, download it, or receive it in printed form.

To improve responsiveness, providers should also offer a simple mechanism for patients to report broken links, outdated information, or accessibility issues, and ensure that these reports are promptly directed to the oversight team for correction.

Recommendations for Implementors

- **Establish a Review Schedule** – Develop a formal schedule to review and update all patient data access materials at least annually, and preferably every six months.
- **Assign Accountability** – Designate a data access oversight team and identify a single accountable lead to ensure reviews and updates are completed on time.
- **Monitor for Changes** – Track regulatory updates, EHR vendor changes, and internal workflow adjustments that may affect data access processes or patient instructions.
- **Maintain a Change Log** – Document all updates, including the date, description, and responsible party, to ensure transparency and traceability.
- **Synchronize Channels** – Ensure that updates made online are reflected in printed or downloadable materials to maintain consistency across all communication channels.
- **Communicate with Staff** – Notify all relevant staff of updates and ensure that training materials and scripts are revised accordingly.
- **Enable Patient Feedback** – Include a visible feedback option on websites and printed materials that allows patients to report errors or outdated information and assign clear responsibility for responding to these reports.

Implementation Toolkit:

Implementation Checklist

Implementation Checklist

Simplicity

Patient Data Resource Center (PDRC)

☐ Establish a central PDRC on the organization's website.

☐ Consolidate all data-related content into this single hub (data rights, privacy, portal, consent, exchange, etc.).

☐ Ensure the PDRC is clearly linked on the homepage with prominent buttons or banners.

☐ Confirm that content is structured around patient needs (not departmental silos).

Content Elements

☐ Data Access Rights & Process: Provide clear step-by-step instructions on how patients can request, view, and receive their data.

☐ Data Privacy Policies: Include a plain-language summary + link to full policies.

☐ Health Information Exchange: Explain how data is shared through HIEs, TEFCA, and private networks.

☐ Portal Access: Provide instructions for logging in, resetting passwords, and what information can be accessed.

☐ Mobile Access: List available apps, secure download links, and mobile access instructions.

☐ Patient Consent Management: Clearly explain opt-in/opt-out policies and how to control sensitive data sharing.

Design & Usability

☐ Test navigation with patients (especially those who are stressed or less tech-savvy).

☐ Prioritize clarity and simplicity over legal/ technical jargon.

☐ Use bullet points, action buttons, and plain language for key patient tasks.

☐ Ensure the PDRC is mobile-friendly, enabling easy reading, actions and links on a mobile device.

☐ Ensure the PDRC is ADA-compliant (usable on screen readers, accessible design).

Internal Processes

☐ Assign a cross-departmental ownership team (legal, IT, compliance, clinical) to maintain the PDRC.

☐ Set up a regular content review/update cycle (e.g., every 6–12 months).

☐ Establish a feedback channel (e.g., short survey, contact form) so patients can flag confusing or missing information.

Verification/Audit

☐ Conduct usability testing with real patients before launch.

☐ Perform an internal audit to confirm all required elements are included in the PDRC.

☐ Benchmark against peer institutions to ensure competitive and patient-friendly design.

Information Needs

Patient Data Rights

☐ Provide a plain-language overview of patient rights under the Information Blocking Rule, HIPAA, the 21st Century Cures Act, HTI-1 and HTI-2.

☐ Post this overview prominently in the Patient Data Resource Center (PDRC).

☐ Keep the explanation brief and straightforward, focused on patient rights, not legal complexity.

☐ Provide links or references to relevant laws and regulations for patients who want more details.

☐ Ensure internal staff are trained to explain rights to patients consistently.

Data Types and Access

☐ Create a comprehensive list of all electronic health information (EHI) your institution collects.

☐ Post this list in the PDRC so patients know what data types exist and how to access them.

☐ For each data type, provide instructions or links on how patients can request/access it.

☐ Confirm compliance with the Information Blocking Rule for all data classes.

☐ Conduct patient testing to confirm that the data type list is easy to understand.

Data Classes Checklist

☐ Clinical Notes
☐ Problem List
☐ Medication List
☐ Allergies and Adverse Reactions
☐ Laboratory Results
☐ Imaging and Diagnostic Reports
☐ Procedures
☐ Vital Signs
☐ Immunization Records
☐ Care Plans
☐ Encounters
☐ Behavioral Health & Substance Use Data (with exceptions noted)
☐ Social Determinants of Health (SDOH)
☐ Genomic & Molecular Data
☐ Device-Generated Data
☐ Longitudinal & Patient-Reported Data
☐ Palliative & End-of-Life Care Details
☐ Advanced Vital Signs & Continuous Monitoring Data
☐ Demographics
☐ Billing & Claims Data
☐ Care Team Information
☐ Legal & Administrative Documents
☐ Nutrition & Dietary Data
☐ Environmental & Occupational Health Data

Data Access Fees

☐ Decide whether your organization will waive fees or charge for data access requests.

☐ If charging, provide transparent explanations of what fees apply and why.

☐ Ensure all fees comply with HIPAA's cost-based standard (no "search and retrieval" fees).

☐ Verify compliance with state maximum fee laws while ensuring HIPAA preemption is respected.

☐ Offer at least one free copy per patient per year, if feasible.

☐ Enable online payment options (credit/debit cards, digital wallets, consistent with those used for service fees and co-pays).

☐ List any fees clearly in the PDRC so patients know what to expect.

Required Forms

- ☐ Review whether each required form is essential for data access.
- ☐ Keep forms simple—only collect required information.
- ☐ Accept written requests from patients even if not submitted via your official form.
- ☐ Provide digital submission options (portal, web-based forms, electronic signatures).
- ☐ Enable digital payment for fees within the form submission process.
- ☐ Consider using vetted AMA template forms.

Proxy Access

- ☐ Develop a clear proxy access policy and publish it in the PDRC.
- ☐ Provide a proxy authorization form that supports both paper and electronic submission.
- ☐ Avoid unnecessary barriers (e.g., notarization, in-person requirements) unless legally mandated.
- ☐ Configure EHR/portal to grant role-based access (e.g., parent vs. adult child).
- ☐ Allow revocation of proxy access through the same channels as authorization.
- ☐ Ensure compliance with HIPAA and the Information Blocking Rule.
- ☐ Train staff on handling proxy-related requests and limitations.

Adolescent Health Data Access

- ☐ Review and document state-specific laws on adolescent consent and confidentiality.
- ☐ Configure EHR/portal to segregate sensitive data (e.g., reproductive health, mental health, substance use).
- ☐ Develop policies for when parents can and cannot access data.
- ☐ Train staff on how to handle adolescent-specific requests.
- ☐ Provide adolescents with a mechanism to request restricted/confidential care.
- ☐ Communicate policies clearly to parents and adolescents.
- ☐ Involve compliance/legal counsel in final policy review.

Patient Portal Access

- ☐ Ensure easy account setup without requiring staff calls.
- ☐ Clearly list which data types are accessible via the portal.
- ☐ Use user experience testing to confirm patients can find data easily.
- ☐ State the time range of available portal data (e.g., post-EHR adoption only).
- ☐ Work with your EHR vendor to improve layout and data discoverability.

Historical Data Access

- ☐ Publish your institution's record retention policy (state-specific).
- ☐ Clearly state which records are accessible electronically vs. manual request.
- ☐ Define and publish a timeline for fulfilling historical data requests.
- ☐ Provide clear instructions for requesting historical data.
- ☐ Enable digital submission and payment for requests.
- ☐ Offer telephone support for patients unable to use online tools.
- ☐ Consider offering an urgent documentation process for time-sensitive needs.

Process & Integration

Data Formats

☐ Conduct an audit of devices used in your institution and identify the types of data they generate.

☐ Document which data formats are standardized vs. non-standard.

☐ For non-standard data formats, prepare clear patient instructions on how to access or use files.

☐ Provide patients with a list of open-source or low-cost tools to view specialty files (PC & Mac).

☐ Develop staff prompts/questions to determine how patients plan to use specialty data.

☐ Train frontline staff on specialty data formats, common patient needs and appropriate guidance.

☐ Ensure providers can supply original file structures when medically necessary.

Data Transfer Options

☐ Establish policies for emailing PHI in compliance with HIPAA.

☐ Review state-specific restrictions on emailing sensitive data.

☐ Evaluate cloud-based image sharing platforms; ensure HIPAA-compliant and patient-friendly.

☐ If using document sharing platforms, confirm HIPAA compliance and ease of access.

☐ Plan for portable storage devices: provide USB-C/USB-A options, avoid patient-supplied devices, and keep costs minimal.

☐ Allow simple electronic payments for device fees.

☐ Post data transfer options and costs clearly in the PDRC.

☐ Train staff on transfer options and patient support needs.

☐ Enable electronic/self-service transfers outside business hours when possible.

Urgent Access Assistance

☐ Configure the PDRC for self-service urgent access (forms, payments, downloads online).

☐ Conduct monthly checks of links, forms, and processes.

☐ Develop a phone-based support process for urgent data requests.

☐ Provide scripts and guidance for call center or triage staff.

☐ Train staff to respond promptly to urgent voicemails/emails.

☐ Set clear response time expectations for urgent data requests.

Design Guidance

User-Centered Design

☐ Develop user stories for patient populations and caregivers.
☐ Design the PDRC around these user stories and real-world needs.
☐ Test design elements with patients under stress or limited attention.

Consistency & Branding

☐ Ensure alignment with organizational style guide and branding.
☐ Maintain consistent look and feel across the website.
☐ Verify predictable and intuitive navigation.

Simplicity & Clarity

☐ Highlight critical information.
☐ Use clear labels for menus, buttons and navigation.
☐ Eliminate unnecessary text/steps.
☐ Use simple everyday language.

Forgiveness & Feedback

☐ Build error-tolerant processes with undo options.
☐ Provide progress indicators.
☐ Clearly inform users of next steps after each action.
☐ Allow sufficient time to complete actions without timeouts.

Accessibility

☐ Ensure ADA and WCAG 2.1 compliance.
☐ Use font size 12pt+ with strong contrast.
☐ Provide keyboard navigation.
☐ Avoid or disable flashing/moving elements.

Efficiency & Readability

☐ Keep instructions short and direct.
☐ Use white space to reduce clutter.
☐ Use color coding consistently.
☐ Optimize for speed and minimal clicks.

Support & Guidance

☐ Provide a help section with searchable FAQs.
☐ Include step-by-step instructions where needed.
☐ Conduct usability testing and gather patient feedback.

Training

Staff Training

☐ Provide training on HIPAA patient access rules (30-day standard).

☐ Provide training on Information Blocking Rule requirements.

☐ Ensure staff understand ASTP enforcement and compliance risks.

☐ Train staff to use and explain the Patient Data Resource Center.

☐ Provide portal access training.

☐ Establish troubleshooting protocols.

☐ Train staff to recognize and escalate urgent access needs.

☐ Incorporate empathy-driven training.

Requirements for Vendor Contracts

☐ Require vendor staff to be trained/tested on HIPAA, Cures Act, and Information Blocking Rule.

☐ Require vendors to enable electronic access without fax/print/mail.

☐ Ensure vendors support electronic form submission.

☐ Require vendors to enable electronic payment.

☐ Require vendors to conduct user testing with real patients.

Updates & Maintenance

Use this checklist to ensure your organization has a consistent, accountable process for keeping all patient-facing information about health data access accurate, up to date, and aligned across channels.

Establishing a Review Process

☐ A formal review and update schedule (at least annual, ideally semi-annual) is documented and approved.

☐ The schedule includes review of website content, printed materials, forms and patient portal guidance.

☐ Review dates are added to the organization's compliance or communication calendar.

Assigning Responsibility

☐ A data access oversight team (or equivalent group) has been formally designated.

☐ The team includes representatives from compliance, communications, IT/web services and patient relations.

☐ A single individual is identified as accountable for ensuring the update process is completed on schedule.

Monitoring for Changes

☐ There is a process for monitoring federal and state policy changes (e.g. ONC, CMS, HIPAA, Cures Act, TEFCA).

☐ There is a process for tracking EHR vendor or technology updates that impact patient data access.

☐ Internal workflow or staffing changes that affect patient access are flagged for website and materials review.

☐ A regular link and content audit identifies broken links, outdated forms or inaccessible content.

Documenting Revisions

☐ A change log is maintained with the date, description and responsible party for each update.

☐ Previous versions of materials are archived in compliance with record-keeping requirements.

☐ The oversight team reviews and approves all updates before publication.

Communicating Internally

☐ All staff are notified of updates to patient data access procedures or content.

☐ Training or refresher sessions are provided when substantive changes occur.

☐ Department leads confirm that all printed materials in circulation reflect the latest version.

Ensuring Consistency

☐ Online updates are reflected immediately in printable and distributed materials.

☐ All channels (website, portal, brochures, discharge packets) display the same information.

☐ Version control procedures are in place to prevent outdated materials from being used.

Patient Feedback

☐ A visible feedback mechanism allows patients to report broken links or outdated information.

☐ Reported issues are routed directly to the oversight team for timely resolution.

☐ Each issue report is tracked and documented until resolved.

Implementation Toolkit:

Appendices

Appendix A: Resources and References

State-Sanctioned Permissible Fees for Providing Patients with Access to Medical Records *(accurate as of July 2025)*

Alabama	Code of Alabama § 12-21-6.1 Albme.gov	$1 per page for the first 25 pages. • $.50 per page for each additional page. • The cost of shipping. • The cost to reproduce special records like X-rays. *Legislation introduced 04/09/2024 to remove the search fee and cap electronically produced records to $6.50 plus postage.
Alaska	Statute 18.23.005 akleg.gov	Alaska does not have specific medical record copying fees.
Arizona	Arizona Revised Statutes §12-2295 https://www.azleg.gov	A healthcare provider or contractor may charge a person who requests reproductions of medical records or payment records a reasonable fee, **except as necessary for continuity of care.**
Arkansas	Arkansas Code § 16-46-106 AR Medical Board	*The cost of each photocopy is:* • $.50 cents for the first 25 pages. • $.25 cents for each additional page. • A labor charge not exceeding $15 may be added for each request. • The actual cost of any required postage may also be charged.
California	California Health & Safety Code, Division 106, Chapter 1, § 123110 https://leginfo.legislature.ca.gov	All reasonable costs, not exceeding actual costs, incurred by a health care provider in providing copies pursuant to this subdivision may be charged to the patient or representative requesting the copies. • The fee from a health care provider shall not exceed $.25 per page for paper copies or $.50 per page for records that are copied from microfilm.
Colorado	Colorado Revised Statutes § 25-1-801 https://cdoc.colorado.gov – Incomplete; copy of the statute is not available on a link.	$18.53 for the first ten pages. • $.85 per page for the next thirty pages. • $.57 per page for each additional page; except if the medical records are stored on microfilm, $1.50 per page. • For radiographic studies, patients will need to pay actual reproduction costs for each copy of a radiograph. • Actual postage and electronic media costs, if applicable. • Applicable taxes.
Connecticut	Connecticut General Statutes § 20-7c(d) https://www.cga.ct.gov	No charge for supporting a claim due to the Social Security Act. • $.65 per page, including any research fees, handling fees or related costs and the cost of first-class postage, if applicable.
Delaware	Delaware Administrative Code, Title 24, Division 1700, § 16.0. https://dpr.delaware.gov	• Practices may require payment of all costs in advance of releasing the records, except for records related to an application for a disability benefits program. • $2.00 per page for pages 1-10. • $1.00 per page for pages 11-20. • $.90 per page for pages 21-60. • $0.50 per page for pages 61 and above. • Actual cost of postage or shipping. • Actual cost of items such as radiology films or fetal monitoring strips.
District of Columbia	D.C. Municipal Regulations § 17-4612.2 https://dchealth.dc.gov	A licensed physician may charge a reasonable fee for duplicating records, and the payment may be required before providing the records in non-emergency situations.

Florida	Florida Statutes, Title XXIX, Chapter 395, § 3025 Florida Administrative Code § 64B8-10.003 https://flrules.org	• The Board of Medicine urges physicians to provide their patients with a copy of their medical records, upon request, without cost. • The Board of Medicine may condition such release upon payment by the requesting party of the reasonable costs of reproducing the records. • For patients and governmental entities: - First 25 pages, the cost shall be $1.00 per page. - Page 26 to completion, $.25. - For other entities, the reasonable costs of reproducing copies of written or typed documents or reports shall not be more than $1.00 per page. • Reasonable costs of reproducing x-rays, and such other special kinds of records, shall be the actual costs. The phrase “actual costs” means the cost of the material and supplies used to duplicate the record, as well as the labor costs and overhead costs associated with such duplication.
Georgia	Official Georgia Code Annotated § 31-33-3, Georgia Dept of Community Health https://dch.georgia.gov	• $.97 per page for the first 20 pages. • $.83 per page for pages 21–100. • $.66 per page for pages in excess of 100. • Full reasonable cost of reproduction for records that are not in paper form, such as radiology films.
Guam	Department of Public Health and Social Services https://dphss.guam.gov/	May charge a reasonable fee. The link no longer directs users directly to the statement.
Hawaii	Hawaii Revised Statutes § 622-57(g) https://www.capitol.hawaii.gov	• If an attorney for a patient asks a health care provider for copies of the patient’s medical records and presents a proper authorization from the patient for the release of the information, the records shall be given to the attorney within a reasonable time not to exceed ten working days. • Reasonable costs.
Idaho	Idaho Code § 39-7301 https://legislature.idaho.gov	*Paper format:* • $.60 per page for the first forty pages. • $.36 per page for each additional page. • The actual reproduction costs of X-rays or other medical records that are difficult or expensive to duplicate. • The actual costs of postage. *Electronic format:* • $.30 per page for the first forty pages. • $.18 per page for each additional page. • The actual reproduction costs of x-rays or other medical records that are difficult or expensive to duplicate. • The actual costs of postage. • The entire fee charged pursuant to paragraph (b) of this subsection 9 shall not exceed $175, regardless of the number of pages provided or the original format of the original medical records.

llinois	Illinois Compiled Statutes, Chapter 735, § 5/8-2001(d) State of Illinois Comptroller https://illinoiscomptroller.gov	A healthcare facility or healthcare practitioner shall provide, without charge, one complete copy of a patient's records. • Pages 1-25 $1.34. • Pages 26-50 $.89. • 50+ $.45. • Copies made from microfiche or microfilm $2.23. • For electronic records, retrieved from a scanning, digital imaging, electronic information, or other digital format in an electronic document, a charge of 50% of the per-page charge for paper copies listed above. This per-page charge includes the cost of each CD-ROM, DVD, or other storage media. • The facility or healthcare practitioner may, however, charge for the reasonable cost of all duplication of record material or information that cannot routinely be copied or duplicated on a standard commercial photocopy machine, such as X-ray films or pictures.
Indiana	Indiana Administrative Code, Title 760, Article 1, Rule 71, § 3 – https://iar.iga.in.gov	*House Bill 1438 in the 2025 Legislative Session:* • $6.50 for producing a patient's medical record in electronic form. • Paper copies to $.05 per page. *Current Rules:* • $1.00 per page for the first ten pages. • $.50 per page for pages eleven through fifty. • $.25 per page for pages fifty-one and higher. • Actual cost of mailing. • May collect an additional $10 if the request is for copies to be provided within two (2) working days.
Iowa	Iowa Administrative Code §876.8.9 https://www.legis.iowa.gov	The amount to be paid for furnishing duplicates of records or reports shall be the actual expense to prepare duplicates, not to exceed: • $20 for 1 to 20 pages. • $20 plus $1 per page for 21 to 30 pages. • $30 plus $.50 per page for 31 to 100 pages. • $65 plus $.25 per page for 101 to 200 pages. • $90 plus $.10 per page for more than 200 pages. • The actual expense of postage.
Kansas	Kansas Statute 65-6836 Kansas Statute	• Reasonable cost of all duplications of health care record information that cannot be routinely duplicated on a standard photocopy machine.
Kentucky	Kentucky Revised Statutes § 422.317 https://apps.legislature.ky.gov	• 1st copy no charge. • 2nd copy $1.00 per page.
Louisiana	Louisiana Revised Statutes §40:1165.1 https://legis.la.gov	• $1.00 per page for the first twenty-five pages. • $.50 per page for twenty-six to three hundred fifty pages. • $.25 per page thereafter. • Actual postage. *Digital format:* • The charges for providing digital copies shall not exceed $100, plus all postage charges actually incurred.
Maine	Maine Revised Statutes, Title 22, Subtitle 2, Part 4, Chapter 401, § 1711-A https://legislature.maine.gov	*Paper format:* • The charge for the copies or the report may not exceed $5 for the first page and 45¢ for each additional page, up to a maximum of $250 for the entire treatment record or medical report. *Electronic format:* • Actual costs may not include a retrieval fee or the costs of new technology, maintenance of the electronic record system, data access or storage infrastructure. Charges assessed under this paragraph may not exceed $150.

Maryland	Code of Maryland, Health – General § 4-304(c)(3) https://health.maryland.gov	• $.50 per page • Actual postage cost
Massachusetts	Massachusetts General Laws, Chapter 111, § 70 https://www.mahima.org	• $28.69 base charge for clerical and other administrative expenses related to complying with the request for making a copy of the record (HIPAA requires this fee to be the actual cost, not standard) • $.96 for the first 100 pages • $.49 for each additional page *Massachusetts AHIMA recommends following HIPAA's $6.50 flat rate for electronic requests
Michigan	Michigan Compiled Laws § 333.26269 https://legislature.mi.gov	• Free for a medically indigent individual. • An initial fee of $20.00 per request for a copy of the record. (HIPAA requires this fee to be the actual cost, not the standard) • $1.00 per page for the first 20 pages. • $.50 per page for pages 21 through 50. • $.20 for pages 51 and over. • If the medical record is in some form or medium other than paper, the actual cost of preparing a duplicate. • Postage or shipping costs • Any actual costs incurred by the health care provider, health facility, or medical records company in retrieving medical records that are 7 years old or older and not maintained or accessible on-site.
Minnesota	Minnesota Statutes § 144.292, subdivision 6, paragraph (d) mn.gov	• When a patient requests a copy of the patient's record for purposes of reviewing current medical care, the provider must not charge a fee. • Free for appealing a denial of Social Security disability income or Social Security disability benefits under title II or title XVI of the Social Security Act when the patient is receiving public assistance, represented by an attorney on behalf of a civil legal services program, or represented by a volunteer attorney program based on indigency. *For other situations:* • For paper copies, $1 per page, plus $10 for time spent retrieving and copying the records (must be exact time per HIPAA) • A total of $30 for retrieving and reproducing x-rays. • For electronic copies, a total of $20 for retrieving the records. *Paper records:* • $30 for copies of records of up to 25 pages • $50 for copies of records of up to 100 pages • Plus an additional 20 cents per page for pages 101 and above; or • $500 for any request.

Missouri	Missouri Revised Statutes § 191.227. https://health.mo.gov	Fees Effective 2/1/25 Based on HB 351, the new maximum fees for copying will be: Paper-$29.47 plus $0.68 per page for the cost of labor and supplies for copies provided in paper form, and $27.59 for additional costs if records are maintained off-site. Electronic-based on HB 351, the new maximum fees for copying will be $29.47 plus $0.68 per page, or $129.16 total, whichever is less, for copies provided electronically.
Montana	Montana Code Annotated § 50-16-540 https://archive.legmt.gov	Reasonable fees allowed. A reasonable fee for providing health care information may not exceed 50 cents for each page for a paper copy or photocopy. (Admin fees not related to labor or actual costs not allowed by HIPAA)
Nebraska	Nebraska Revised Statute § 71-8405 https://nebraskalegislature.gov	(Admin fees not related to labor or actual costs not allowed by HIPAA) • $.50 per page as a copying fee. • A provider may charge for the reasonable cost of all duplications of medical records that cannot routinely be copied or duplicated on a standard photocopy machine. A provider may charge an amount necessary to cover the cost of labor and materials for furnishing a copy of an X-ray or similar special medical record. • A provider shall not charge a fee for medical records requested by a patient for use in supporting an application for disability or other benefits or assistance or an appeal relating to the denial of such benefits or assistance under: – Sections 43-501 to 43-536 regarding assistance for certain children. – The Medical Assistance Act relating to the medical assistance program. – Title II of the federal Social Security Act, as amended, 42 U.S.C. 401 et seq. – Title XVI of the federal Social Security Act, as amended, 42 U.S.C. 1382 et seq. – Title XVIII of the federal Social Security Act, as amended, 42 U.S.C. 1395 et seq.
Nevada	Nevada Revised Statutes § 629.061(5) https://www.leg.state.nv.us	• One free copy for records necessary to support a claim or appeal under any provision of the Social Security Act. • Actual cost of postage. • Not to exceed $.60 per page for photocopies. • Reasonable cost for copies of X-ray photographs and other health care records produced by similar processes. No administrative fee or additional service fee of any kind may be charged for furnishing such a copy.
New Hampshire	New Hampshire Revised Statutes, Title XXX, § 332-I:1 https://www.oplc.nh.gov	The charge for the copying of a patient's medical records shall not exceed: • $15 for the first 30 pages or $.50 per page, whichever is greater; provided that copies of filmed records such as radiograms, x-rays, and sonograms shall be copied at a reasonable cost.
New Jersey	New Jersey Administrative Code § 8:43G-15.3(d), § 13:35-6.5(c) https://www.nj.gov https://www.njconsumeraffairs.gov	*Hospital:* • $1.00 per page or $100.00 • $0.25 per page may be charged for pages in excess of the first 100 pages, up to a maximum of $200.00 for the entire record. • A postage charge of actual costs for mailing *Doctors:* • $1 per page or $100 for the entire record • $10 to cover shipping, postage, and retrieval costs • Cost of duplication for special records like X-rays.
New Mexico	New Mexico Administrative Code § 7.1.10.10 https://www.srca.nm.gov	A reasonable fee for copying and furnishing requested medical records may be charged by the health care provider. No health care provider shall charge more than: • $2.00 per page for the first 10 one-sided pages. • For each page after the first 10 one-sided pages, not more than $0.20.

New York	New York Public Health Law § 17 https://www.nysenate.gov	No charge may be imposed under this section for providing, releasing, or delivering medical records or copies of medical records where requested for the purpose of supporting an application, claim, or appeal for any government benefit or program. • Reasonable charge for paper copies shall not exceed $.75 cents per page.
North Carolina	North Carolina General Statutes § 90-411 https://www.ncleg.net	The maximum fee for each request shall be: • $.75 per page for the first 25 pages. • $.50 per page for pages 26 through 100. • $.25 for each page in excess of 100 pages. • The health care provider may impose a minimum fee of up to ten dollars ($10.00), inclusive of copying costs. If requested by the patient or the patient's designated representative, nothing herein shall limit a reasonable professional fee charged by a physician for reviewing and preparing a narrative summary of the patient's medical record.
North Dakota	North Dakota Century Code § 23-12-14.2 ND Century page 7	If either the patient or someone the patient authorized requests documents, the provider shall provide a free copy of a patient's health care records to a health care provider designated by the patient or the authorized person. This will only happen if the records are requested for the purpose of transferring that patient's health care to another health care provider for the continuation of treatment. Except as provided in subsection 1, upon the request for medical records or medical bills with the signed authorization of the patient, the health care provider shall provide medical records and any associated medical bills either in paper or facsimile format at a charge of: • $20.00 for the first twenty-five pages. • $.75 per page after twenty-five pages. Or in an electronic, digital, or other computerized format at a charge of: • $30.00 for the first twenty-five pages. • $.25 per page after twenty-five pages.
Ohio	Ohio Revised Code § 3701.741(C)(1)(e) https://codes.ohio.gov	Without charge when the request is necessary for: • The bureau of workers' compensation. • The industrial commission. • The Department of Medicaid or a county department of job and family services. • The attorney general. • A patient, the patient's personal representative, or authorized person if the medical record is necessary to support a claim under Title II or Title XVI of the "Social Security Act" if the request is for access to digital records or electronically transmitted records. In that case, the total cost for that access or for the electronic transmission, and all related services, shall not exceed $50.00. Except as provided in division (B)(2)(c) of this section, with respect to data recorded on paper or electronically, the following amounts are adjusted in accordance with section 3701.742 of the Revised Code: (i) $1.11 per page for the first ten pages (ii) $.57 per page for pages eleven through fifty (iii) $.23 per page for pages fifty-one and higher. (c) With respect to data resulting from an x-ray, magnetic resonance imaging (MRI), or computed axial tomography (CAT) scan and recorded on paper or film, $1.87 per page. (d) The actual cost of any related postage incurred by the health care provider or medical records company.

Oregon	Oregon Revised Statutes § 192.576 https://oregon.public.law	In the case of an individual appealing the denial of Social Security disability benefits, a covered entity shall upon request provide to the individual or the individual's personal representative, free of charge, one copy of the individual's health information created after the date that the individual alleged as the onset of disability in the individual's initial application for Social Security disability benefits and before the date of the administrative hearing. A covered entity may charge a fee for providing copies of health information, as provided in ORS 192.563 (Health care provider and state health plan charges), if: (a) The request for copies is made by a person other than the individual or the individual's personal representative; or (b) The covered entity has already provided to the individual or the individual's personal representative one copy of the information. [2015 c.360 §2; 2017 c.551 §1 Fees: • No more than $30.00 for copying 10 or fewer pages of written material. • No more than $.50 cents per page for pages 11 through 50. • No more than $.25 cents for each additional page.
Puerto Rico		No limit specified per last AMA update. Unable to find a valid, current source and government website does not open.
Rhode Island	https://health.ri.gov	When patients request copies of their own medical records, healthcare providers cannot charge a patient a retrieval or certifying fee for copying documents, and the physician cannot require a patient to pay any outstanding bills before retrieving and copying medical records. No fees can be charged for copies of immunization records that are required for school entry. No fees can be charged for copies of records that will be used to support a claim or an appeal for Social Security, medical assistance, Rite Care, Temporary Disability Insurance, unemployment compensation, or any other federal or state needs-based benefits program. No fees can be charged for copies of records that will be used in a civil court certification proceeding or for a Worker's Compensation claim. No fees can be charged for copies of medical records that are being sent to another consulting provider. X-rays and any other documents that cannot be reproduced by photocopy: The physician can charge the actual cost to reproduce the document, plus a reasonable fee of no more than $25.00.
South Carolina	South Carolina Code of Laws § 44-7-325 https://www.scstatehouse.gov	The Department of Health and Environmental Control is responsible for calculating this annual adjustment, which takes effect on July 1 of each year, starting with July 1, 2015. *Electronic format:* • The total charge to the requester may not exceed $150.00 per request, regardless of the number of records produced or the number of times the patient has been admitted to the health care facility. • The charge shall be calculated as follows: - $.65 per page for the first thirty pages. - $.50 per page for all other pages provided in an electronic format - Actual postage and applicable sales tax. *Paper requests:* • $.65 per page for the first thirty printed pages. • $.50 per page for all other printed pages. • Which, combined with the per-page print costs may not exceed two hundred dollars per admission to the healthcare facility. • Actual postage and applicable sales tax. • The facility or provider may charge a patient or the patient's representative no more than the actual cost of reproduction of an X-ray.

South Dakota	South Dakota 2023, ch 134, § 4. https://sdlegislature.gov	A health care provider or a medical records company may charge the following fees: *For a paper copy of a medical record not specified below, the fee may not exceed:* • $10.00 for the first ten pages. • $.33 for each additional page. *For an electronic copy of a medical record not specified below, the fee may not exceed:* • $.25 per page. For a printed copy of an x-ray, magnetic resonance imaging (MRI) scan, computerized tomography (CT) scan, or any other form of medical imaging, the fee may not exceed $10.00. For an x-ray, magnetic resonance imaging, computerized tomography scan, or any other form of medical imaging copied onto a compact disc, digital video disc, or other transportable electronic media, the fee may not exceed $15.00. Postage or shipping, plus any applicable taxes.
Tennessee	Tennessee Code Annotated § 63-2-102 https://www.capitol.tn.gov	*Paper format:* • $20.00 for medical records, 5 pages or fewer in length. • $.50 per page for each page copied after the first 5 page. • The actual cost of mailing the patient's records. *Electronic format:* • The provider may charge no more than a flat fee of $20.00 plus the actual cost of shipping if the records are shipped on portable media. • (Same cost as electronic for a response to Social Security or Disability)
Texas	Texas Health & Safety Code § 161.202 https://statutes.capitol.texas.gov	May not charge a fee for a medical record for use in supporting an application for disability benefits or other benefits, or an appeal relating to the denial of those benefits or assistance under: • The state Medicaid program. • The federal Social Security Act. A provider may charge a reasonable fee for other situations.
Vermont	Vermont Statutes Title 18, § 9419 https://legislature.vermont.gov/	No charge for providing copies of any health care record requested to support a claim or an appeal under any provision of the Social Security Act or for any other federal or State needs-based benefit or program. Other than above: No more than a flat $5.00 fee or no more than $0.50 per page, whichever is greater, for providing copies of an individual's health care record. A custodian shall provide an individual or the authorized recipient with an itemized bill for the charges assessed. A custodian may charge an individual a fee, reasonably related to the associated costs, for providing copies of X-rays, films, models, disks, tapes, or other health care record information maintained in other formats.
Virginia	Code of Virginia § 8.01-413 https://law.lis.virginia.gov	*Paper or hard copy format:* • Not to exceed $0.50 per page for up to 50 pages • $0.25 per page thereafter • $1.00 per page for hard copies from microfilm or other micrographic process (not allowed by HIPAA) • Postage and shipping costs. *Electronic format:* • Not to exceed $0.37 per page for up to 50 pages • $0.18 per page thereafter (not allowed by HIPAA) • Postage and shipping costs. The total amount charged to the requester for health records produced in electronic format pursuant to this subsection, including any postage and shipping costs shall not exceed $160 for any request made on or after July 1, 2021.

Washington	WAC Section 246-08-400 https://app.leg.wa.gov	Copying charge per page: • $1.24 per page for the first thirty pages • $.94 per page for all other pages
West Virginia	West Virginia Code § 16-29-2. https://code.wvlegislature.gov	A provider shall not impose a charge on an indigent person or his or her authorized representative if the medical records are necessary for the purpose of supporting a claim or appeal under any provisions of the Social Security Act. *Paper:* • $.40 cents per page • Postage, if the person requested that the records be mailed, plus any applicable taxes. *Electronic:* Unless the person requesting the record specifically requests a paper copy, the records will be delivered in electronic or digital form. • $.20 cents per page. In no event shall the amount exceed $150, inclusive of all fees. (Search and certification fees listed in the statute are not allowable by HIPAA)
Wisconsin	Wisconsin Department of Health https://www.dhs.wisconsin.gov	Note: If a patient or person authorized by the patient requests copies of the patient's health care records under this section for use in appealing a denial of social security disability insurance, under 42 USC 401 to 433, or supplemental security income, under 42 USC 1381 to 1385, the health care provider may charge the patient or person authorized by the patient no more than the amount that the federal social security administration reimburses the department for copies of patient health care records. As of 07/01/2024: *Paper Copies:* • First 25 pages = $1.40 • Pages 26 to 50 = $1.04 • Pages 51 to 100 = $0.68 • Pages 101 and above = $0.40 • Microfiche or Microfilm per page = $2.05 • Print of an X-ray per image = $13.78
Wyoming	No site located - Previous reference no longer available.	Reasonable fees - see HIPAA guidelines.

Data Access Fees References

References Used to Develop Guidance and Recommendations Related to Data Access Fees

American Medical Association. (2020). Patient Records Electronic Access Playbook. https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf. Referenced with permission from Jeff Coughlin of the American Medical Association on 03/18/25.

ASTP/ONC. (2018). https://www.healthit.gov/sites/default/files/2018-12/LeveragingHITtoPromotePatientAccess2.pdf

Health Information Privacy Division. (2024b, January 5). Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#maximumflatfee

Health Information Privacy Division. (2024, January 5). Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs

Leritz, A. D. (2022, April 2). Clarifying the HITECH Act and answers to frequent questions. Adler Giersch. https://www.adlergiersch.com/provider-blog/clarifying-hitech-act-answers-frequent-questions

Sample Forms

Several professional societies have developed sample forms that provider practices can use to facilitate patient data access requests. These forms were developed by these groups with input from a range of professionals and legal experts. They are a valuable resource for you. These include: AMA - AMA forms starting from page 91.

Below is a copy of the AMA form elements, which we recommend you use as templates for your institution. These elements can be built into your EHR portal and made available on your organization's website. Fillable form options should be considered to minimize the need for printing/scanning.

Patient Record Request Form Image:

PATIENT RECORD REQUEST FORM

You have the right to inspect and obtain a copy of your medical and billing records that we maintain. If you request copies of your records, we will notify you of any charge.

Patient Information: (Individual whose information will be released)

Name: (First, Middle, Last)
Date of Birth: (Month/Day/Year)

Address: (Street, City, State, Zip Code)

Description of requested records:

Records requested from: (Date) **to** (Date)

Please indicate whether you want to inspect your records or obtain a copy of your records:

☐ Inspect ☐ Obtain a copy on:
- ☐ CD
- ☐ USB Drive
- ☐ Paper records
- ☐ Secure message (will require a login)
- ☐ Unencrypted email (By choosing this option, you understand that there is a risk that the requested information could be viewed by an unauthorized person when transmitted over the internet)
- ☐ Other preferred form and format:

If you are requesting to obtain a copy:

☐ For pickup

☐ Mail to the following physical address:

Name

Street City State Zip Code

☐ Email or send secure message to the following email address:

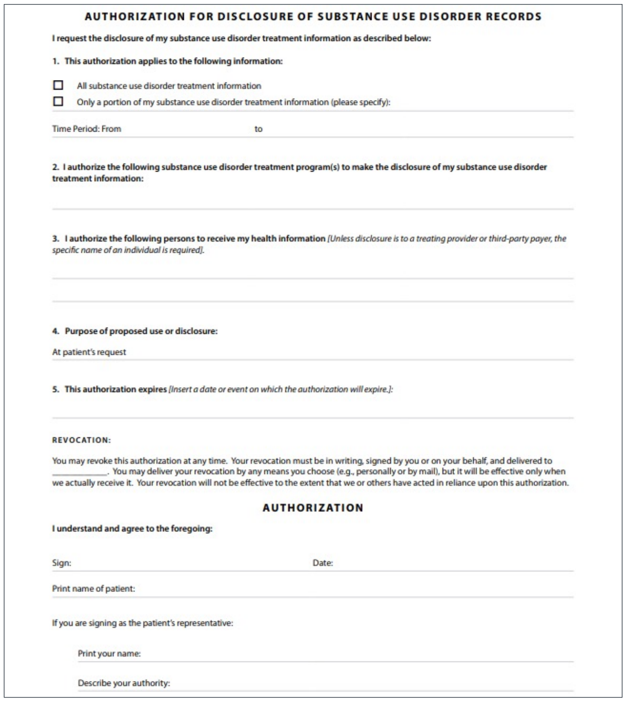
Print Name:

Relationship (if authorized representative of patient):

Signature: **Date:**

If you are an authorized representative (other than a parent of a minor child), you will need to provide documentation or an explanation of your authority to act for the patient (e.g., Health Care Power of Attorney).

Sample Form for Substance Use Disorder Information Governed by 42 C.F.R. Part 2 Image:



AUTHORIZATION FOR DISCLOSURE OF SUBSTANCE USE DISORDER RECORDS

I request the disclosure of my substance use disorder treatment information as described below:

1. This authorization applies to the following information:

☐ All substance use disorder treatment information
☐ Only a portion of my substance use disorder treatment information (please specify):

Time Period: From to

2. I authorize the following substance use disorder treatment program(s) to make the disclosure of my substance use disorder treatment information:

3. I authorize the following persons to receive my health information *[Unless disclosure is to a treating provider or third-party payer, the specific name of an individual is required].*

4. Purpose of proposed use or disclosure:

At patient's request

5. This authorization expires *[Insert a date or event on which the authorization will expire.]:*

REVOCATION:

You may revoke this authorization at any time. Your revocation must be in writing, signed by you or on your behalf, and delivered to ____________. You may deliver your revocation by any means you choose (e.g., personally or by mail), but it will be effective only when we actually receive it. Your revocation will not be effective to the extent that we or others have acted in reliance upon this authorization.

AUTHORIZATION

I understand and agree to the foregoing:

Sign: Date:

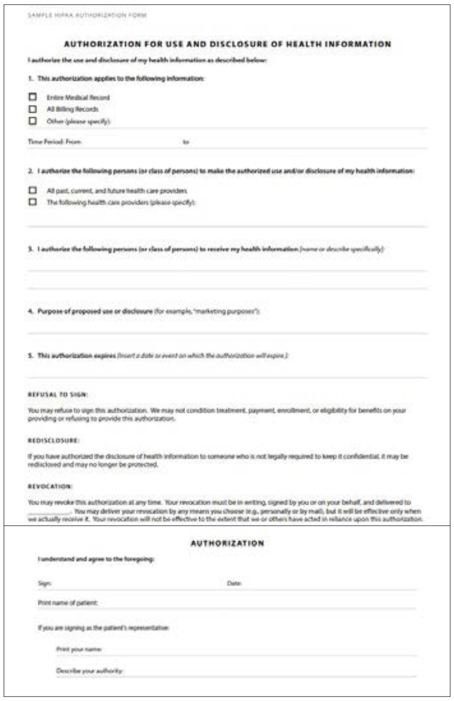
Print name of patient:

If you are signing as the patient's representative:

Print your name:

Describe your authority:

Sample Proxy Authorization Form Image:



SAMPLE HIPAA AUTHORIZATION FORM

AUTHORIZATION FOR USE AND DISCLOSURE OF HEALTH INFORMATION

I authorize the use and disclosure of my health information as described below:

1. This authorization applies to the following information:

☐ Entire Medical Record
☐ All Billing Records
☐ Other (please specify):

Time Period: From to

2. I authorize the following persons (or class of persons) to make the authorized use and/or disclosure of my health information:

☐ All past, current, and future health care providers
☐ The following health care providers (please specify):

3. I authorize the following persons (or class of persons) to receive my health information *(name or describe specifically):*

4. Purpose of proposed use or disclosure (for example, "marketing purposes"):

5. This authorization expires *[Insert a date or event on which the authorization will expire.]:*

REFUSAL TO SIGN:

You may refuse to sign this authorization. We may not condition treatment, payment, enrollment, or eligibility for benefits on your providing or refusing to provide this authorization.

REDISCLOSURE:

If you have authorized the disclosure of health information to someone who is not legally required to keep it confidential, it may be redisclosed and may no longer be protected.

REVOCATION:

You may revoke this authorization at any time. Your revocation must be in writing, signed by you or on your behalf, and delivered to ____________. You may deliver your revocation by any means you choose (e.g., personally or by mail), but it will be effective only when we actually receive it. Your revocation will not be effective to the extent that we or others have acted in reliance upon this authorization.

AUTHORIZATION

I understand and agree to the foregoing:

Sign: Date:

Print name of patient:

If you are signing as the patient's representative:

Print your name:

Describe your authority:

Adolescent Data Access Policies References

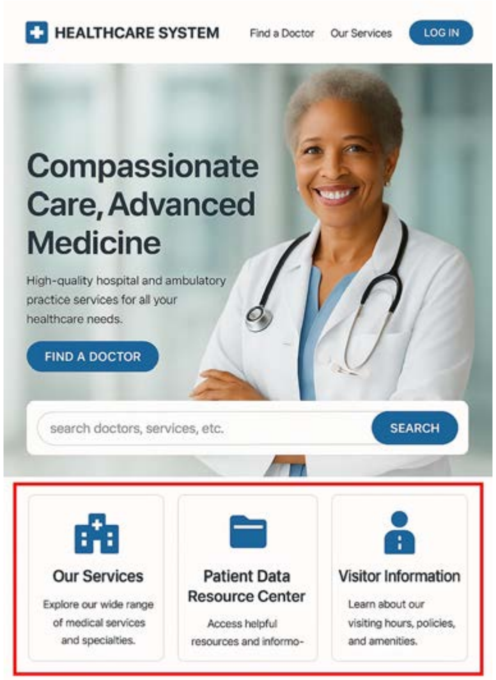
Resources and References for Adolescent Data Access Policies

- https://www.hhs.gov/hipaa/for-professionals/faq/personal-representatives-and-minors/index.html
- https://www.aap.org/en/practice-management/liability-and-regulation/health-insurance-portability-and-accountability-act-hipaa/parental-access-to-medical-records/
- https://kidshealth.org/en/teens/medical-records.html
- https://www.hhs.gov/sites/default/files/minors-hipaa-decision-tool.pdf
- https://thehipaaetool.com/parents-children-and-health-privacy/
- https://docs.legis.wisconsin.gov/misc/lc/issue_briefs/2024/health/ib_confidentiality_minors__health_records_eh_msk_2024_10_18
- https://newsroom.tricare.mil/News/TRICARE-News/Article/3714321/the-hipaa-privacy-rule-and-military-health-care-what-parents-of-minors-need-to
- https://www.hhs.gov/hipaa/for-professionals/faq/227/can-i-access-medical-record-if-i-have-power-of-attorney/index.html
- https://totalmedicalcompliance.com/hipaa-and-battling-parents/
- http://www.aclu.org/Files/OpenFile.cfm?id=12117&gt
- Privacy and Security Solutions for Interoperable Health Information Exchange Report on State Medical Record Access Laws: Appendix A8 Minors Overview
- https://www.healthit.gov/sites/default/files/appa8-1.pdf

Sample Designs

To help users find the Patient Data Resource Center, add a link to your home page using one of the following design elements in order of ease of discovery:

1. Large buttons (outlined in red box)



Compassionate Care, Advanced Medicine

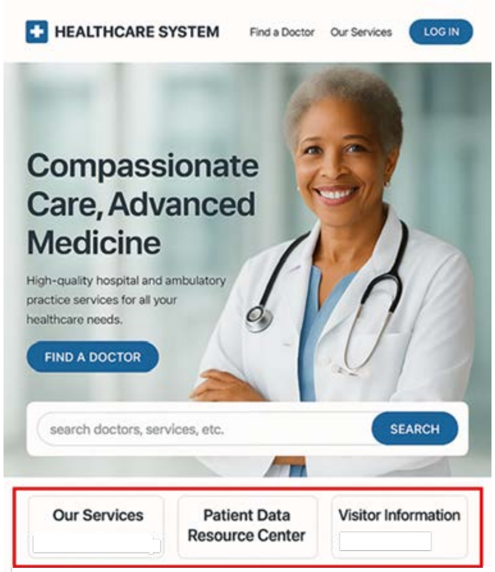
High-quality hospital and ambulatory practice services for all your healthcare needs.

Explore our wide range of medical services and specialties.

Access helpful resources and informo-

Learn about our visiting hours, policies, and amenities.

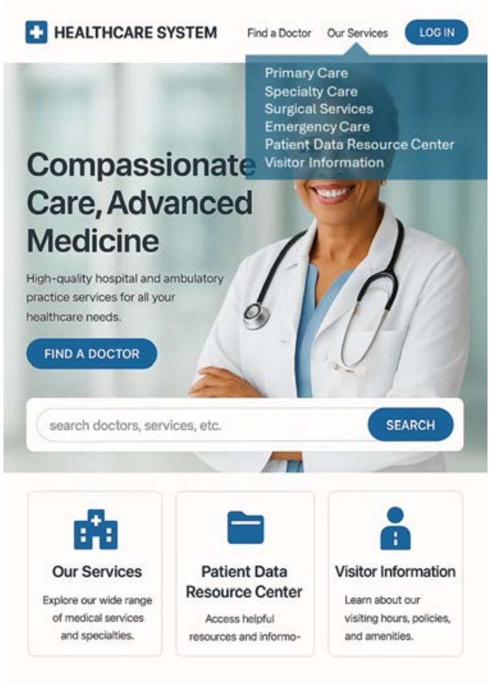
2. Small buttons (outlined in red box)



Compassionate Care, Advanced Medicine

High-quality hospital and ambulatory practice services for all your healthcare needs.

3. Menu (shown in green, expanded from the Our Services option)



Compassionate Care, Advanced Medicine

High-quality hospital and ambulatory practice services for all your healthcare needs.

Explore our wide range of medical services and specialties.

Access helpful resources and informo-

Learn about our visiting hours, policies, and amenities.

Now that patients have found the Patient Data Resource Center (PDRC), the all-in-one resource should also follow the same design principles. By creating a trustworthy, comprehensive tool for users to find, they will feel empowered to complete more actions on their own and direct them to the right place when they have follow-up needs.

Appendix B: Sample Text for Patients

Patient Data Access Rights – Sample Text

You Have a Right to Your Health Data!

Federal law gives you the right to see and get copies of your full medical record. It doesn't matter where your records are kept or what kind of system your doctor or hospital uses. If a doctor, hospital, or health plan has information about your care, such as test results, visit notes, or claims for payment, you have the right to get a copy.

If your records are electronic (digital), the process for getting them should be quick, easy, and often free or low-cost. If you need the records quickly and they're in digital form, your provider must provide them to you promptly.

What Laws Protect This Right?

Two federal laws give you this right:

1. The Health Insurance Portability and Accountability Act (HIPAA)
2. The 21st Century Cures Act

Both of these laws include rules requiring providers and health plans to allow patients to access their health records. A part of the Cures Act, known as the Information Blocking Rule, says clearly that patients must be allowed to obtain their digital health information without delay. These rules apply to most doctors, hospitals, labs, and pharmacies. HIPAA also applies to health plans.

What Records Can I Get?

You have the right to get records from any doctor, hospital, or other provider where you've received care. This includes:

- Records created during your visits.
- Records sent from other doctors.
- Health plan documents like claims and coverage decisions.

Here are some examples of the kinds of records you can get:

- Test results (like blood work or imaging).
- Notes written by your doctors or nurses.
- A list of your medications.
- Diagnoses (what you were treated for).
- Images like X-rays, MRIs, or CT scans.
- Insurance claims and explanations of benefits.

Are There Any Exceptions?

Yes, but they are rare. A provider may deny your request if they believe seeing your record could cause serious harm to you or to someone else mentioned in the record (like a family member). If this happens, they must explain why. You also have the right to ask them to reconsider the decision.

What About Older Records?

Doctors and health plans don't have to keep your records forever. Some old records may no longer be available. For example, records from when you were a child may no longer be kept once you reach adulthood (depending on your state's laws).

That's why it's smart to ask for and save copies of your records after each visit or hospital stay, so that you can build your own full history of care.

Types of Data and How to Get Them

During your care, we collect and create different kinds of health data. What we have depends on your visits, test results, and other information we've received.

Your PDRC includes a list of the types of data we may have about you, along with instructions on how to get them. If you're looking for a specific type of record and don't see it listed, please contact [insert contact name here].

About the Sequoia Project

The Sequoia Project is a non-profit, 501c3, public-private collaborative chartered to advance implementation of secure, interoperable nationwide health information exchange. The Sequoia Project focuses on solving real-world interoperability challenges and brings together public and private stakeholders in forums, such as the Interoperability Matters cooperative, to overcome barriers. The Sequoia Project is the Recognized Coordinating Entity® (RCE®) for the Office of the National Coordinator for Health IT's Trusted Exchange Framework and Common Agreement (TEFCA). In this role, The Sequoia Project developed and will implement and maintain TEFCA's Common Agreement component and operationalize the Qualified Health Information Network® (QHIN™) designation and monitoring process.

Acknowledgments

Many individuals contributed to the development of this guidance. We are thankful to everyone who participated in our regular calls, contributing to robust and thoughtful discussions of this complex topic. We are especially grateful to those who volunteered their time to draft the group's ideas into this paper. Lead authors and contributors are **bolded** in the Consumer Engagement Workgroup roster below. Additionally, we'd like to thank the staff at The Sequoia Project for their support, particularly Bren Shipley, Amber Nava, and Sadie Andersen.

Workgroup Co-Chairs

Anna McCollister,
Brian Van Wyck
Cathriona Dolphin-Dempsey

Workgroup Members

Henry Archibong, *HealthMark Group*
Allison Aubuchon, *WellConnector*
James Bateman, *Marble*
Jennifer Blumenthal, *OneRecord*
Whitney Bowman-Zatzkin, *Rare Dots*
Stephanie Broderick, *Clinical Architecture*
Hans Buitendijk, *Oracle Corp*
Hugo Campos, *Consultant/Patient Advocate*
Bart Carlson, *Azuba Corporation*
Barbara Carr, *Verisma*
Dan Chavez, *Serving Communities HIO*
Grace Cordovano, *Enlightening Results*
David Corso, *Azuba Corporation*
Jeff Coughlin, *American Medical Association*
Tammy Coutts, *EHRA*
James Cummings, *Consumer/Patient Advocate*
Dave deBronkart, *Consumer/Patient Advocate*
Cathriona Dolphin-Dempsey, *Stanford Health Care*
Carole Gammarino, *MRO Corporation*
Vicki Giatzikis, *New York Presbyterian*
Eddie Gonzalez-Loumiet, *Ruvos*
Katie Goulette, *Michigan Health Information Network*
Mike Graglia, *Cure SynGAP1*
Thomas Grannan, *Azuba Corporation*
Leigh Hanes, *Retired*
Joseph Hernandez, *BluIP*
Gena Jarosch, *Michigan Health Information Network*
Chris Jones, *MatchRite*
Nabbil Khan, *Lifeline Biosciences*
Katy Knowlin, *Solverein*
Shannah Koss, *Koss on Care LLC*
Allison Kozee, *MRO Corporation*
Jason Kulatunga, *FastenHealth*
Amy Laine, *Sandwych*
Virginia Lorenzi, *Consumer/Patient Advocate*
Tushar Malhotra, *eClinicalWorks*
Shamekka Marty, *The Marty Firm LLC*
Josh Mast, *Oracle Corp*
Elizabeth McElhiney, *Verisma*
Chrissa McFarlane, *Patientory*
Deven McGraw, *Citizen Health*
Lana Moriarty, *ASTP*
Leslie Nance, *Humana*
Tiffany O'Donnell, *MRO Corporation*
Adaeze Okonkwo, *Government of DC*
Melis Ozturk, *IBM*
Eric Pan, *Stoa Medical*
Josh Parker, *AthenaHealth*
AJ Peterson, *Netsmart*
Aileen Rowan, *Oliver Wyman*
Brandi Ryan-Cabot, *Contexture*
Paul Seville, *Deloitte*
Alexis Shaner, *Hawai'i Pacific Health*
Sachin Sharma, *JHCP*
Stacey Tinianov, *Consumer/Patient Advocate*
Jaffer Traish, *FindHelp*
Janice Tufte, *Hassanah Consulting*
Brian Van Wyk, *Epic*
Vanessa Vogel-Farley, *Global Genes*
Diana Warner, *MRO Corporation*
Duncan Weatherston, *Smile Digital Health*
Carol Zindler, *inTandem Health*

Interoperability MATTERS

Consumer Engagement Workgroup

the sequoia project