Brochure

Watson Health Community Practice Integration

Frequently asked questions about implementing the IBM Explorys Platform within community practices in support of Clinically Integrated Networks (CIN) and population health initiatives

Watson Health™

IBM

Introduction

Effective community practice integration is a key element of successful value-based care programs. In order to deliver fluid continuity of care among providers in the ambulatory and inpatient settings, data must flow in a secure and timely manner. This document is intended to answer commonly asked technical questions about how IBM® Explorys Platform is deployed within community practices in support of Clinically Integrated Networks (CIN) and population health initiatives. The following questions are addressed in this document:

Q: How does Watson Health define community practice integration?

Q: From which practice data and systems does Watson Health collect data?

Q: How does Watson Health connect to a community practice?

Q: What are the best practices for Community Practice Integration?

Q: What happens to data once it enters the Watson Health Data Center?

Q: Does Watson Health support other data types or connection approaches?

Q: Who uses the IBM Explorys Platform today?

Q: Which health IT vendors are compatible with the IBM Explorys Platform?

Q: How does Watson Health define community practice integration?

A: Community practice integration is the process of establishing data connections with authorized provider offices so information can be exchanged in a secure manner. The goal is to empower continuity of care and reporting. This is done with both employed and independent/affiliate providers, typically within the legal construct of a clinically integrated network (CIN).

A CIN is collaboration among independent/private practice and employed physicians and a hospital or health system to develop a clinical integration program. A clinical integration program is an active and ongoing program of clinical initiatives with the goal of improving the quality and delivery of health care services, leading to greater efficiency in care delivery and cost savings.

Q: From which practice data and systems does Watson Health collect data?

A: The types of data and level of granularity necessary for successful community practice integration depends in large part on the types of programs the network needs to support. For instance, some initiatives may require only basic administrative data from claims files, whereas a Medicare Shared Savings Program (MSSP) ACO will require a broad range of clinical data.

Watson Health supports a myriad of data types and source systems, deployed either on-premises at the practice or at a cloud-based service provider, including:

Electronic Medical Record (EMR) systems: Watson Health supports a wide range of EMRs through a number of interface approaches, including HL7, health information exchange (HIE) protocols, direct database queries, and file import (usually obtained by configuring the system to periodically export data via a reporting function). Data collected from EMRs typically includes provider information, locations, patient information/demographics, appointments, encounters, diagnoses, procedures, observations, lab results, vitals, allergies, immunizations, drug orders, social history, habits, and billing/claim records. However, depending on the practice, some of this data may be contained within other systems. Additional fees from these vendors may apply.

Practice Management Systems: Watson Health supports a wide range of Practice Management Systems (PMS) through direct database queries and file import (usually obtained by configuring the system to periodically export data via a reporting function). Data collected from a PMS typically includes provider information, locations, patient information/demographics, appointments, encounters, and billing/claim records. However, depending on the practice, some of this data may be contained within other systems. Additional fees from these vendors may apply.

Lab systems: If not contained in the practice's EMR system, Watson Health can support remotely-hosted lab systems such as LabCorp and Quest Diagnostics. Additional fees from these vendors may apply.

Outbound billing data: Watson Health supports the collection and processing of outbound claims data in EDI-837 format. The EDI-837 transaction set is the format established to meet HIPAA requirements for the electronic submission of healthcare claim information. An EDI-837 file contains the data necessary to be reimbursed for a medical service. It is normally generated by the EMR or the practice management system. The claim information included amounts to the following, for a single care encounter between patient and provider:

- Description of the patient
- Patient's condition for which treatment was provided
- Services provided
- Cost of the treatment

Payer provided claims data: Watson Health supports the collection and processing of payer processed claims data in EDI-835 or similar format. The EDI-835 transaction set is called Health Care Claim Payment and Remittance Advice. The EDI-835 is used primarily by healthcare insurance plans to make payments to healthcare providers, to provide explanations of benefits (EOBs), or both. When a healthcare service provider submits a Care Claim EDI-837, the insurance plan uses the EDI-835 to detail the payment to that claim, including:

- What charges were paid, reduced or denied
- Whether there was a deductible, co-insurance, co-pay, etc.
- Any bundling or splitting of claims or line items
- How the payment was made, such as through a clearinghouse

A particular EDI-835 document may not necessarily match up one-for-one with a specific EDI-837. In fact, it is not uncommon for multiple EDI-835 transactions to be used in response to a single EDI-837, or for one EDI-835 to address multiple EDI-837 submissions. As a result, processing these interactions between providers and payers is complex and requires a high level of technical sophistication, scale, and human expertise when curation is necessary.

Q: How does Watson Health connect to a community practice?

A: Watson Health can connect to a community practice via several different methods. Selection of these methods depends on types of systems available within the practice, as well as the type of data necessary to support their initiatives.

Always-on connection: This connection type establishes a permanent and secure network link between the Watson Health Data Center and the community practice. This enables the IBM® Explorys Virtual Health Data Gateway (vHDG) to remotely connect to the EMR, PMS, or other hosts that contain relevant data in a secure manner; whether that data is periodically pulled or pushed to the IBM Explorys vHDG via HL7, or some other data transfer method. One key advantage of the Always-on connection type is that it is designed to enable continuous access between systems, providing for highly granular data exchange and near real-time monitoring. The Always-on connection type can be configured in different ways, as described below:

1. **The IBM® Explorys Mini Health Data Gateway (HDG)** configuration, whereby IBM ships a small device that creates a secure connection between the practice and the Watson Health Data Center. Once received, a Watson Health technician walks a representative at the practice through the process of connecting this device to the practice's local-area network, both wirelessly and via supplied Ethernet cables. The typical setup duration of this approach is approximately 20 minutes.
2. **VPN firewall-to-firewall** configuration, whereby a Watson Health technician walks a representative at the practice through the process of configuring their local Internet router to connect to the Watson Health Data Center, in a secure way. This approach requires that the practice has an Internet router that supports firewall-to-firewall VPN connections. The typical setup duration of this approach is approximately 20 minutes.

Secure file transfer: This connection type establishes a secure method to transfer a file from a practice to the Watson Health Data Center. The secure file transfer connection type can be configured in two different ways:

1. **Secure file transfer agent configuration**, whereby a Watson Health technician walks a representative at the practice through the process to download and install a software program to allow manual push or automated flat file transfer to the IBM Explorys vHDG at the Watson Health Data Center. This can also include added configurations within the practice to detect when new files are added to a directory and then automatically transport the file(s). Secure file transfer agent is well suited for situations where a source system cannot easily be connected to, but can be configured to produce data extracts manually or automatically on a scheduled basis. The typical setup duration of this approach is approximately 20-40 minutes per source.
2. **IBM® Explorys Enterprise Performance Management (EPM) Application Suite secure upload feature** configuration, whereby an authorized user within the practice logs into the IBM Explorys EPM Application Suite via a standard web browser and uploads one or more files to the IBM Explorys vHDG at the Watson Health Data Center, in a secure manner. Users may also view the status of previous uploads.

The HIE interface: The Health Information Exchange (HIE) interface connection type establishes a robust, near real-time, and secure method to transfer data from a Certified Electronic Health Record Technology (CEHRT) within a practice to the Watson Health Data Center. In this approach, as events, such as encounters, lab results, or other items of interest, are saved to patients' records in the EMR, the EMR automatically posts security-protected messages containing all the relevant data for that encounter to the IBM Explorys vHDG's HIE interface.

This interface supports a number of data structures including HL7 v2.x/v3.x, CCDA, CCD, CCR, X12, delimited text, XML, and EDI. IBM will supply a file type specification consistent with the data requirements of the CIN's initiatives that may include provider information, locations, patient information/demographics, appointments, encounters, diagnoses, procedures, observations, lab results, vitals, allergies, immunizations, drug orders, social history, habits data relative to patients who participate in the programs.

Q: What are best practices for Community Practice Integration?

A: Over the years Watson Health has learned, through the configuration of thousands of data connectors, CINs must weigh both cost and time against benefit when integrating into practices across large and diverse practice landscapes. Technically, the IBM Explorys HDG can acquire data from virtually any system, but the first part of your integration strategy should be to determine what your CIN's minimum data exchange and reporting requirements are, relative to the programs that you plan to run, such as a PCMH, MSSP ACO, or bundled payment initiatives. Watson Health provides services to help you choose the approach for your CIN.

Fortunately, there are many options to choose from. For instance, if Watson Health has access to an EMR, one popular method of data acquisition is to connect directly to the EMR's

database using a Mini-HDG or Virtual HDG that has a secure network route from the Watson Health Cloud, through the practice's firewall, and directly to the EMR. In that database are tables containing records of patients, procedures, lab results, medication orders/prescriptions, vitals such as blood pressure height, weight, pulse, O2 saturation, appointments, allergies, immunizations and other relevant information.

The advantage to getting data from an EMR is that this approach yields rich and robust data. The disadvantage, however, is that this data usually requires significant mapping from its native data model into the Watson Health data model (e.g., from a field named "lab_value" in the EMR to a field called "observation_value" in Watson Health). It becomes ever more challenging when this data resides in multiple places in the EMR due to workflow variations. And, in addition, this approach also requires that Watson Health standardizes the values in those fields to common ontologies (e.g., LOINC) and units of measure (e.g., mm HG). The timeframe to do this for an EMR can take up to five to eight weeks, so when a CIN has hundreds of these, time is a factor to consider.

Another approach is the "hybrid" method. This method sources data from several places and "weaves" it together using the curation and patient matching engines in the IBM Explorys Platform. For instance, Watson Health can combine data from a practice's EDI-837 billing files with lab results from third-party providers like Quest, plus a limited set of selective data extracts from the EMR (e.g., vitals and appointments) to satisfy other program requirements. Since there is no rate card price for hybrid approaches, they are priced on an hourly basis or as part of a specialized statement of work.

Q: What happens to data once it enters the Watson Health Data Center?

A: As data moves into the Watson Health Data Center, the first stop is the Virtual Health Data Gateway (vHDG). The vHDG makes data available for consumption into the IBM Explorys Platform. The IBM Explorys Platform brings patient data together from across the continuum of care. As data continuously moves into the Watson Health Cloud, Watson Health processing engines process it into useful information. This includes curating the data so that diagnoses, labs, procedures, claims, and other data elements are standardized and able to be compared effectively. Separate records from across all care settings for the same patient are combined, so providers have a more complete picture of the patient. Data governance and provider-to-panel attribution rules are applied and risk scores, measures, and care gaps are calculated.

A graphic representing this process is included below.

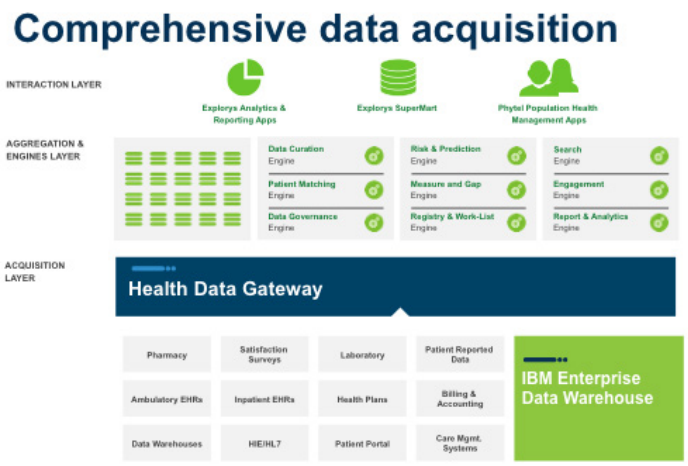

Figure 1: Graphic demonstrating the Watson Health data acquisition process.

With this data now turned into actionable information, it is made available to authorized providers and staff via web applications (apps). These apps can be easily integrated into certain supported EMRs. Watson Health also makes this information available through standard reporting tools, as well as web-service API that allow for bi-directional communication with other third-party systems.

On top of all this, Watson Health can assist in implementing a wide range of risk models to identify opportunities to intervene and improve outcomes. This enables the three key components of value-based care: population assessment, population management, and performance measurement.

For population assessment, this provides the ability to better understand the past in order to predict future utilization, costs, and outcomes. Watson Health provides a data-informed view of at-risk populations including their demographics, their diseases relative to utilization, their proximity to the services that your CIN provides, and some of the biggest opportunities for risk mitigation. With this in hand, organizations can now enact plans, for example, care coordination and patient outreach, that are even better suited to their objectives.

The IBM® Explorys Program Framework also offers a wide range of pre-built registries, workflow, and engagement templates so that your care coordinators and providers can act upon that information. Watson Health also provides performance measurement templates that provide standard but configurable dashboards, measure libraries, and reports for leadership, care coordinators, and providers to track improvement and measure their success.

Q: Does Watson Health support other data types or connection approaches?

A: Having worked with clients of virtually all sizes and configurations, Watson Health has developed the ability to pull data from nearly any type of system. The team is committed to working with you to find creative ways to accomplish your community practice integration goals.

Q: Who uses the IBM Explorys Platform today?

A: Some of the largest integrated healthcare delivery networks in the United States, like Cleveland Clinic, MedStar Health, Centura Health and Mercy Health, run the IBM Explorys Platform to manage their value-based care and analytic initiatives. Together, they constitute more than 360 hospitals, 920,000 providers, and 64 million unique cared-for-lives.

Q: Which IT vendors are compatible with the IBM Explorys Platform?

A: The IBM Explorys Platform works with a myriad of health IT vendors and continues to add support for new vendors regularly. Watson Health will support virtually any CEHRT system that provides open access to your data. Both connectors and productive working relationships currently exist with most health IT vendors.

About IBM Watson Health

In April 2015, IBM launched IBM Watson Health and the Watson Health Cloud platform. The new unit will work with doctors, researchers and insurers to help them innovate by surfacing insights from the massive amount of personal health data being created and shared daily. The Watson Health Cloud can mask patient identities and allow for information to be shared and combined with a dynamic and constantly growing aggregated view of clinical, research and social health data.

For more information on IBM Watson Health, visit: ibm.com/watsonhealth.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2016

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others.

No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

HPB03010-USEN-02

Watson Health™