INFRASTRUCTURE

The Infrastructure section of the survey assess an HCO's performance in four topic areas:

1. Infrastructure Monitoring practices
2. Infrastructure Capabilities Supported
3. Infrastructure Governance
4. Infrastructure Performance

Section 1: Infrastructure Monitoring Practices

(PDF-001) How would you characterize the adoption of the following tools/methods in your organization to monitor your IT systems?
(Check one per row)

Fully Adopted: A condition where the technology/solution has been implemented organization wide and the relevant users are generally utilizing the technology/solution as intended per industry expectations and organizational policy.
Partially Adopted: A condition where the technology/solution has been implemented in at least one area of the organization but not organization wide, or the technology/solution has been implemented organization wide but the relevant users are not utilizing the technology/solution as intended per industry expectations and/or organizational policy.
Not Adopted: A condition where the organization has not yet implemented the technology/solution in at least one area of the organization, has no intention of implementing the technology/solution at this time or has not yet achieved funding approval for the acquisition of the technology/solution.

	Fully Adopted	Partially Adopted	Not Adopted
A. Automated tools to escalate problems to highly skilled technicians (Level 2 or 3) based on category and type			
B. Dashboard to manage infrastructure by exceptions/anomalies			
C. Log collection automation			
D. Utilize pattern detection against automated login attempts			
E. Gather and trend data to mitigate potential issues before they occur			
F. Perform and escalate on system log exceptions/errors			
G. Utilize tools such as user behavior analytics or user/entity behavior analytics (UBA/UEBA)			

The intent of this question is to not only ensure the healthcare organization (HCO) has varied IT system monitoring and support procedures in place to safeguard the functioning of the HCO's IT hardware and

software, but the extent to which the solutions are used throughout the HCO. Basic monitoring is performed through device operation checks, while more advanced monitoring gives granular views on operational statuses, including average response times, number of application instances, error and request rates, CPU usage and application availability.

A. Automated tools to escalate problems to highly skilled technicians (Level 2 or 3) based on category and type

IT Support within an organization tends to be partitioned into different levels of technical support. The level of support offered is partitioned into Tiers (typically Tier 1 – Tier 4) with Tier 1 being the most basic level of support and higher tiers reflecting more advanced degrees of support. Tier 2 staff have the knowledge base and skills to handle more complex customer issues and will often use remote control tools. Tier 3 is usually the highest level of technical skill within an organization, and often includes the product engineers or developers. Automated tools can be used to assist IT Support operations by leveraging keywords to escalate IT support requests to the appropriate Tiered level of support.

Examples:

- InvGate Service Desk
- ServiceNow ITSM
- Wrike

B. Dashboard to manage infrastructure by exceptions/anomalies

Exceptions and *anomalies* are actions or behaviors that exceed set thresholds in Threat Protection. While they do not always indicate malicious behavior, they should be investigated to determine their cause as it helps organizations know if there is gradual performance degradation. Dashboards are used to facilitate viewing performance metrics and help users intuitively scan through hundreds of performance metrics with ease.

Examples:

- AppDynamics
- New Relic
- Sentry

C. Log collection automation

Log collection is the process of automatically collecting log data from various log sources within an organization's network and bringing them together in a central location for better analysis. This makes it easier to understand how your systems are interacting with each other and helps you identify potential issues you need to troubleshoot.

Examples:

- ManageEngine EventLog Analyzer
- SolarWinds Kiwi Syslog Server
- Syslog-ng Store Box

D. Utilize pattern detection against automated login attempts

To keep an IT system secure, organizations will often investigate user logins to uncover suspicious user activity. This helps to identify user accounts that may have had their credentials

compromised, focus the investigation on certain time frames, and identify other computers that are compromised.

Examples:

- AWS WAF Bot Control
- Cyber Triage
- F5 Distributed Cloud Bot Defense

E. Gather and trend data to mitigate potential issues before they occur

Data quality profiling is the process of examining data from an existing source and summarizing information about the data. It helps identify corrective actions to be taken and provides valuable insights that can be presented to the business to drive ideation on improvement plans. Data profiling can be helpful in identifying which data quality issues must be fixed at the source, and which can be fixed later.

Examples:

- Atlan
- Datamartist
- Dataedo

F. Perform and escalate on system log exceptions/errors

Events that occur in end-user devices or IT systems are commonly recorded in log files. Security teams can use security logs to track users on the corporate network, identify suspicious activity and detect vulnerabilities. Most security and IT organizations find that systems generate more log information than they can process. Event and log management tools help analyze logs, monitor important events recorded in logs, and leverage them to identify and investigate security incidents.

Examples:

- Appian
- Exabeam
- Servicenow

G. Utilize tools such as user behavior analytics or user/entity behavior analytics (UBA/UEBA)

User and Entity Behavior Analytics (UBA/UEBA) is an algorithmic approach to network monitoring that focuses on the activities of both human actors and entities such as hosts, software platforms, and endpoints. While UBA is designed to track insider threats, UEBA is designed to use machine learning to look for more types of anomalous activities associated with more types of threats, including advanced threats, that may be obscured by legitimate network activities. Through machine learning, UBA/UEBA solutions establish a baseline for what constitutes 'normal' behavior on a network. They then use this baseline to identify potential threat actors and compromised systems.

Examples:

- IBM QRadar
- Rapid7 InsightIDR
- LogPoint

(NEW-002) Which of the following functions are automated in your IT asset management (ITAM) program?
(Check all that apply)

A. Software license management
B. Software inventory
C. Hardware inventory
D. Procurement management

The intent of this question is to ensure healthcare organizations (HCO) have automated solutions in place designed to assist with the management of an HCOs' IT assets.

A. **Software License Management**

A Software License Management system, part of software asset management, involves software license tracking, documenting, and controlling how and where software is used in your organization. A software license management tool can assist you in complying with license agreements, i.e., end-user license agreements (EULA).

B. **Software Inventory**

Software inventory is a catalog of all software and applications that are functioning in an IT network. An automated software inventory tool helps HCOs stay on top of all the software-related changes or additions in their network and ensures they are software audit-ready at all times.

C. **Hardware Inventory**

Hardware inventory management is the recording and tracking of hardware assets and IT inventory in an organization. Hardware inventory software is a tool that automatically tracks and fetches all hardware data and provides administrators with a snapshot on the state of hardware in their corporate network.

D. **Procurement Management**

Software procurement is the overarching process of buying software for an organization. The procurement management function encompasses sourcing, purchasing, and paying for the software. While sourcing activities are an important part of the process, sourcing is a subset of procurement.

Section 2: Infrastructure Capabilities Supported

(PDF-003) Which of the following wireless applications and/or technologies does your organization(s) support?
(Check all that apply)

A. RFID/RTLS Locator System
B. Wander Management/Patient Elopement/Infant Abduction (Acute/LTPAC)
C. Telemetry over Internet Protocol (TMoIP)
D. Patient wearables integrated with the EHR

The intent of this question is to ensure the HCO's IT environment can wirelessly support select IT functionalities, applications and/or technologies.

A. RFID/RTLS Locator System

A system to wirelessly manage assets within an HCO (e.g., for medical devices). Radio Frequency Identification (RFID) describes any locating system, either passive or active, that uses the radio-frequency range of electromagnetic signals (LF, HF and UHF) to transmit identification and location data. But, because its namesake radio frequencies are now used primarily for passive locating systems, the broader term, RFID, is increasingly used as shorthand for passive systems only. Real Time Location Systems (RFLS) deploy "active" tags, meaning that each tag transponder has its own power source, unlike those of "passive" RFID systems in which the transponder is powered remotely by the sensor that reads it. RTLS systems allow HCOs to identify an object and determine its approximate location in real time.

Examples

- Centrak
- Cox Blue
- Litum

B. Wander Management/Patient Elopement/Infant Abduction

A system to wirelessly locate patients within an inpatient facility.

Examples

- Centrak
- Securitas Healthcare
- Kenton Brothers

C. Telemetry over Internet Protocol (TMoIP)

A method of transporting telemetry data wirelessly over a network at OSI layer 3 (provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network, while maintaining the quality of service requested by the transport layer).

Example

- CenSin
- NetAcquire
- Vitec

D. Patient wearables integrated with the EHR

Wearables can enable remote monitoring of patients at all times to support the needs of the real-time virtual care of patients. This data can then be recorded in EHR system to create a 360° health view for patients and their physicians.

Example

- Apexon
- Cprime
- Webmedy

(PDF-004) How would you characterize the adoption of the following technologies used to improve caregiver workflow in your organization?
(Check one per row)

Fully Adopted: A condition where the technology/solution has been implemented organization wide and the relevant users are generally utilizing the technology/solution as intended per industry expectations and organizational policy.
Partially Adopted: A condition where the technology/solution has been implemented in at least one area of the organization but not organization wide, or the technology/solution has been implemented organization wide but the relevant users are not utilizing the technology/solution as intended per industry expectations and/or organizational policy.
Not Adopted: A condition where the organization has not yet implemented the technology/solution in at least one area of the organization, has no intention of implementing the technology/solution at this time or has not yet achieved funding approval for the acquisition of the technology/solution.

	Fully Adopted	Partially Adopted	Not Adopted
A. Patient context management between applications			
B. Single sign-on—biometrics			
C. Single sign-on—proximity systems (tap-n-go)			
D. Roaming virtual desktop sessions (Virtual Desktop Infrastructure)			
E. Traveling profiles			
F. Mobile POC devices			
G. Mobile voice recognition for clinician notes, order entry, etc.			
H. Voice assistants/activated devices (e.g., Amazon Echo Dot, Google Nest, etc.) to streamline some patient/exam room tasks			
I. Remote published applications			

The intent of this question is to assess the HCO's efforts to leverage IT in realizing efficiencies in caregiver work processes, and the extent to which the solutions are used throughout the HCO.

A. Patient context management between applications

With context management, a clinician can have access to the same clinical information stored in different healthcare applications. Examples of clinical information are the identity of a patient, identity of a user, or a particular encounter with a patient.

Examples

Imprivata
Sirenia

B. Single sign-on—biometrics

Single sign-on (SSO) is an identification method that enables users to log in to multiple applications and websites with one set of credentials. SSO-biometric identification system allows users to securely access several different apps and services using their biometric credentials instead of passwords.

Examples

Ikosmos

Bayometric
Imprivata

C. Single sign-on—proximity systems (tap-n-go)

Single sign-on (SSO) is an identification method that enables users to log in to multiple applications and websites with one set of credentials. SSO streamlines the authentication process for users. Tap-and-go functionality enables clinicians to use a single username and password to gain access to several key applications on clinical workstations by waving a badge over a reader, which automatically logs them in to their virtual desktops, etc.

Examples

Authx
Hideez
Imprivata

D. Roaming virtual desktop sessions (Virtual Desktop Infrastructure)

Virtual desktop infrastructure (VDI) delivers desktop images over a network to endpoint devices, enabling users to access their desktops from anywhere. VDI requires enterprises to host the desktop operating systems on remote servers located inside the data center and manage them.

Example

Citrix
Microsoft
Vmare

E. Traveling profiles

A traveling (a.k.a. roaming) user profile is a file synchronization idea that allows users to log on to any computer on the same domain and access their documents and have a consistent desktop experience, such as applications remembering toolbar positions and preferences, or the desktop appearance staying the sam.

Example

Microsoft

F. Mobile POC devices

Mobile Point-of-care (POC) devices allow caregivers to instantaneous access results supporting the provision of timely patient care without having the devices being tethered to a LAN-like plug-in.

Example

PTS Diagnostics
Siemens

G. Mobile voice recognition for clinician notes, order entry, etc.

Using mobile voice recognition, healthcare providers can dictate notes into their computers without having to take time away from patient care. As a result, they can devote more time to personal interactions or other tasks while completing their work efficiently.

Example

DeepScribe
Webmedy

H. Voice assistants/activated devices (e.g., Amazon Echo Dot, Google Nest, etc.) to streamline some patient/exam room tasks

A voice assistant is a digital assistant that uses voice recognition, language processing algorithms, and voice synthesis to listen to specific voice commands and return relevant information or perform specific functions as requested by the user.

I. Remote published applications

A remote application is an application delivery solution wherein the actual application is installed on a central server and is used from a remote device. The end user receives screenshots of the application while being able to provide keyboard, thumb tap and mouse inputs. Remote apps have many names: remote application, server-client apps, app remoting, application virtualization and virtual apps.

Example

Vmware

(PDF-005) How would you characterize your clinical staff's authorized use of the following types of employee-owned devices in the care of your patients?
(Check one per row)

Used Extensively: A condition where authorized clinical staff leverage the technology/solution on a routine basis.
Allowed but not Used Extensively/Limited Use: A condition where authorized clinical staff leverage the technology/solution as an exception, or few authorized clinical staff leverage the technology/solution on a routine basis.
Use Not Authorized: A condition where the organization does not authorize the use of employee-owned devices in the care of patients.

	Used Extensively	Allowed but not Used Extensively/ Limited Use	Use Not Authorized
A. Laptops/Tablets			
B. Smartphones/Smartwatches (to include embedded voice activated functionalities)			
C. Voice assistants/activated devices (e.g., Amazon Echo Dot, Google Nest, etc.)			

As employees are increasingly bringing their own personal technological devices to work (whether HCO leaders want them to or not), the intent of this question is to ascertain the HCO's support of employee-owned devices allowed in the care of patients, and the extent to which these devices are used.

A. Laptops/Tablets

B. Smartphones/Smartwatches (to include embedded voice activated functionalities)
Nurses can use personal smartphones and embedded voice activated functionalities in smartwatches as an efficient method to gather patient care information and to communicate with the health care team.

C. Voice assistants/activated devices (e.g., Amazon Echo Dot, Google Nest, etc.)
Smart speakers like Amazon Echo and Google Home offer a much-needed conversational voice interface, thereby allowing providers to ask questions and retrieve information essential for patient treatments without breaking sterile scrub or using a traditional computer.

(PDF-006) Which of the following communication equipment and services could your staff potentially use in the event of an emergency? (ACUTE/AMBULATORY/LTPAC) (Check all that apply)

A. Fixed line network
B. First Responder Network
C. Satellite phone, VSAT, MSAT and other satellite communications
D. Government Emergency Telephone Service (GETS) cards
E. Prioritized wireless communication (Wireless Priority Service or Telecommunication Service Priority)
F. Crisis communications platform

Employees are increasingly bringing their own personal technological devices to work (whether HCO leaders want them to or not). The intent of this question is to ascertain the HCO's support of varied devices owned by employees allowed in the care of patients.

A. Fixed line network

A wired network used for voice and data communications through which a user can make phone calls or connect to the internet.

B. First Responder Network

The First Responder Network Authority (FirstNet) was created to implement the 9/11 Commission recommendation to give public safety providers 21st-century communication tools to help save lives, solve crimes, and keep our communities and emergency responders safe..

C. Satellite phone, VSAT, MSAT and other satellite communications

VSAT (Very Small Aperture Terminal): is a small-sized earth station used in the transmit/receive of data, voice and video signals over a satellite communication network, excluding broadcast television.

MSAT (Mobile Satellite): is a satellite-based mobile telephony service developed by the National Research Council of Canada. Supported by a number of companies in the US and Canada, MSAT hosts a number of services, including the broadcast of CDGPS signals.

D. Government Emergency Telephone Service (GETS) cards

GETS is a program of the Department of Homeland Security, Office of Emergency Communications that prioritizes calls over wireline networks. Users receive an access card (GETS card), which has both the universal GETS access number and a Personal Identification Number (PIN).

E. Prioritized wireless communication (Wireless Priority Service or Telecommunication Service Priority)

WPS: A Federal program that authorizes cellular communications service providers to prioritize calls over wireless networks. Participation in the WPS program is voluntary.

TSP: An FCC program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program and the U.S. Department of Homeland Security, manages the TSP program. The TSP program is in effect all

the time--it is not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

F. Crisis communications platform

A secure, web-based communications platform designed to manage stakeholder engagement for day-to-day media relations, as well as in times of a crisis.

Example:

Jetty

Section 3: Infrastructure Governance

(PDF-007) Which of the following elements are included in your organization's bring-your-own-device (BYOD) policy?
(Check all that apply)
Definitions

Key definitions: Scope, purpose, and governance structure of the BYOD program, along with the definition of important terms used in the policy.
Service provision: Specifies the process of enrollment, registration, and deregistration.
Access control: Defines who will have access to what information and when. This is particularly important for personal health information, where the principle of least privileges must be applied. Only the required information must be supplied and only when needed, especially when it comes to patient data.
Data storage: Specifies what patient data are allowed to be stored on BYOD devices and how. If backup is involved, the policy should also advocate for separate backup of personal and patient data.
Incident reporting: Defines the procedure for reporting cases of breaches, including cases of theft/loss of device. Employees must report such cases to the IT department, especially if patient data are involved, and the IT department must report it to government agencies in case of major breaches.
Legislation and noncompliance: Defines applicable privacy or health care laws as well as actions or penalties in case of noncompliance with the policy or in case of breaches caused by employee's personal devices.
Education strategy: Strategies to train employees periodically to ensure secure user behavior. BYOD users should be constantly updated about latest cybersecurity threats. Policies should be disseminated through all means possible. Changes in policies should also be communicated.
Acceptable use: States the purposes for which BYOD devices could be used, whether clinical or nonclinical, and by whom. It defines reasonable use and prohibited activities.
Not applicable: Our organization does not allow employees to use their own devices while at work and/or in the care of our patients.

A. Key definitions
B. Service provision
C. Access control
D. Data storage
E. Incident reporting
F. Legislation and noncompliance
G. Education strategy
H. Acceptable use
I. Not applicable

As employees are increasingly bringing their own personal technological devices to work (whether HCO leaders want them to or not), the intent of this question is to ascertain the policy and procedures the HCO has in place to support the use of varied devices owned by employees allowed in the care of patients.

Citation

Considerations for Conducting Bring Your Own “Device” (BYOD) Clinical Studies

Section 4: Infrastructure Performance

(PDF-00) How quickly can your organization restore mission critical operations should a disaster cause the complete loss of your organization's primary data center? (Check one per row)

	<4 hrs.	4 - 24 hrs.	>24 hrs.	Don't Know
A. Clinical information systems (EHR, lab, radiology)				
B. Administrative systems (Financial, Human Resources and Supply Chain)				
C. Network and phone systems				
D. Employee access and communication systems (Active directory, email, messaging)				

The intent of this question is to ascertain the HCO's ability to restore **mission critical operations** in the event the organization's primary data center is compromised.