SECURITY

The Security section of the survey assess an HCO's performance in five topic areas:

1. Security Leadership
2. Security Governance
3. Security Practices – Leveraging External Resources
4. Security Practices – Internal Processes
5. Security Insurance

Section 1: Security Leadership

(PDF-009) Whom on your executive team is primarily responsible for leading information security in your organization?
(Check one)

A. CISO, Vice President of Information Security or other similar security related title in your executive suite
B. CIO
C. An executive other than a CISO or CIO (e.g., CFO; COO)
D. We outsource this function (e.g., external security leader/vendor)
E. A non-executive team member (e.g., Director of Security)
F. No security leader

The intent of this question is to ascertain if the HCO has a dedicated person overseeing the HCO's cybersecurity efforts.

Section 2: Security Governance

(PDF-010) How often does your organization's formally chartered cybersecurity governance, risk and/or compliance committee meet?
(Check one)

A. Weekly
B. Monthly
C. Quarterly
D. At least once a year
E. As requested (no regular cadence)
F. We do not have a formally chartered cybersecurity governance, risk and compliance committee

The intent of this question is to ascertain the priority cybersecurity holds within the HCO as reflected in the frequency by which the cybersecurity leaders formally meet.

(PDF-011) Which of the following groups receive a formal report regarding your organization's information security efforts and/or performance at least every quarter? (Check all that apply)

A. Board of trustees, or committee of the board
B. Executive leadership / executive governance
C. IT leadership
D. Clinical staff and leadership
E. Front lines staff and data leaders

The intent of this question is to ascertain the priority cybersecurity holds within the HCO as reflected in the frequency by which varied leadership groups within the HCO are informed of the HCO's cybersecurity efforts.

Section 3: Security Practices – Leveraging External Resources

(PDF-012) Which of the following information security frameworks does your organization use to guide your information security program?
(Check all that apply)

A. NIST Cybersecurity Framework
B. 405(d) (Acute/Ambulatory/LTPAC)
C. HITRUST
D. ISO 27000 series
E. COBIT
F. Critical Security Controls

The intent of this question is to ascertain that the HCO has at least one framework guiding their cybersecurity risk management efforts. An information security framework is designed to reduce risk levels and the organizations exposure to vulnerabilities allowing security leaders to more intelligently manage their organizations cyber risk. The framework should consist of a number of documents that clearly define the adopted policies, procedures, and processes by which the organization abides. It effectively explains to all parties (internal, tangential and external) how information, systems and services are managed within the HCO.

A. NIST Cybersecurity Framework

NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology based on existing standards, guidelines, and practices.

B. 405(d)

The 405(d) Program aims to develop consensus-based best practices, and methodologies to strengthen the healthcare & public health (HPH) sector's cybersecurity posture against cyber threats.

C. HITRUST

Health Information Trust Alliance (HITRUST) is a privately held company located in Frisco, TX that, in collaboration with healthcare, technology and information security organizations, established the HITRUST CSF. The HITRUST Common Security Framework (HITRUST CSF) is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.

D. ISO 27000 series

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization and the International Electrotechnical Commission. ISO 27000 recommends best practices for managing information risks by implementing security controls, within the framework of an overall Information Security Management System (ISMS). It is very similar to standard management systems such as those for quality assurance and environmental protection.

E. COBIT

COBIT (Control Objectives for Information and Related Technology) helps organizations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organizational goals. The framework is business focused and defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.

F. Critical Security Controls

The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.

(PDF-013) How would you characterize your organization's use of the following information sharing and analysis organizations used to identify cybersecurity threats and vulnerabilities? (Check one per row)

Used Extensively: A condition where relevant staff in the organization leverage the resource/solution on a routine basis.

Used but not Extensively: A condition where relevant staff in the organization leverage the resource/solution as an exception, or few relevant staff leverage the resource/solution on a routine basis.

Not Used: A condition where relevant staff in the organization do not leverage the resource/solution at all.

	Used Extensively	Used but not Extensively	Not Used
A. Cyber Information Sharing and Collaboration Program (CISCP): DHS's program for public-private information sharing (Acute/Ambulatory/LTPAC)			
B. Health Information Trust Alliance (HITRUST)			
C. Informal sharing in HIT user groups			
D. Informal sharing in professional society			
E. Health Information Sharing and Analysis Center (H-ISAC)			
F. State hospital associations (Acute/Ambulatory/LTPAC)			
G. Department of Homeland Security/CISA (Acute/Ambulatory/LTPAC)			
H. National Cybersecurity & Communication Integration Center (NCCIC) (Acute/Ambulatory/LTPAC)			
I. Health Cybersecurity & Communication Integration Center (HC3) (Acute/Ambulatory/LTPAC)			
J. Private Information Sharing and analysis organizations			

The intent of this question is to ascertain that the HCO is involved at some level with at least one cybersecurity information sharing and analysis organization, and the extent to which it is used throughout the HCO.

A. Cyber Information Sharing and Collaboration Program (CISCP): DHS's program for public-private information sharing

The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors.

B. Health Information Trust Alliance (HITRUST)

Health Information Trust Alliance (HITRUST) is a privately held company located in Frisco, TX that, in collaboration with healthcare, technology and information security organizations, established the HITRUST CSF. The HITRUST Common Security Framework (HITRUST CSF) is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.

C. **Informal sharing in HIT user groups**

An informally established HIT user group designed to connect HIT professionals together to share insights, strategies and best practices around cybersecurity issues/threats.

D. **Informal sharing in professional society**

An informally established network within a professional society (e.g., CHIME) designed to connect professionals together to share insights, strategies and best practices around cybersecurity issues/threats.

E. **Health Information Sharing and Analysis Center (H-ISAC)**

H-ISAC (Health Information Sharing and Analysis Center) is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.

F. **State industry associations (e.g., hospital/nursing home association)**

Regional hospital, nursing home, etc. membership organizations structured to address member concerns (to include cybersecurity).

G. **Department of Homeland Security/CISA Department of Homeland Security/CISA**

The Cybersecurity and Infrastructure Security Agency (CISA) is an operational component of the Department of Homeland Security (DHS). Under the leadership of Director Jen Easterly, CISA works to understand, manage, and mitigate risk to the nation's cyber and physical infrastructure in the public and private sector.

H. **National Cybersecurity & Communication Integration Center (NCCIC)**

The National Cybersecurity and Communications Integration Center (NCCIC) is part of the Cybersecurity Division of the Cybersecurity and Infrastructure Security Agency, an agency of the U.S. Department of Homeland Security. It acts to coordinate various aspects of the U.S. federal government's cybersecurity and cyberattack mitigation efforts through cooperation with civilian agencies, infrastructure operators, state and local governments, and international partners. It is also responsible for coordinating the national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP)

I. **Health Cybersecurity & Communication Integration Center (HC3)**

As part of its mission, the National Cybersecurity and Communications Integration Center (NCCIC) works to reduce risks within and across all critical infrastructure (CI) sectors by partnering with law enforcement agencies and the intelligence community and by coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, NCCIC collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share information about control systems-related security incidents and mitigation measures.

J. **Private Information Sharing and analysis organizations (ISAOs)**

An ISAO is a group created to gather, analyze, and disseminate cyber threat information. Unlike ISACs, ISAOs are not directly tied to critical infrastructure sectors, as outlined in Presidential

Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc.

(PDF-014) Does your organization use the services of a 3rd party to conduct the following assessments?
(Check one per row)

	Yes – At least annually	Yes – Every two years	Yes – But not on a regular basis	No
A. Risk (identify compliance gaps and security vulnerabilities)				
B. Cybersecurity Maturity				

The intent of this question is to ascertain;

- that the HCO leverages the services of a 3rd party to conduct key cybersecurity assessments
- the frequency by which the HCO conducts the aforementioned assessments.

A. Risk (identify compliance gaps and security vulnerabilities)

Leveraging the services of a 3rd party vendor/contractor, the HCO commissions a study to identify gaps in the HCO's current state of compliance and its desired level or standard. It also conducts an assessment of the HCO's security vulnerabilities.

B. Cybersecurity Maturity

A cyber maturity assessment framework defines multi-distinct maturity levels, which indicate the degree to which an organization has optimized security systems and processes. During the progression from level one to the highest level, an organization will develop, refine, and enhance its cybersecurity posture.

Section 4: Security Practices – Internal Processes

(PDF-015) How often are the following components of your risk management program reviewed (and updated when deemed necessary)?
(Check one per row; Leave blank if not applicable)
IDENTIFICATION OF…

		At Least Weekly	Monthly	Quarterly	Every 6 Months	Less than Annually	Annually /As Requested
A.	Risks						
B.	Who is responsible for managing/mitigating those risks						
C.	Contingency/mitigation plans						
D.	Risk level/ranking						
DETECTION OF…							
E.	Threats						
F.	Vulnerabilities						
PROTECTION BY…							
G.	Mitigation (people, process, technology)						
H.	Training and education						
RESPONDING THROUGH…							
I.	Notification processes						
J.	Mitigation processes						
K.	Initiation of response, recovery and contingency plans						
RECOVERY BY…							
L.	Incorporation lessons learned into all areas after an exercise or incident						

The intent of this question is to ascertain the HCO's effort to ensure their cybersecurity risk management efforts remain current. This question follows the components of the NIST framework.

The **Identify** Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.
The **Detect** Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.
The **Protect** Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services.
The **Respond** Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact.
The **Recover** Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents.

www.nist.gov/cyberframework

(PDF-016) How often does your organization conduct each of the following?
(Check one per row; Leave blank if not conducted)

A. Assessments

		Weekly	Monthly	Quarterly	Every 6 Months	Less than Annually	Annually /As Requested
A.	An inventory of all 3rd parties/ business vendors						
B.	The ranking of business vendors based on the potential risk they pose your organization						
C.	An evaluation of high-risk vendors						
D.	An assessment of sub-contractors used by our business vendors						

B. Audits/tests

A. Unannounced vulnerability scans
B. Unannounced wireless penetration tests
C. System/application access audits

C. Exercises

A. IT/Security
B. Red/Blue Team Exercises
C. Enterprise
D. Tabletop exercises or drills

The intent of this question is to ascertain that the HCO

- conducts key varied cybersecurity information assessments/audits & tests/exercises
- the frequency by which the aforementioned are conducted.

ASSESSMENTS

A. An inventory of all 3rd parties/ business vendors

At any given time, organizations should be able to review a complete list of all vendors and their services as a first step in understanding the risks associated with third party vendors. Lack of a vendor inventory list is potentially a sign of an immature third-party program and could mean that an organization is opening itself up to significant risk.

B. The ranking of business vendors based on the potential risk they pose your organization

Vendor ranking or tiering is a method of classifying vendors based on the level of security risk they introduce to an organization. The level of security criticality decreases with each subsequent level. The number of tiering levels depends on personal preference. The basic vendor tiering structure is comprised of three levels: Tier 1, Tier 2, Tier 3, where Tier 1 represents high-risk vendors. Each vendor could be assigned to a tier manually, or the process could be based on a security questionnaire scoring system.

C. An evaluation of high-risk vendors

If not properly evaluated and managed, third-party vendors can entail considerable risks to partnering organizations. Each vendor can have a different type of risk such as strategic risk, compliance risk, operational risk and so on. Overlooking these risks can expose enterprises to a data breach or compliance issues.

D. An assessment of sub-contractors used by our business vendors

A vendor/contractor works directly with the HCO and is responsible for overall completion of a contracted project/promised deliverable. A subcontractor works with the vendor/contractor.

AUDITS/TESTS

A. Unannounced vulnerability scans

In an unannounced vulnerability scan, the vulnerability assessment team gives no prior intimation to the target staff. It's kind of a surprise test scan with the intent of examining the security preparedness and responsiveness of the HCO.

B. Unannounced wireless penetration tests

The unannounced Penetration test is done to see the target network in it's "natural" state; the way the security and system admins have it patched or unpatched with the current patches and fixes.

C. System/application access audits

An application control audit is designed to ensure that an application's transactions and the data it outputs are secure, accurate and valid.

EXERCISES

A. IT/Security

The IT/cybersecurity exercise involves the selection of a scenario or case-study limited to the IT operations of the HCO through which a hypothetical cyber incident is introduced to exercise participants.

B. Red/Blue Team Exercises

A red team v. blue team is a training exercise conducted by an organization to test their own cybersecurity defenses. The exercise is made up of attackers (the red team) and defenders (the blue team), and cybersecurity protocols, defenses, and responses are tested through a variety of pre-determined scenarios.

C. Enterprise

The enterprise exercise involves the selection of a scenario or case-study impacting the entire HCO through which a hypothetical cyber incident is introduced to exercise participants.

D. Tabletop exercises or drills

Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios.

(PDF-017) How would you characterize the adoption of the following types of security authentication measures used by your organization to authenticate/manage authorized users?

(Check one per row)

Fully Adopted: A condition where the technology/solution has been implemented organization wide to impact intended users per organization policy and the technology/solution is being used 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 is not impacting the intended users 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 and 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. Knowledge-based authentication measures (passwords)			
B. Possession-based authentication measures (something the user has like a one-time password sent to the user’s cell phone; USB keys)			
C. Inherence-based authentication measures (biometrics)			
D. Location-based authentication measures (geolocation security checks)			
E. Behavior-based authentication measures (picture selection)			
F. Multi-factor authentication for remote connections			
G. Multi-factor authentication for internal network connections			

The intent of this question is to determine;

- The array of authentication measures used by HCOs, and
- The pervasiveness of multi-factor authentication as a security tactic in HCOs.

A. Knowledge-based authentication measures (passwords)

Knowledge-based authentication, also known by its acronym KBA, is an authentication method based on a series of knowledge questions that are used to verify a person's identity in order to prevent access of an unauthorized person to a place or most commonly today, to an account..

B. Possession-based authentication measures (something the user has like a one-time password sent to the user’s cell phone; USB keys)

An authentication based on what the user has, such as memory cards and smart card tokens. Possession-based authentication is also referred to as token-based authentication.

C. Inherence-based authentication measures (biometrics)

Inherence factors authenticate access credentials based on factors that are unique to the user. These include fingerprints, thumbprints, and palm or handprints. Voice and facial recognition and retina or iris scans are also types of inherent authentication factors.

D. Location-based authentication measures (geolocation security checks)

Location-based authentication is a special procedure to prove an individual's identity on appearance simply by detecting its presence at a distinct location. To enable location-based authentication, a special combination of objects is required.

E. Behavior-based authentication measures (picture selection)

Behavioral authentication is an authentication mechanism that uses a person's unique movement characteristics to determine whether to grant access or not.

F. Multi-factor authentication for remote connections

An authentication system applied to remote connections requiring more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.

G. Multi-factor authentication for internal network connections

An authentication system applied to internal network connections requiring more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.

(PDF-018) How would you characterize the adoption of the following security measures used by your organization to authenticate/manage devices accessing your network?
(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 and 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. Control inventory of **non-medical devices** authorized to access our network			
B. Control inventory of **medical devices** authorized to access our network			
C. Control inventory of **mobile devices** authorized to access our network			
D. Inventory personal devices accessing our network			
E. Approve devices accessing our network			
F. Monitor devices accessing our network			
G. Approve users accessing specific device			

The intent of this question is to determine the array of security controls used by HCOs in authenticating and/or managing devices attempting to access their network, and the extent to which they are used throughout an organization.

A. Control inventory of non-medical devices authorized to access our network

Non-medical devices are all devices that do not meet the definition (of a medical device) as set out in the Medical Device Directive, Article 3(1).

B. Control inventory of medical devices authorized to access our network

Medical devices are all devices that meet the definition (of a medical device) as set out in the Medical Device Directive, Article 3(1). Medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers, and closed loop artificial pancreas systems. Additionally, medical devices include in vitro diagnostic (IVD) products, such as reagents, test kits, and blood glucose meters.

C. Control inventory of mobile devices authorized to access our network

Mobile Devices means tablets and smartphones running mobile operating systems (e.g., iOS, Blackberry OS, Android, or Windows Mobile operating systems). Laptops are not considered to be Mobile Devices. Mobile Devices means tablets, smartphones and similar devices running mobile operating systems.

D. Inventory personal devices accessing our network

Personal Devices means any device, owned by an individual, with the capability to process, store or transmit information independently. This includes, but is not limited to, mobile phones, smartphones, tablets, PCs, laptops and cameras.

E. Approve devices accessing our network

Involves a software-based access control system with a user interface which manages the entry and exit of carriers, based on functional rules controlling access rights.

F. Monitor devices accessing our network

Network monitoring tools collect data in some form from active network devices, such as routers, switches, load balancers, servers, firewalls, or dedicated probes, which they analyze to paint a picture of the network's condition.

G. Approve users accessing specific device

A security control which gives Administrators the ability to require approval before a user's device can sync data.

(PDF-019) How would you characterize the adoption of the following capabilities your organization uses as part of your organization's security processes?
(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 and 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.

A. Technical security capabilities

	Fully Adopted	Partially Adopted	Not Adopted
A. Encryption			
B. Data loss prevention (DLP)			
C. Intrusion prevention or detection systems (IPS, IDS)			
D. Security Information and Event Management (SIEM) system			
E. Next generation endpoint protection systems; EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), EPP (Endpoint Protection Platform)			
F. Network segmentation			
G. Network monitoring and analytics			
H. Cloud access security broker (CASB)			

B. Data protection capabilities

	Fully Adopted	Partially Adopted	Not Adopted
A. Database monitoring			
B. Privacy monitoring/auditing systems (end-user behavior analytics)			
C. Basic spam/phishing protection (signatures, digests, spam blacklists, etc.)			

C. Process control capabilities

	Fully Adopted	Partially Adopted	Not Adopted
A. Log management			
B. Governance, risk, and compliance (GRC) systems			
C. Vulnerability management			

The intent of this question is to determine the array of capabilities the HCO has instituted as part of their security efforts.

Technical security capabilities

A. Encryption

Encryption in cyber security is the conversion of data from a readable format into an encoded format. Encrypted data can only be read or processed after it's been decrypted. Encryption is the basic building block of data security.

B. Data loss prevention (DLP)

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations.

C. Intrusion prevention or detection systems (IPS, IDS)

Intrusion detection and prevention are two broad terms describing application security practices used to mitigate attacks and block new threats. An IPS is used to identify malicious activity, record detected threats, report detected threats and take preventative action to stop a threat from doing damage. An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered

D. Security Information and Event Management (SIEM) system

Security information and event management (SIEM) is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

E. Next generation endpoint protection systems; EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), EPP (Endpoint Protection Platform)

Endpoint Detection and Response (EDR) is next generation antivirus protection and is also referred to as next gen AV. The EDR platforms continually monitor and respond to cyber threats. They are effectively a prevention against zero-day vulnerabilities including new or undetected malware.

Extended Detection and Response (XDR) is an enterprise cybersecurity solution that provides automated cyber threat detection and response through data visibility, threat intelligence, and big data analytics.

Endpoint Protection Platform (EPP) is a comprehensive security solution deployed on endpoint devices to protect against threats. EPP solutions are typically cloud-managed and utilize cloud data to assist in advanced monitoring and remote remediation.

F. Network segmentation

Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of network traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security.

G. **Network monitoring and analytics**

Network monitoring is an IT process that continuously monitors and evaluates a computer network and its assets. A network monitoring system proactively identifies and remediates slow network traffic or inadequate network components to ensure network integrity is maintained.

H. **Cloud access security broker (CASB)**

Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

<u>Data protection capabilities</u>

A. **Database monitoring**

Database monitoring refers to the tasks associated with examining the operational status of a database. Database monitoring is a vital activity for the maintenance of the performance and health of your database management system. Database monitoring offers the ability to gather essential database performance metrics to help optimize and tune database processes for high performance.

B. **Privacy monitoring/auditing systems (end-user behavior analytics)**

User and entity behavior analytics (UEBA or entity behavior analytics) is cybersecurity technology that uses monitoring tools to gather and assess data from user activity, with the goal of proactively finding and flagging suspicious behavior before it leads to a data breach.

C. **Basic spam/phishing protection (signatures, digests, spam blacklists, etc.)**

A spam filter is a program used to detect unsolicited, unwanted and virus-infected emails and prevent those messages from getting to a user's inbox. Like other types of filtering programs, a spam filter looks for specific criteria on which to base its judgments.

Phishing is when attackers send malicious emails designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials or other sensitive data.

<u>Data protection capabilities</u>

A. **Log Management**

Log management is the practice of continuously gathering, storing, processing, synthesizing and analyzing data from disparate programs and applications in order to optimize system performance, identify technical issues, better manage resources, strengthen security and improve compliance.

B. Governance, risk, and compliance (GRC) systems

Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption.

C. Vulnerability management

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems.

(PDF-020) How would you characterize the adoption of the following security processes your organization currently uses to safeguard information?
(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 and 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. Encryption at rest (device encryption)			
B. Encryption in motion (data sent outside an organization's firewall)			
C. Medical device password/access controls			
D. Consumption of threat intelligence information from other organizations (ISAC, ISAO, DHS, etc.)			
E. Procurement/contracting with security firm including vendor risk assessment			
F. Segmentation of medical devices on specialized network segments			
G. 24/7/365 Security operations center (insourced, outsourced, hybrid)			
H. Data classification			
I. Secure system baseline images			
J. Privilege access management			

The intent of this question is to determine the array of security processes the HCO has instituted as part of their security efforts, and the extent to which they are used throughout the organization.

A. Encryption at rest (device encryption)

Data at rest refers to data residing in computer storage in any digital form. This data type is currently inactive and is not moving between devices or two network points. No app, service, tool, third-party, or employee is actively using this type of info. Encryption at rest is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. If an attacker obtains a hard drive with encrypted data but not the encryption keys, the attacker must defeat the encryption to read the data.

B. Encryption in motion (data sent outside an organization’s firewall)

“Data in motion” refers to data traveling from one location to another. Many different kinds of networks can be utilized for data transportation in this way. Data in motion must be protected in order to increase the security of a network because a network often consists of several nodes with numerous clients interconnected to the same network. This procedure is known as encryption.

C. Medical device password/access controls

Configurable access controls (such as the use of username and password) to help ensure that only trusted users can gain access to networked medical devices and the sensitive PHI with which they interact. These access controls help align medical devices more tightly with the National Institute of Standards and Technology (NIST)’s cybersecurity best practices for protection, detection, and remediation.

D. Consumption of threat intelligence information from other organizations (ISAC, ISAO, DHS, etc.)

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources. Threat intelligence services are designed to gather data across the global landscape of potential cyber threats, including existing and emerging threats and cybercrime actors, using state-of-the-art tools and methods.
NOTE: PDF-015 is associated to this question

E. Procurement/contracting with security firm including vendor risk assessment

Cyber security firms deal with processes, monitoring, and alerts to help an HCO keep critical systems online as well as resume lost operations and systems after an incident. The contract firm will also conduct an assessment into the risks the HCO faces when using third-party vendors' products or services.

F. Segmentation of medical devices on specialized network segments

Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of network traffic between subnets based on granular policies.

G. 24/7/365 Security operations center (insourced, outsourced, hybrid)

Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

H. Data classification

Data classification is the process of organizing data into categories that make it easy to retrieve, sort and store for future use. A well-planned data classification system makes essential data easy to find and retrieve. Written procedures and guidelines for data classification policies should define what categories and criteria the organization will use to classify data. They also specify the roles and responsibilities of employees within the organization regarding data stewardship. Once a data classification scheme is created, security standards should be identified that specify appropriate handling practices for each category. Storage standards that define the data's lifecycle requirements must be addressed, as well.

I. Secure system baseline images

A baseline identifies an agreed-to description of the attributes of a system at a point in time and provides a known configuration to which changes are addressed. Establishing baselines and managing changes to baselines are the key functions of configuration management.

J. Privilege access management

Privileged access management (PAM) is an identity security solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources. Privileged access management helps organizations make sure that that people have only the necessary levels of access to do their jobs. PAM also enables security teams to identify malicious activities linked to privilege abuse and take swift action to remediate risk. In digital business, privileges are everywhere.

(NEW-021) How would you characterize the deployment of Artificial Intelligence based solutions to support your cybersecurity efforts in each of the following areas?

Artificial Intelligence: A system that may utilize machine learning and predictive analytics to assess a situation and either recommend or take actions that maximize chances of success/positive outcomes.

Deployed: A condition where the technology/solution has been tested and integrated into the organization's cybersecurity efforts and the relevant users are utilizing the technology/solution as intended per industry expectations and organizational policy.

Piloting: A condition where the technology/solution is being tested to be included as part of the organization's cybersecurity effort.

Not Supported: A condition where the organization has not yet tested the technology/solution, has no intention of testing/implementing the technology/solution at this time or has not yet achieved funding approval for the acquisition of the technology/solution.

(Check one per row)

	Deployed	Piloting	Not Supported
A. App security			
B. Cloud security			
C. Endpoint security			
D. Identity and Access Management (IAM) security			
E. Network security			

The intent of this question is to determine how the HCO is using AI to support the security of varied vulnerabilities within the HCO.

A. App Security

Application security includes all tasks that introduce a secure software development life cycle to development teams. Its final goal is to improve security practices and, through that, to find, fix and preferably prevent security issues within applications.

B. Cloud Security

Cloud computing security or, more simply, cloud security, refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing.

C. Endpoint Security

Endpoint security or endpoint protection is an approach to the protection of computer networks that are remotely bridged to client devices. The connection of endpoint devices such as laptops, tablets, mobile phones, Internet-of-things devices, and other wireless devices to corporate networks creates attack paths for security threats. Endpoint security attempts to ensure that such devices follow a definite level of compliance to standards.

D. Identity and Access Management (IAM) security

Identity and Access Management (IAM) security is an essential part of overall IT security that manages digital identities and user access to data, systems, and resources within an organization. IAM security includes the policies, programs, and technologies that reduce identity-related access risks within a business. IAM programs enable organizations to mitigate risks, improve compliance, and increase efficiencies across the enterprise.

E. Network Security

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Section 5: Security Insurance

(PDF-022) Which of the following cybersecurity related insurance coverages does your organization currently carry? (ACUTE/AMBULATORY/LTPAC)
(Check all that apply)

A. Cyber liability
B. Data breach
C. Crime insurance coverage
D. Business loss
E. Network security and privacy
F. Media liability (coverage for intellectual property infringement resulting from the online advertising of an organization's services, to include social media posts)
G. Natural disaster
H. We are self-insured

The intent of this question is to determine the array of cybersecurity insurance coverages HCO's carry.

A. Cyber liability

A policy to mitigate a businesses' financial risk exposure by offsetting costs related to damages and recovery after a data breach, ransomware attack, or another cybersecurity incident.

B. Data breach

Data breach insurance only offers first-party coverages for losses related to a data breach, hack, or theft of company documents. The policies generally cover expenses associated with informing parties affected by a breach to minimize the damage.

C. Crime insurance coverage

Crime Insurance and Financial Institution Bonds provide coverage for loss of money, securities, or other assets resulting from acts such as employee theft, certain types of fraud by third parties (forgery, for example), theft of property from the premises, and social engineering (impersonation fraud). Crime policies cover the direct loss of your funds, whether through maleficence, employee dishonesty or social engineering whereas cyber liability policies cover economic damages arising through a failure of network security or privacy controls which may cause indirect losses.

D. Business loss

Cyber insurance generally covers a business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records.

E. Network security and privacy

Network Security and Privacy Liability protects the Insured against losses for the failure to protect a customer's personally identifiable information (SSN, credit card numbers, medical information, passwords, etc.) via theft, unauthorized access, viruses, or denial of service attack.

F. Media liability

Coverage for intellectual property infringement resulting from the online advertising of an organization's services, to include social media posts.

G. Natural disaster

Natural disaster coverage protects a business from natural disasters such as earthquakes, floods and hurricanes, and even extends protections into human-made disasters such as terrorism. In the context of cybersecurity, it is the act of doing something designed to destabilize a country or to use pressure on a government by using methods defined in the category of computer crimes. It is applicable to carry out three types of actions against an information system, such as physical, syntactic attack and semantic attack.

H. We are self-insured

Self-insurance typically involves putting aside funds on an organization's balance sheet to cover future expenses stemming from a cyber incident or writing cyber risks through an organization's captive insurer.