Digital Business

Ensure Compliance: A 25-Point Inspection Plan for Interoperability Initiatives

Does your organization have what it needs for a successful interoperability journey? Follow this checklist of actions, considerations and specific areas where clarity is absolutely required.

Executive Summary

Compliance with the new Interoperability and Patient Access final rule (CMS-9115-F) requires payers to meet significant requirements by the end of 2020. Evaluating initiatives against a comprehensive checklist can help ensure that you capture required activities and meet key benchmarks.

Interoperability is a significant undertaking—more sweeping than recent years' regulatory changes, such as the transition to the 5010 set for HIPAA or ICD-10 diagnostic codes. Meeting the 2021 Patient Access API and Provider Directory API deadline is more than a technical challenge: payers must coordinate interoperability compliance activities across their entire organization. Given interoperability's vast scope, it will be all too easy to overlook crucial dependencies and belatedly identify potential gaps that can delay efforts.

To help guide interoperability efforts and ensure a comprehensive journey to compliance, we've assembled critical assessment areas into a 25-point checkpoint plan (see Figure 1, next page). This tool is based on our two years of experience assisting early-adopting organizations in applying the final rule. By applying these 25 checkpoints against their respective interoperability initiatives, payers can quickly gauge whether their plans are sufficiently comprehensive in scope and deep enough in detail to comply efficiently and with minimal business disruption.

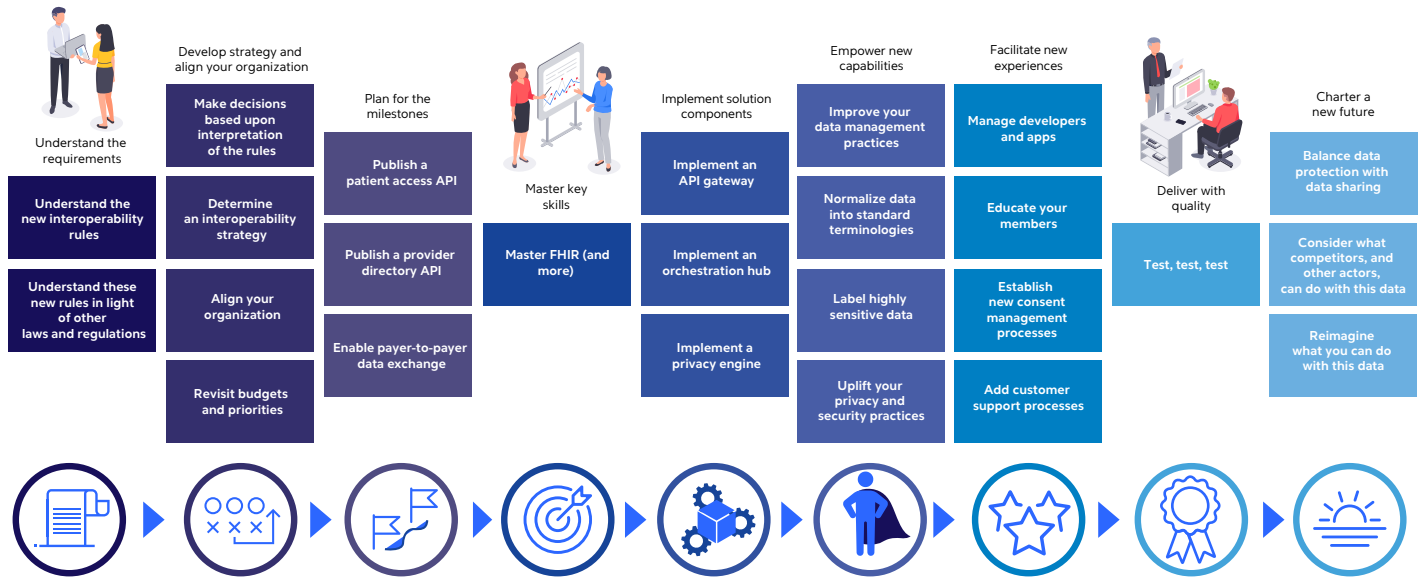**Cognizant**®

25 points of interoperability

Figure 1

Understand the requirements

#1 **Understand the new interoperability rules.** Start by fully comprehending the details within the Centers for Medicare and Medicaid Services' (CMS) Interoperability and Patient Access final rule and CMS' Act final rule. Payers must understand:

❙ The deadlines.

❙ The use of Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR).

❙ The US CORE FHIR profiles involved.

❙ The terminology standards identified.

❙ Education requirements and resources.

❙ Testing and monitoring requirements.

Has your team analyzed this information in detail—engaging IT, the business, compliance, and legal departments?

Have you created your interoperability requirements documentation with traceability to the sections and paragraphs of these rules?

#2 **Understand the new rules in light of other laws and regulations.** The Interoperability and Patient Access final rule indicates that existing laws and regulations go unchanged. Points to check include:

❙ Relation to existing federal, state, tribal and local regulations.

❙ Age of consent.

❙ HIPAA.

❙ State laws such as the California Consumer Privacy Act.

❙ Other regulations.

Has your team's analysis identified and examined in detail all of the above laws and regulations?

Have you created your interoperability requirements documentation with traceability to the sections and paragraphs of related federal, state, tribal and local laws?

Develop a strategy and align the organization

#3 **Make decisions based upon interpretation of the rules.** Points include:

❙ How to best inform patients of their rights and risks.

❙ How to engage application developers.

❙ Know which FHIR resources and profiles to implement.

❙ Define third-party app denial reasons, and more.

Do you have an interoperability governance group that spans IT, the business, legal and compliance?

Do you have a decision log on interpretive decisions, with sign-off from affected stakeholders?

#4 **Determine an interoperability strategy.** Each payer may create a unique strategy based on its vision, strategic objectives and market position. Factors to consider:

❙ Minimum compliance approach vs. proactive market positioning.

❙ Which processes to improve and uplift.

❙ Which new experiences to empower, and more.

Do you have an interoperability vision statement?

Does the vision statement align with your corporate mission; does it help you prioritize your roadmap and decisions?

#5 **Align your organization.** Transformational programs often fail when all roles and functions across an organization are not aligned with key activities and goals. Points to be clear on include:

❙ Vision and strategy.

❙ Tools and technologies.

❙ Definition of success.

❙ Metrics.

❙ Roles and responsibilities.

Have you conducted an interoperability vision workshop, or similar exercise?

Have your organizational alignment activities involved IT, the business, compliance and legal?

#6 **Revisit budgets and priorities.** Some elements necessary for interoperability may already be on organization roadmaps. Areas to examine include:

❙ Inflight initiatives reassessment.

❙ Roadmap reconsideration.

❙ API management.

❙ Master data management.

❙ Partner integration.

Have you factored in reusability of existing assets in defining your interoperability solution?

Have you adjusted project scope, requirements and a schedule for components that can be used in your interoperability solution?

Plan for the milestones

#7 **Publish a patient-access API.** This is one of the priorities for this year. Key considerations include:

❙ Deadline: January 1, 2021 (deferred enforcement date of July 1, 2021).

❙ Includes administrative and clinical data after January 1, 2016, available within one day.

❙ Use of OAuth 2.0 and OpenID.

❙ Use of FHIR.

❙ Use of U.S. Core Data for Interoperability (USCDI).

❙ Use of CARIN Common Payer Consumer Data Set (CPCDS).

Do you have a detailed project plan to reach the Patient Access API compliance date?

Does the project plan identify the dependencies across the organization?

Enable payer-to-payer data exchange. Payers must, at the member's request, send data to any other payer that currently covers the individual or any payer designated by the member.

#8 Publish a provider directory API. The final rule addresses the problem of inaccurate provider data by mandating that insurers publish directory data via API. Key considerations include:

❚ Deadline: January 1, 2021 (deferred enforcement date of July 1, 2021), data within 30 days.

❚ No authentication and authorization.

❚ Public discovery and access.

❚ Use of data formatting and terminology standards.

Do you have a detailed project plan to reach the Patient Access API compliance date?

Does the project plan identify the dependencies across the organization?

#9 Enable payer-to-payer data exchange. Payers must, at the member's request, send data to any other payer that currently covers the individual or any payer designated by the member. Payers must also be able to receive such data. Key considerations include:

❚ Deadline: January 1, 2022.

❚ Within five years of member leaving the plan.

❚ Eligible data: all collected after January 1, 2016.

❚ Must incorporate data into the member record.

❚ Must provide data from prior plan(s).

Do you have a detailed project plan to reach the payer-to-payer data exchange compliance date?

Does the project plan identify the dependencies across the organization?

Master key skills

#10 Master FHIR (and more). FHIR is central to all the requirements of the interoperability rule. Complementary technology and disciplines to learn include:

❚ FHIR.

❚ USCDI.

❚ DaVinci.

❚ Security: OAuth 2.0, OpenID.

❚ Terminologies such as SNOMED CT, ICD-10, RxNorm, and more.

Do you have a training plan to master FHIR, the related security standards, and health informatics standard?

Is your team trained, experienced and effectively using these new skills in the interoperability initiative's planning and execution?

Implement solution components

#11 Implement an API gateway. While the rule itself does not specifically mention an API gateway, payers should implement one that offers:

❚ API management capabilities:

❚ Authentication.

❚ Authorization.

❚ Logging and statistics.

❚ Rate limiting.

❚ Security protections (e.g., against denial of service attacks, SQL injections, etc.).

Have you identified an API management solution?

Does your interoperability solution utilize the best practices of API management?

#12 **Implement an orchestration hub.** An orchestration hub does more than an API gateway or a FHIR server alone. Consider how to manage:

❚ FHIR server.

❚ Repository.

❚ Business rules.

❚ Support for API orchestration.

❚ Support for data consolidation.

❚ Points of integration (e.g., patient and provider matching).

Does your interoperability solution orchestrate APIs and the required data?

Does your interoperability solution enable the governance of APIs and required data?

#13 **Implement a privacy engine.** The privacy engine is responsible for ensuring privacy— managing consents, tagging sensitive data, and auditing based upon sensitive data disclosure. A component separate and distinct from the API gateway and orchestration hub, the privacy engine is responsible for ensuring features such as:

❚ Consent management (with extensibility).

❚ Sensitive data labeling, tagging and segmentation.

❚ Access and disclosure logging and auditing.

❚ Sensitive data filtering masking (future).

Does your interoperability solution provide a component to manage consents?

Does your interoperability solution provide a component to log and analyze access, ensuring privacy?

Empower new capabilities

#14 **Improve data management practices.** Interoperability will expose data management practices to the outside world. Organizations should review how they manage the following:

❚ Data quality.

❚ Data currency.

❚ Member identity and crosswalks.

❚ Provider identity and crosswalks.

Have you identified which data management practices need to be uplifted to provide patients with quality data?

Have you identified which data management practices need to be accelerated to meet the "one business day" requirement of the rule?

#15 **Normalize data into standard terminologies.** Interoperability requires using standardized vocabularies for sharing different types of information. These terms include:

❚ ICD-10.

❚ SNOMED CT.

❚ RxNorm.

❚ NDC.

❚ LOINC.

❚ CPT.

❚ ITU–T. E.123.

❚ eNCPT, and more.

Have you identified each gap in consistent use of terminology ?

Does your interoperability solution provide means to normalize terminologies to the required standards?

#16 **Label highly sensitive data.** "All or nothing" consent for the interoperability API does not reduce audit and reporting requirements or risk management measures. Payers must still comply with all laws and requirements governing sensitive data, such as:

❚ Alcoholism and/or drug abuse or dependence.

❚ Mental health and rehabilitation.

❚ HIV/AIDS.

Does your interoperability solution provide the capability to label highly sensitive data?

Will your interoperability solution enable "data segmentation" by data type and sensitivity; should CMS require such in a future regulation?

#17 **Strengthen your privacy and security practices.** The benefits of increased data portability greatly outweigh new security risks when payers take care to review and ensure that they are following best practices in the following areas:

❚ Identity and access management.

❚ Enterprise data protection.

❚ Application security.

❚ Threat management.

Have you identified and analyzed the size and scope of the new threat vectors with interoperability?

Have you defined specific security uplifts necessary to manage the new risks?

Facilitate new experiences

#18 **Manage developers and apps.** Note that HIPAA does not extend to third-party apps and their use. Payers must then consider the following:

❚ Review apps' AUPs.

❚ Disapprove apps for certain reasons.

❚ Need developer portal and support program.

Have you defined your processes for supporting application developers and application lifecycles?

Have you detailed your processes and criteria for monitoring apps' use of the data?

#19 **Educate members.** The CMS plans to help with materials, covering topics such as:

❚ Members' understanding of rights and risks.

❚ App and usage recommendations.

❚ Anticipate emergent scams and abuses.

Have you identified how you will educate members at key moments (e.g., enrollment, portal login, etc.)?
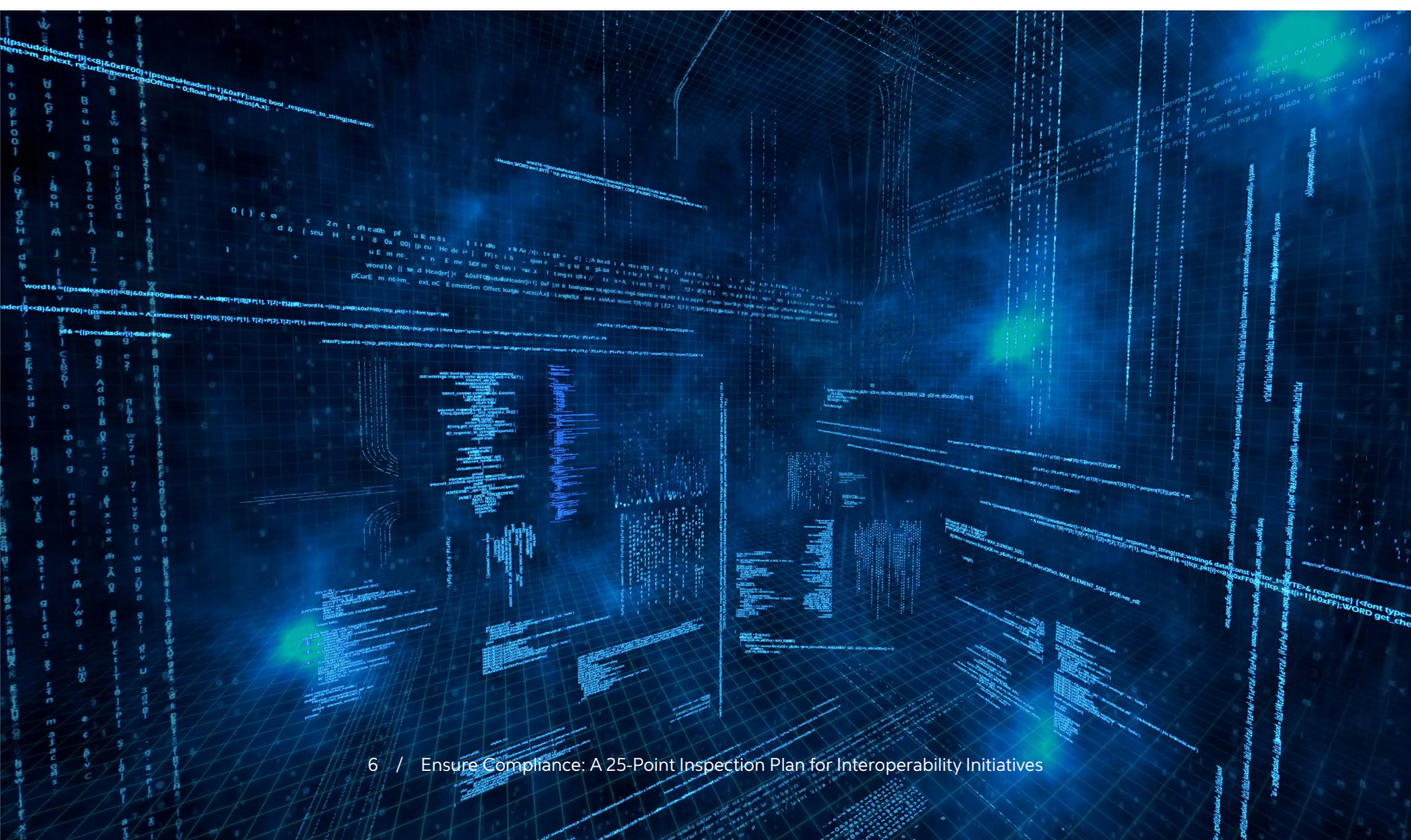
Have you defined the review processes for authoring and editing content and who needs to sign off?

#20 **Establish new consent management processes.** Consent is "all or nothing" for an API, so collecting and tracking consent data is critical. Factors to consider:

❙ Members can still exercise rights in traditional channels.

❙ Need for centralized consent management process.

❙ Need for handling failures, grievances, etc.

Have you defined the processes for how members inquire or can change their consents granted?

Have you identified how interoperability app consent management processes are seamless with existing authorization to release medical information processes?

#21 **Add customer support processes.** Payers must be clear about how they will handle these member-facing issues:

❙ How to handle app questions.

❙ How to grant and revoke consents.

❙ How to see data shared.

❙ How to raise interoperability support issues.

Have you identified the operating model and business processes for supporting members through the contact center?

Have you identified what content and features need to be provided within the member portal?

Deliver with quality

#22 **Test, test, test.** Note that the rule mandates routine testing and monitoring. Additional test planning should cover:

❙ Need for component-level testing (API gateway, etc.).

❙ Need for end-to-end process testing.

❙ Need for performance testing.

❙ Need for penetration testing.

Does your test plan include end-to-end business process testing, addressing complex scenarios such as those involving unique minor's rights, highly sensitive data, and more?

Does your test plan check for attacks and that data cannot be exposed to the wrong party?

Charter a new future

#23 **Balance data protection with data sharing.** Expect the regulatory and industry emphasis on data sharing to increase.

❙ CMS describes this rule as a "first step."

❙ The Cures Act enables much more.

❙ HHS's declared goal is to drive disruption.

Have you identified what priorities your organization will take "beyond compliance?"

Are you tracking all proposed regulation and identifying scenarios that could impact your organization?

By conducting a rigorous and thorough inspection of their interoperability initiatives, payers likely will uncover misunderstandings about how to apply different aspects of the rule, identify critical gaps, and determine where complementary activities are required, such as for vocabulary normalization.

#24 Consider what competitors and other actors can do with this data.
Interoperability effectively reveals competitive differentiators such as network design and benefits. Payers must analyze business strategies in light of these questions:

❚ What might competitors do with this data?

❚ What might other bad actors do?

Have you analyzed how you will monitor the egress of data from your organization?

Have you identified and prioritized your greatest data exposure risks, and what you need to do in response?

#25 Reimagine what your organization can do with this data. Interoperability creates change and opportunity for new efficiency and value creation across such areas as:

❚ Enrollment and high-value "Day 2" activities: consents, primary care physician assignment, program enrollment, wellness, etc.

❚ Utilization management continuity.

❚ Care management continuity.

❚ Retention campaigning.

Have you identified how and when you will excel at obtaining patient consents?

Have you prioritized which processes will benefit the most from the injection of interoperability data?

De-risk and accelerate interoperability activities

By conducting a rigorous and thorough inspection of their interoperability initiatives, payers likely will uncover misunderstandings about how to apply different aspects of the rule, identify critical gaps, and determine where complementary activities are required, such as for vocabulary normalization. A second set of expert eyes on the plan can help eliminate blind spots about which actual vs. aspirational capabilities are needed to achieve compliance. Whether attempting the inspection internally as a self-inspection or working in collaboration with a trusted advisor, payers that ensure their interoperability plans address all 25 points will eliminate much risk from interoperability compliance and accelerate its achievement.

About the author

Gary Meyer

Assistant Vice President, Healthcare Practice, Cognizant Consulting

Gary Meyer is an Assistant Vice President within Cognizant Consulting's healthcare practice. He brings 25 years of industry experience, having brought innovation to leading health plans, health systems, and others in the industry. Gary leads Cognizant Consulting's advisory services for healthcare interoperability, helping organizations define and execute their strategies to achieve compliance as well as to better position themselves in their markets through interoperability. Gary can be reached at Gary.Meyer@cognizant.com.

About Cognizant Healthcare

Cognizant's Healthcare business unit works with healthcare organizations to provide collaborative, innovative solutions that address the industry's most pressing IT and business challenges — from rethinking new business models, to optimizing operations and enabling technology innovation. As a global leader in healthcare, our industry-specific services and solutions support leading payers, providers and pharmacy benefit managers worldwide. For more information, visit www.cognizant.com/healthcare.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 194 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

APAC Headquarters

1 Changi Business Park Crescent,
Plaza 8@CBP # 07-04/05/06,
Tower A, Singapore 486025
Phone: + 65 6812 4051
Fax: + 65 6324 4051