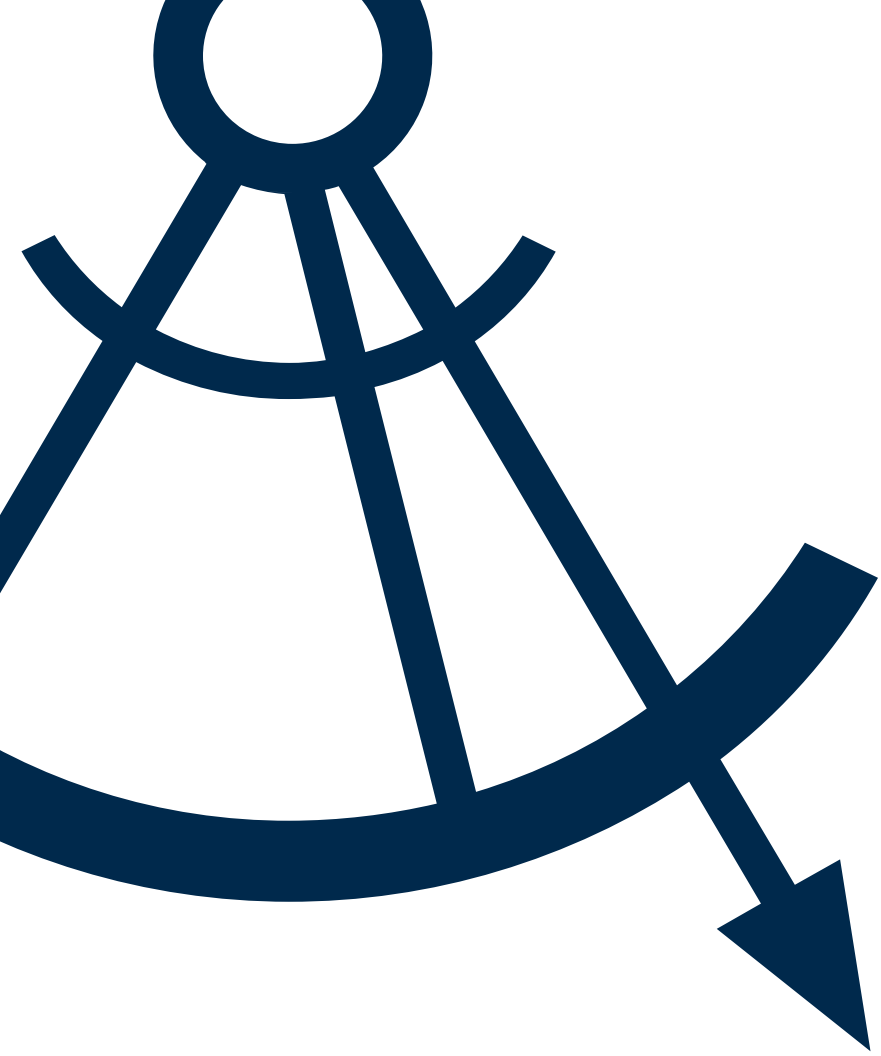


What Providers Need to Know:

Cures Act Compliance and Strategic Connected for Health Opportunities

THE CHARTIS GROUP

TABLE OF CONTENTS

CHAPTER 1

Interoperability Deadlines Are Here: Are You Prepared?

70%

of CIOs indicate they are concerned about being ready to meet the original compliance deadlines.

Since the onset of the pandemic, healthcare executives have been leading through the crisis to deliver more, faster — with fewer operating, capital and human resources.

With an already-full agenda, executives are faced with looming interoperability compliance deadlines, beginning in early 2021 spanning through 2023. Given competing demands and time, many are questioning whether to address new requirements now or wait until further clarity on penalties are published by the Office of the Inspector General (OIG).

Taking action now is essential. Those who do not meet deadlines risk near-term public reporting exposure, and substantial penalties still stand, even though enforcement has been pushed out in recognition of the COVID-19 impact. Moreover, waiting means a missed opportunity to leverage the effort to achieve broader IT and organizational goals.

In this first chapter aimed to help healthcare executives take a strategic approach to compliance, we explore the rules, timelines and provider responsibilities.

"There's growing concern that health systems are falling behind in addressing requirements. The level of effort is sizable, complex and enterprise-wide."

The Impact and Risk of Noncompliance

The rules were released March 9, 2020 amidst the outset of the pandemic and became effective June 30, 2020, with compliance deadlines beginning early 2021. Noncompliance will impact quality payment incentives and include public reporting — which some liken to the Department of Health and Human Services (HHS)'s cybersecurity "Wall of Shame." For providers promoting apps or working on an extension of their EHRs, they may be considered a developer, with penalties as high as $1M per violation.

There's growing concern that health systems are falling behind in addressing requirements. The level of effort over the coming months will be sizable and enterprise-wide. It will require a mindset shift from protected health information (PHI) to electronic health information (EHI) and complex process, policy and technology changes. In fact, in a June CHIME survey, 70 percent of CIOs indicated that they were concerned their organizations wouldn't be able to address the steps required by the original November 2 compliance deadlines.[1] Another 7 percent noted they hadn't had time, given the demands of COVID-19 response and recovery, to figure out how to respond as an organization. Based on our conversations with executives across the country, we suspect that an even higher portion of organizations may be challenged to meet requirements.

The Rules at a High Level

In the two highly anticipated rules, HHS laid out a vision where a patient's health information can move seamlessly between health plans and providers and where every American can see and use EHI through common technologies such as smart phones, home computers, laptops and tablets. Key components of the Cures Act interoperability rules are summarized in Figure 1. The ONC released one set of components; concurrently, CMS released a complementary set of rules and components. Together, they form the basis for the interoperability rules.

Figure 1: Cures Act Interoperability Rules and Key Components

ONC CURES ACT

On March 9, 2020, ONC within HHS released a 1,244-page **federal** final rule on interoperability, information blocking and the health information technology certification program.

ONC CURES ACT COMPONENTS

PROVIDERS, HIE/HINs & DEVELOPERS

- Information Blocking
- Conditions of Health IT Certification

CMS-9115-F

Concurrently, CMS released a 474-page final rule to **support the Cures Act,** designed to help patients access their complete health information in interoperable forms across the programs that CMS administers.

CMS RULE COMPONENTS

PROVIDERS

- Attestation and Public Reporting
- ADT Event Notifications
- Digital Contact Information (NPPES)

HIE/HINs & DEVELOPERS

- Patient Access API
- Provider Directory API
- Payor to Payor Data Exchange
- Dually Eligible Experience Improvement
- Patient Education

What's the Provider Effort, and Why Is This Time-Sensitive?

The rules include aggressive timeframes for compliance with the information blocking, digital contact information, and attestation and reporting components of the regulations with additional rolling compliance deadlines through the end of 2023 that will affect providers for years to come.

Chartis has identified five provider responsibilities for compliance with the ONC and CMS interoperability rules, shown in Figure 2.

Figure 2: Provider Responsibilities and Compliance Timeframes

ONC and CMS rules present a **dramatic shift in mindset** from treating patient data as a confidential asset that should be **closely guarded** and secured to one in which patient data must be **shared openly** when appropriately authorized by the patient.

	URGENCY	PROVIDER EFFORT
March 31, 2021 **ATTESTATION & PUBLIC REPORTING** Enhance tracking and attestations around information blocking.	●	●
March 31, 2021 **DIGITAL CONTACT INFORMATION** Update and use national provider contact information.	●	●
APRIL 5, 2021 **INFORMATION BLOCKING** Refine workflows and policies to ensure information is not blocked, with eight exceptions permitted.	●	●
MAY 1, 2021 **ADT NOTIFICATIONS** Expand workflows to support notification of admit, discharge or transfer to community providers.	●	●
DECEMBER 31, 2022 **CERTIFICATION OF ELECTRONIC HEALTH RECORD TECHNOLOGY (CEHRT)** Recommended to ensure your EHR vendors are certified and configured to support compliance.	●	●

Below are the deadlines, implications and key considerations for each of the five provider responsibilities.

Information Blocking

April 5, 2021

Implications

Providers must share EHI with patients, community providers, HIEs and other actors securely with patient authorization (first United States Core Data for Interoperability .[USCDI] data by April 5, 2021, then all EHI by October 6, 2022).

Key Considerations and Actions Required

This represents a dramatic shift in data management, from guarding to open access for patients and authorized third parties. Not only are technical changes required; material operational changes will be required to respond to data requests, including updating HIPAA, other business agreements and policies, and new processes and clinical workflows to ensure that the necessary data is available, accessible and provided in a timely manner in the method requested. This necessitates a comprehensive change management and operational readiness program. Plus, since EHR developers are not required to implement functionality for USCDI now, providers will need to develop their own request response workflows to include all USCDI items. Use case analysis outlining the various operationally impacted workflows will be critical.

Digital Contact Information Updates

March 31, 2021

Implications

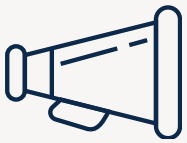
Health systems must ensure their providers' digital contact information is up to date in the National Plan and Provider Enumeration System (NPPES) database — the CMS provider digital contact information database — and have an ongoing maintenance program.

Key Considerations and Actions Required

The effort may be large as current noncompliance is high. Providers must complete updates themselves or delegate access, and contact information like DirectTrust address is not always known by the provider. Bulk uploads are possible but require setup and accurate contact information.

Attestation and Public Reporting

March 31, 2021



Implications

Health systems continue to submit quarterly attestations for CMS Quality Program (Promoting Interoperability) incentives indicating they are not information blocking, but now these blocking attestations will be reported.

Key Considerations and Actions Required

A structured process to track data requests and responses is needed to support the attestation responses. Information blocked by a provider will be publicly reported on the CMS Care Compare site and incur penalties, expected to be disincentives.

ADT Notifications to Providers for Patient Moves

May 1, 2021

Implications

Health systems must notify community providers on patients' primary care teams and post-acute care providers of any admission, discharge or transfer (ADT) — not just the Primary Care Provider (PCP) or referring providers, as is common practice.

Key Considerations and Actions Required

Automating notifications may create alarming new levels of "alert fatigue" which will need to be addressed early on. Enterprise notification services, with Customer Relationship Management embedded, can prevent this and improve satisfaction. Care team providers and post-acute care providers will need to be correctly updated in EHRs from potentially multiple provider databases. CIOs need to know what data is going to whom now and through what route in order to identify those primary care team providers and post-acute care providers who are not already receiving the notification via HIE, interface, DirectTrust, fax server or other route.

Certification of EHR Vendor Technology (CEHRT)

December 31, 2022

Implications

Health systems must identify all applications that are patient data sources, including the EHRs and understand/ monitor vendor plans for CEHRT compliance.

Key Considerations and Actions Required

Technical updates and assurances will be needed from vendors to ensure the health system is not exposed to information blocking by having a business relationship with them. Inventory the applications, identify the contracts and set up a tickler system.

Interoperability rules impact strategic decisions across digital health, partnerships, COVID-19 operational changes, consumer engagement and patient experience.

Next Steps for Preparing for the Cures Act

Interoperability rules impact strategic decisions health systems are making today — across digital health, partnerships, COVID-19 operational changes, consumer engagement and patient experience, among others. Executives must take immediate actions to assess and educate the organization on these impacts and build an interoperability plan that will advance their strategic agendas, while meeting the deadlines.

Consider these questions regarding readiness:

- To what extent is your organization successful at sharing medical data with stakeholders — within the health system, with ACOs, with patients, with other health systems? And what data in the designated record set is not shared now?
- How ready will the organization be to respond to data requests — technically and operationally? And what implications will a use case like clinical notes sharing have?
- Is marketing aware that blocking information or inaccurate NPPES data for providers could result in public reporting of the organization, and does HIM have a process to respond to release of more USCDI information after April 5, 2021 and the designated record set after October 6, 2022?
- How accurate is provider data currently in the NPPES? Do you have a centralized source-of-truth provider contact directory that holds provider preferences including primary DirectTrust address?
- Have you attested to positively blocking information in 2019 on the quarterly Promoting Interoperability attestation, and are staff aware that patients and other third parties can report the organization (and an individual) for information blocking?
- How much change will be required to alert the full care team and post-acute care facilities — not just PCPs or referring providers — of admission, discharge or transfer? Are clinical advisory groups involved in decisions on how ADT notifications will be sent to reduce notifications and "alert fatigue"?
- What are your vendors' roadmaps for CEHRT certification, and will they be ready? (Consider all that have EHI.)
- Have you considered how interoperability serves as a springboard for digital transformation and consumer empowerment and as a driver for robust provider relationship management?

The next chapter focuses on how interoperability rules impact the strategic decisions health systems are making today.

CHAPTER 2

Why Healthcare Executives Should Take a Strategic Approach to Compliance with the New Interoperability Rules

Know where your organization stands:

Complete our eight-question readiness assessment and see your score.

Learn more

With the deadlines for the 21st Century Cares Act becoming effective and penalties now looming, health systems are recognizing they need to take significant workflow and operational actions to comply. Above and beyond complying with the rules, providers can also leverage the work they are already doing to achieve broader IT and organizational strategic goals.

In this second chapter, we explore the strategic implications and benefits of thinking beyond compliance. The first chapter explains the interoperability rules and deadlines as well as the associated provider efforts that are required.

"Consumers are clamoring for their data and greater access, and demand for records during the pandemic has only grown, showing the immediate need for interoperability."

Interoperability Impacts Decisions Health Systems Are Already Making

Health system executives must approach interoperability not simply to comply with the rules but as a strategic advantage. This means taking immediate action to build a holistic interoperability roadmap. Why? The interoperability rules impact strategic decisions health systems are making today, such as those noted below.

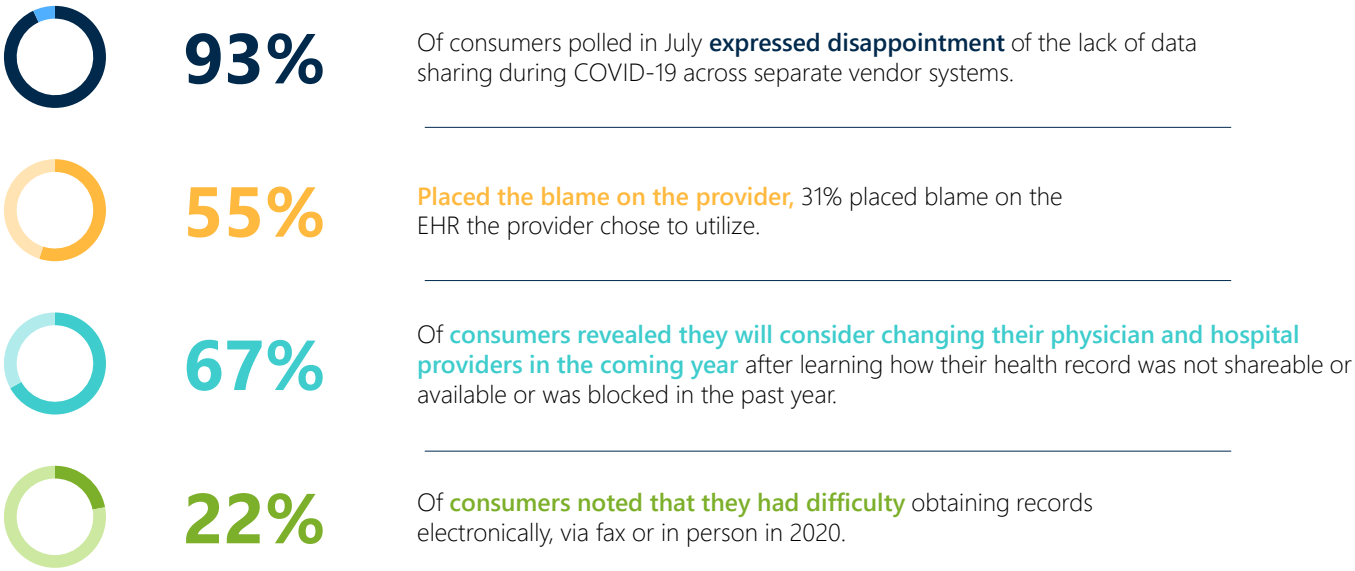
Digital

Digital strategy should incorporate interoperability and patient data management strategies, including patient access to records through personal health records and a digital front door. In fact, the digital front door will be hampered without strategic interoperability. Patient and consumer engagement are increasingly mediated via digital tools and platforms, which are in turn dependent upon the accuracy and quality of data and effective mechanisms for data exchange. As such, a health system's interoperability plan must consider how requests for data received via digital platforms will be managed from a data-flow perspective.

Consumer Demand and Competitive Advantage

Consumers are clamoring for their data and greater access, and demand for records during the pandemic has only grown, showing the immediate need for interoperability. The following findings from a July Black Book Report showed changing consumer perceptions of interoperability and the impact on the providers to whom they turn for their care.[2] As patients expect and increasingly ask providers to share data, they will be dissatisfied when organizations are not ready. Ultimately, patients may redirect their care to organizations that promote interoperability and data access.

Figure 3: Consumer Demand for Interoperability



Source: Black Book Market Research Interoperability Survey 2020. http://www.digitaljournal.com/pr/4761739

Operational Changes

Health systems have already been altering workflows to address the dual system of care required for COVID-19 and non-COVID-19 patients, and the interoperability rules have wide-sweeping operational implications, requiring an enterprise effort. Two examples show the impact:

- **Clinical notes sharing:** Patients or providers can request clinical notes, including progress notes, history of present illness, procedure notes, and even lab and imaging narratives. The health system is required to provide those notes or cite one of the eight blocking exceptions.

  To comply with this request, many operational areas need to work together. For instance, legal will need to work on the HIPAA and Release of Information form updates. Physician and clinical leadership will need to train clinicians on appropriate note content. Compliance will need to ensure staff are aware that they must share these notes to avoid public reporting. Digital and EHR teams will need to provide the data. HIM, the owners of Release of Information, now will need to include these notes in request responses. And the EHR, informatics and physician advisory councils will need to make updates to notes and ensure physicians clean up the problem list and understand implications of the new workflow.

  Significant change leadership is required to drive changes across all these areas to ensure not only compliance with interoperability but also a satisfying patient experience and understanding of the new note content.

- **NPPES updates:** For minimum compliance with the rules, providers must update their contact information in NPPES. They can either do this directly, or a provider organization can aggregate updates through a delegate, such as the Medical Staff Office.

  Leading health systems are taking advantage of the update requirements and strategically using the NPPES as a source-of-truth provider directory or enterprise provider master index to ensure all health system directories are in sync. They understand they can then use their provider index to enhance provider relationship management.

Regardless of the minimal compliance path or strategic path to interoperability, operational and workflow changes are both required.

Partnerships

EHR technology and interoperability strategy may play a factor in evaluating potential partnerships or ensuring existing partnerships are fruitful. In a Center for Connected Medicine survey from August 2019, 57 percent of health systems felt they were successful sharing data with patients, but less felt successful sharing data with other health systems (37 percent) and other partners (35 percent).[3] Holistically caring for the patient requires seamless interoperability between care partners. Partners who have the same approach to interoperability, and even the same systems, may be a best fit for growth strategies.

Penalties

Penalties have been set for developers at up to $1 million per violation for information blocking. These penalties could be just as high for provider organizations once they are set. Providers that promote apps or an extension of their EHRs may be considered a developer, and providers with a health plan also must address the payor components. Moreover, delays in enforcement are short. Compliance dates began in 2021.

Industry Developments

The ban on federal funding for a nationwide patient identifier was repealed, allowing for a national identifier to facilitate patient data exchange. More than 99 percent of providers have adopted EHRs, paving the way for electronic data exchange.[4] HHS and ONC are providing monetary boosts to HIE for improved structure and innovation. ONC is setting up a Trusted Exchange Framework (TEFCA), which will provide a network for national exchange of data. All these factors will drive continued growth of interoperable exchange.

The Next Steps Matter

The key is in not adding one more thing to health system executives' already-full plates; it is in aligning this effort with health systems' current strategic agendas. We recommend taking immediate actions to prepare for compliance with the rules — aligning interoperability efforts with the current strategic agenda.

Start now by building an interoperability plan that will accelerate the health system's strategic agenda, while meeting fall compliance deadlines.

Align with operational changes. In tandem with legal and operations, assess current policy, data flow, and interoperability and processes, identifying gaps. Focus on high-impact use cases — like clinical notes sharing — for data requests, and create an interoperability plan for all five provider requirements.

Sync with digital and patient engagement strategies. Determine how to facilitate sharing and patient points of contact with other digital and consumer engagement efforts like the digital front door.

Build data management into the strategy. A strong data management strategy is key to everything; this data now will be shared with patients, other providers and third parties to make holistic care decisions. Streamlining the numerous provider directories into a single source of truth with strong data governance and data management practices will ensure the data requirements are met for information blocking, NPPES and ADT, and evolve your strategic provider engagement efforts.

Initiate provider outreach. Individual providers will have to make the NPPES database updates themselves, and their notes now will be shared with patients. Begin education and evaluate bulk options, obtaining DirectTrust address early on to streamline the process and considering the role of an enterprise master provider database with up-to-date information.

Build a plan for patient and vendor outreach. Communication plans should be developed to ensure vendors are ready and patients understand how third parties may use their data.

Assess Readiness and Build a Roadmap

Pausing to assess the health system's readiness for interoperability compliance can be a helpful step at this stage. Health system executives need to know where they stand in relation to the rapidly approaching deadlines to understand where it is most important to focus attention. We've prepared a simple assessment to help executives gauge their level of preparation. Complete this assessment to see how you score for readiness.

Take Survey Now

The third chapter discusses the steps health systems need to take to address interoperability compliance and beyond.

CHAPTER 3

The Roadmap to Compliance and Beyond: How to Advance Your Strategic Agenda with Interoperability

There are drawbacks to simply executing minimum-level compliance.

After discussing the interoperability requirements and deadlines and why healthcare executives should take a strategic approach to compliance in the first two chapters, this final chapter turns to the steps IT and operational leaders should take.

We outline the steps that are needed to achieve basic compliance with the five provider requirements and address additional considerations for how health systems can approach interoperability strategically.

Information Blocking

Under the information blocking requirement, providers must share EHI with patients, community providers, and other authorized third-party requestors. This requirement first applies to USCDI data, effective April 5, 2021, then to all EHI in the designated record set by October 6, 2022.

Taking the following steps will help health systems prepare for this provider requirement:

1. **Educate staff.** The health system will need to create an education plan and deploy education that ensures staff creating or delivering patient EHI understand the information blocking requirement and their role in ensuring that the health system can meet requests for information. The education should be targeted to each group's needs, including physicians and clinicians, other front-line staff, and IT members and executives. Staff education should cover some of these topics: HIPAA documentation updates; regulatory and public perception ramifications; differences between what's shared today and what will need to be shared moving forward; and how to respond to patient, provider, or third-party requests for information.
2. **Establish a process and any supporting technology to track requests, responses and exceptions.** The health system's compliance team needs to track requests for information as well as the health system's responses to prove compliance, including any exceptions noted. The compliance team should coordinate this effort with the HIM, IT and operations departments. Depending on the type of information requested, other stakeholders also will play a role. For example, physicians will be involved when sharing clinical notes, which are now required to be shared as part of USCDI.

3. **Evaluate and refine workflows that block information, and address concerns regarding information blocking and sharing.** IT and operations teams should work together to understand where workflows could inhibit sharing of patient information. Health systems need to create plans to address these workflows, including how HIM receives requests today, what is shared, potential areas that could receive data requests in the future and how they should respond. Additionally, since EHR developers are not required to implement functionality for USCDI version 1 until 2022, providers will need to develop their own request response workflows to include all USCDI items. They should also determine how to address concerns from patients or providers regarding information sharing.

In addition to the minimal compliance efforts noted above, we recommend taking further steps that address interoperability holistically, aligning this effort with strategic decisions the organization is already making and avoiding some of the drawbacks that can result.

While not an exhaustive list, the following are some examples:

- Inventory the data currently shared with patients and providers, and incorporate it into the go-forward plan or make adjustments to avoid duplication of data and effort.
- Plan for high-volume use cases, such as requests for provider notes, to ensure the content is appropriate to share and the organization has an established route to share it.
- Ensure clear channels of information delivery with appropriate tracking and receipt confirmation. Create a proactive technology plan that covers sharing patient data with providers and integration into your operational systems, facilitating a decrease in the use of fax machines or other traditional delivery methods.
- Set up performance monitoring and measures to identify and avoid delays.
- Establish a comprehensive change management and operational readiness program to address this dramatic shift in data management, from guarding data to providing open access for patients and authorized third parties.
- Determine the role the organization's service center could play in handling all inbound requests or questions about requests.
- Provide patient education that focuses on how patients can request information and ways the organization is prohibiting information blocking. Also, educate patients on the new role they can play in being an advocate in their own care, helping them understand that they have a right to their data and what USCDI version 1 includes. Health systems also can suggest a method for requests, such as through the patient portal or a digital front door approach, streamlining where patient traffic is received.

Digital Contact Information

Compliance with the requirement for all physicians to update their digital contact information was due March 31, 2021. Organizations need to create a process to make regular updates beyond an initial update.

Basic compliance with the digital contact requirement includes the following steps:

1. **Determine which physicians require updates and notify them.** Identify appropriate providers who need to make updates to their NPPES records, including their digital contact information. These include employed providers and any credentialed providers. Organizations may even want to work with their affiliate providers to avoid an impact to their own reputations or public reporting of those providers.
2. **Establish a process for ongoing updates.** Monitor the regulation guidance for further updates, and establish a regular process for maintaining correct provider digital contact information moving forward. The Medical Staff Office and provider leadership need to be involved in creating and implementing a process for regular provider digital information updates.

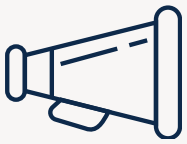
Limited effort for updating provider digital contact information may result in additional effort required down the road. Based on experience across several clients, provider contact information changes at a rate of about 10 percent per year. Not having a process in place for regular updates could lead to a 50 percent error rate for physician contact information after just five years. We recommend seizing the opportunity to create a single source of truth for provider data that can be leveraged for ongoing updates and a broader physician relationship management strategy.

Some steps to consider include:

- Establish a single enterprise-wide owner for accountability to ensure individual provider NPPES record updates don't fall through the cracks.
- Coordinate updates to capture valuable data, such as a correct DirectTrust address.
- Develop a single source of truth to consolidate the silos of provider directories, improve accuracy, lower maintenance efforts and set a foundation for provider relationship management capabilities.

50% The possible error rate after just five years without a process for regular updates to provider information.

Attestation and Public Reporting



CMS will publicly report eligible clinicians, hospitals and critical access hospitals that may be information blocking based on both public reporting and current health system attestation requirements for the Promoting Interoperability Program. In fact, patients and providers can already publicly report providers for alleged information blocking through the Health IT Feedback and Inquiry Portal.

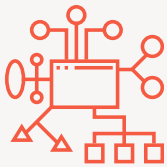
Taking the following step will help health systems prepare for this provider requirement:

1. **Refine efforts for the existing Promoting Interoperability Program attestation that occurs quarterly.** Health systems are already regularly attesting quarterly to CMS for the Promoting Interoperability Program. To prepare for the attestation and public reporting, health systems now must also indicate whether their organization blocked information during the reporting period. This will require a process for collecting that information and incorporating it into the attestation.

Akin to the other requirements, we recommend health systems go beyond minimal compliance to maximize value for the effort and manage their risk. Below is one example:

- Establish a process to regularly review public reports of information blocking so that issues and unfounded reports can be corrected or addressed. Once penalties are stipulated by the OIG, public reports of information blocking could lead to a potential fine.

ADT Notifications



The provider compliance requirement for ADT notifications had a May 1, 2021 deadline. Given the effort required, providers need to plan now for these ADT changes. Health systems should establish a way to capture all the care team members a patient provides and their contact information, not just the referring or ordering physician and the patient's primary care provider. Health systems will need to notify additional care team members and post-acute care facilities of any ADT event.

To attain minimal compliance for this step, we suggest the following:

1. **Train staff.** Staff need to understand how to handle patient or provider requests for ADT notification, including where the information should be captured.
2. **Employ existing technology where possible.** Providers should use existing technology to send ADT event notices to the patient's care team. This should be captured in the EHR where possible or through other electronic methods.
3. **Educate providers about the requirement.** Notify providers that there may be additional alerts due to expansion of the care team and this new requirement. They should be aware of potential alert fatigue, know how to address any redundant incoming information and understand not ignore any necessary action items.

Lack of a planned approach to ADT notifications can lead to duplicate notifications and alert fatigue. It is critical to approach this component strategically. Below are some examples:

- Identify and educate staff about which providers already receive an ADT notification for which use cases and scenarios. For example, if the health system already sends admission notifications to a practice, ensure staff is aware of this to avoid pushing a second notification to the practice physician.
- Pay close attention to how the EHR is designed to capture contact information in a discrete field to avoid duplicate entry of frequent care team members. For example, some registration systems do not have expanded care provider fields to enter the care team members whom a patient requests. Avoid using a comment or free-text note field to capture provider contact information; discrete data pulled from a provider directory is more efficient for repeat ADT events.
- Consider evaluating third-party technology that can automate this process for the organization. There are vendors that provide the service through automated tools, relieving some of the burden on already strapped organizational resources.

Certification of EHR Vendor Technology (CEHRT)

Just as health systems did for ICD-10, provider organizations should monitor that their EHR vendors meet new certification requirements. Beginning in 2022, EHR vendors must retain certification with accredited certification bodies using the new ONC criteria, which include:

- Adoption of the USCDI by December 31, 2022
- Creation of API by December 31, 2022
- Exports of EHI by December 31, 2023

For basic compliance with this requirement, provider organizations should do the following to ensure their vendors are certified:

1. **Confirm core EHR vendor meets certification.** Validate that your core EHR vendor will meet the new CEHRT guidelines.
2. **Inventory remaining relevant EHR vendors.** Ensure that your USCDI data does not come from another source beyond the core EHR. There may be other systems, such as radiology, lab or surgical systems, that need to be included as UCSDI sources and will need to adopt the above requirements. If so, inventory remaining EHR and ancillary applications, and ensure those vendors are also certified. Include each of the facilities across the enterprise, including new acquisitions if those exist.

Additionally, we recommend health systems address vendor certification holistically. Example steps include:

- Create a comprehensive application inventory beyond just EHR vendors to capture systems with patient data. The requirement to provide patient data expands to all EHI in 2022, and a comprehensive inventory will help ensure the organization is prepared.
- If necessary and recommended by the organization's legal team, update vendor contracts with language that validates the EHR vendors will be CEHRT compliant.

The Alternate Approach: Viewing Cures Act Compliance as a Strategic Opportunity

Given the magnitude of Cures Act compliance, we recommended health systems use this effort as a springboard to advance their health system's interoperability and supporting strategic objectives.

Health systems can include the following steps in their plans for a strategic approach to interoperability:

- Perform an assessment of current readiness to comply with the regulations and identify gaps.
- Create a holistic interoperability plan to address gaps from the current state assessment and outline a path to correct workflow or process changes needed for compliance. Be sure to align with strategic decisions the health system is already making, such as digital health and the digital front door, and partnerships and operational decisions for COVID-19.
- Identify this effort as a program with a project manager or project director, sponsors, timeline, milestones, and goals.
- Create an interoperability steering committee involving many of the following stakeholders for a holistic approach: Medical Staff Office, compliance, IT, HIM, marketing and legal.
- Review and update necessary workflows and processes to ensure your organization is not information blocking.
- Establish a single source of truth for provider digital contact information and build upon it to support an ongoing physician relationship management strategy.
- Implement a surveillance process for any public reporting of information blocking and address these issues in a timely manner.
- Educate staff and physicians on the rules, including how to best prevent information blocking, how to address sharing clinical notes and results, where to capture care team member contact information in the EHR or alternate locations, and how to update their digital contact information.
- Include staff beyond the steering committee's hospital and physician leadership, such as marketing and communications, patient experience, digital, HIM and EHR teams, in interoperability planning to create a streamlined, strategic approach across the organization.

Health systems are in a unique position now to use the Cures Act to strengthen their interoperability foundation. Provider organizations can reap many benefits from a strategic approach to compliance — including a central source of truth for provider contact information, improved clinical content, an enhanced patient experience and stronger provider relations.

Sources

1. CHIME IT Executive Survey June 2020. https://chimecentral.org/survey-underscores-telehealths-benefits-during-covid-19-and-beyond/
2. Black Book Market Research Interoperability Survey 2020. http://www.digitaljournal.com/pr/4761739
3. Center for Connected Medicine August 2019 Survey https://connectedmed.com/resources/improving-health-care-interoperability-are-we-making-progress/
4. Pederson, Craig A. "ASHP national survey of pharmacy practice in hospital settings: Prescribing and transcribing—2016." American Journal of Health System-Pharmacy, Volume 74, Issue

Contact us for a review of the rules and implications for your organization.

Learn More from the Authors

Claudia Miller
Associate Principal
cmiller@chartis.com

Chelsea Wyatt
Principal

Paul Murphy
Principal
pmurphy@chartis.com

Robert Faix
Principal
rfaix@chartis.com

Robert Schwartz, MD
Principal

Tonya Edwards, MD
Principal
tedwards@chartis.com

Tony Boerbon
Associate Principal
tborebon@chartis.com

Shawna Schueller
Vice President, Practice Operations
sschueller@chartis.com

About The Chartis Group

The Chartis Group® (Chartis) is a leading healthcare advisory services firm serving healthcare providers, payers, service organizations, and investors. Different by design, Chartis brings an unparalleled breadth and depth of expertise in strategy, performance improvement, digital and technology, clinical quality and patient safety, and strategic communications. Learn how Chartis is helping to build a healthier world at www.chartis.com.

Connect with us: LinkedIn | Twitter | YouTube

THE CHARTIS GROUP