FEATURE

Secure Your Epic Environment

Optimize you audits

By Paul Hinds

Electronic health records (EHRs) have been widely adopted to provide accurate and complete information about patients at the point of care, to facilitate coordinated care, to lower costs through decreased paperwork, and to reduce duplication of testing. Epic has established a dominant position in the EHR field, with its software holding most patient medical records in the U.S. Internal auditors need to determine that the configuration of Epic complies with Health Insurance Portability and Accountability Act (HIPAA) security requirements.

Epic is interested in helping their customers improve their return on investment on their product by providing an Executive Packet (EP) feature that provides metrics, maturity and benchmarking comparisons to similar organizations for as many as 16 topical areas. The EP indicates how many features your organization has turned on and, based on your peers' outlines, which items to implement next. Many EP metrics are intended to measure and increase clinician use and efficiency with the EHR, and benchmark revenue cycle performance.

One section of the EP summarizes the activation status of Epic security features that are available to protect electronic protected health information (ePHI). The section allows you to compare your organization's use of Epic security features to the Epic community (customer base) and identify important features to implement.

Epic security audit approach

1. Develop an ePHI application audit program, mapped to the HIPAA security requirements
2. Develop an Epic security audit program
3. Map Epic controls to ePHI application audit framework
4. Assess effectiveness of Epic-enabled controls
5. Evaluate non-enabled Epic controls for risk and mitigating controls
6. Identify and evaluate ePHI systems and controls outside of Epic
7. Provide input to the HIPAA security risk assessment

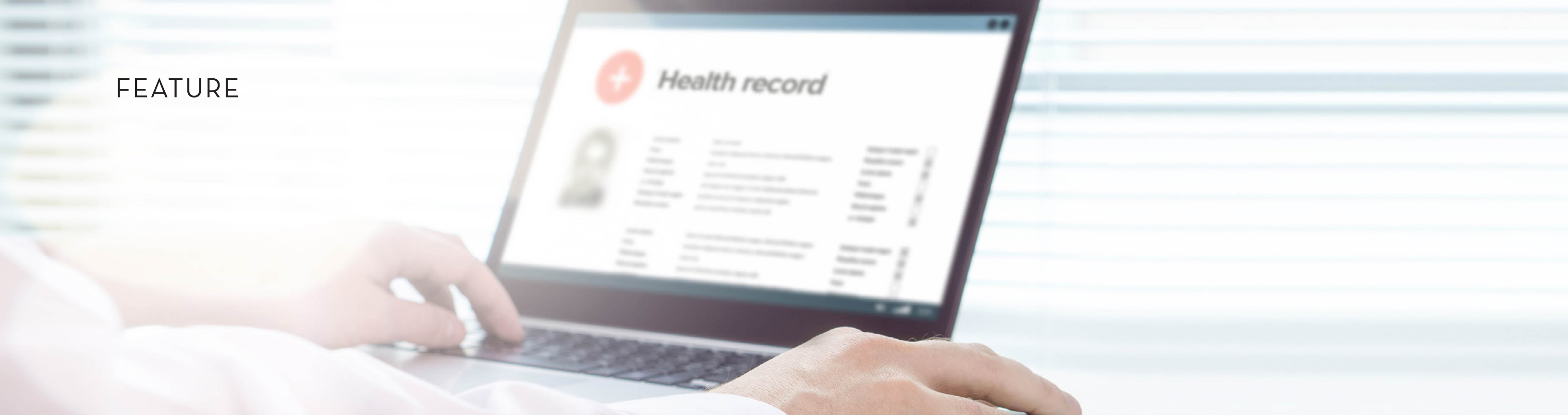
Optimize your Epic security

The EP "outlines key features and best practices for securing your Epic environment based on Epic's knowledge of your system configuration and supporting infrastructure. It helps you understand which features you are using, which recommendations you are following, and it gives you a benchmark for how you compare to the rest of the Epic community."[1]

The expanded use of telehealth and more remote access due to Covid-19 has increased the threats to your EHRs. With budgets limited, you are being asked to maximize the benefit from the controls that your organization already has, rather than make additional investments for new solutions and increased complexity. Leveraging the security and privacy controls that come with the technologies, systems and services you use will usually provide the best return to your organization.

Historically, internal auditors have primarily performed information technology general controls (ITGC) assessments on Epic. The audits covered traditional process controls such as change management, as well as extensive audits around roles and responsibilities, with the goal of limiting

[1] EPIC, Executive Packet, 2020



access and ensuring appropriate segregation of duties. The audits supported both the organization's HIPAA security requirement compliance as well as some of the HIPAA privacy compliance requirements, including need-to-know, business associate agreements and consent. However, the ITGC audits usually do not identify and assess all of the technical vulnerabilities and risks in your Epic environment.

Epic security audit program

To effectively assess the highest control risks, you must go deeper into the automated controls that protect your organization's ePHI data within Epic. The Securing Your Epic Environment section of the EP provides insights into the six security capabilities in Exhibit 1, which cover 41 available controls.

Exhibit 1 – Epic security categories

1. Access and auditing – 9 controls
2. Application and infrastructure – 8 controls
3. Cogito Systems – 6 controls
4. Interconnect web services security – 4 controls
5. MyChart patient access – 9 controls
6. Operational database – 5 controls

The EP provides your organization with an accounting of the features and controls that are enabled, and the community adoption rate (CAR) of that feature or control (i.e., the percentage of organizations that have turned on the feature). You can use this data to develop a better understanding of your Epic environment and build an Epic security audit program specific to your organization that complements your ITGC and privacy audits.

Develop an ePHI application audit plan

You may already have an inventory of control areas to assess for each ePHI application that maps the HIPAA security requirements into a framework unique to your organization. If not, Exhibit 2 is a list of potential control areas that can be used.

Place these control areas and corresponding controls in a spreadsheet to document your audit coverage of critical ePHI systems and the HIPAA security requirements over a multiyear period (e.g., four to five years). You can come back to these audit areas as part of your periodic audit planning process and evaluate the cadence of your rotation testing schedule.

Develop an Epic audit plan

Begin constructing your Epic security audit program by mapping your ePHI audit program assessment areas to the Epic controls provided in the EP. The mapping should

Exhibit 2 – ePHI application audit areas

Access controls	Access provisioning	Termination procedures
Periodic access review	Sensitive access/segregation of duties	Emergency access
Privileged access	Person or entity authentication	Third-party access
Access authentication/passwords	Event logging and monitoring	Change management
Computer operations (interface, backups)	Disaster recovery	Transmission security/encryption
Protection from malicious software	Incident response and reporting	Encryption and decryption
Disposal	Business continuity	Threat and vulnerability management

Compare your organization's use of Epic security features to that of the Epic customer base.

Exhibit 3 – Mapping the ePHI audit area to Epic feature to HIPAA requirement – Example

ePHI application audit	Epic EP details			HIPAA security requirement		
Area	Category	Subcategory	Additional details	HIPAA §	HIPAA description	Regulatory requirement
Access	Access and auditing	Access logging extracted from all PHI environments	You can extract auditing data from all your PHI environments to your production Epic Clarity database to monitor access. Work with your Epic Cogito Systems technical support to extract the appropriate information.	164.312(b)	Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use (ePHI).

provide a clear alignment to the ePHI audit program you have, as well as to the HIPAA security control requirements that each control area addresses.

For example, the EP access and auditing control—Access Logging Extracted for All PHI Environments—should be mapped to HIPAA § 164.312(b) – Access Controls. By mapping all controls, Epic-specific or others, you can show a multi-year picture of the assessed and unassessed controls. The mapping is also an important input to your organization's annual HIPAA risk assessment. Exhibit 3 gives an example of the mapping.

Execute the Epic audit plan

When reviewing the Epic EP for security, you will reference a series of summary tables for each of the six areas in Exhibit 1.

Using access and auditing as an example, Exhibit 4 shows an example of the summary table.

Exhibit 4 – Epic EP access and auditing summary table

	Access And Auditing	Community Adoption Rate
ON	Access Logging Extracted from All PHI Environments	74%
ON	Administrative Security Classes Implemented	63%
ON	Auto-Deactivate Users in Copies of Production	38%
ON	Command Prompt Auditing Enabled	94%
ON	Epic Employee Check in Production	78%
ON	Generic Accounts Deactivated in PHI Environments	70%
ON	Secure After-Hours Process	98%
OFF	Single Sign-On Enabled for UserWeb Access	34%
ON	Two-Factor Authentication Required for Epic Employee Access	92%

Source: Epic Executive Packet – 2020

Exhibit 5 – Epic EP enabled control example

Control	Enabled?	Community adoption rate	Additional details
Access logging extracted from all PHI environments	On	74%	You can extract auditing data from all your PHI environments to your production database to monitor access. Work with your Epic Cogito Systems technical support to extract the appropriate information.

Source: Epic Executive Packet – 2020

For the nine security control areas noted in Exhibit 4, eight have been enabled and most of the enabled controls have a high adoption rate in other healthcare organizations. When controls have a high adoption rate among peer organizations but are not enabled in your organization, determine why they have not been enabled.

The single sign-on control could be disabled for a valid reason, but you need to find out why the control is not enabled. A CAR of less than a 50 percent may suggest that other areas with higher CARs need your attention first.

Assess enabled controls

Select the controls that are already implemented for further assessment. However, be aware that controls that are identified as enabled may not be fully operational or effective. For example, Exhibit 5 indicates a control that is enabled in Epic.

You find that Epic access logging to provide a security audit trail is enabled for the PHI environments to capture changes to user security and roles, and the logs are retained in the analytics tool. But your further testing and inquiry determine that the control is not fully operational: the manager of applications indicates that the data are not used by the security team for any monitoring activities.

Test each enabled control to ensure the output or intent of the control is realized. In the access logging example, although audit data was being extracted, the data were not being used by the security team in their monitoring tools and processes. As a result, the value and importance of having this audit information was not fully realized.

You should repeat this process for all the controls that Epic has identified as enabled, so that you fully understand the effectiveness of each control, and whether additional controls are needed.

Assess non-enabled controls

For the controls that are not enabled, determine if mitigating controls exist outside of Epic or if these non-enabled security features represent control gaps. Start with the highest CAR controls and conduct in-depth interviews with the various infrastructure and technology owners to gain an understanding of how controls operate in place.

From your interviews, you can identify controls that were:

- Implemented through other third-party products
- Thought to cause performance problems and were not enabled
- Considered to be quick fixes and easy but were not implemented
- Are expected to take more time

If these discussions have never been held, you may provide a lot of useful risk and control insights to all interested parties—internal audit, IT infrastructure, IT security and risk management.

Exhibit 6 shows an example of a key control showing up in the Epic EP as not being enabled.

In this example, you would gain an understanding through further inquiry and inspection of whether this control is

Exhibit 6 – Epic EP feature not enabled

Category	Category/key features	Enabled?	Community adoption rate	Additional details
Application and Infrastructure	Hyperspace browser whitelist	Off (critical feature)	83%	Use the hyperspace browser whitelist to control users' access to external websites from within hyperspace.

Source: Epic Executive Packet – 2020

Map your ePHI audit areas and Epic features to the HIPAA requirements.

For Epic controls that are not enabled, determine if mitigating controls exist outside of Epic.

addressed. You could inquire of the Epic applications manager who indicates that the action whitelist is enabled, but the navigation whitelist is not, and no organizational policy or standard exists regarding whitelisting.

Depending upon your configuration, whitelist procedures could be split into three layers: one for Epic, one for Citrix, and one for web filters. You could note that the Epic whitelist has a standard message informing the end user that their request was blocked, access to modify the whitelist configuration is restricted, and access is reviewed quarterly.

You collect a screenshot of the web filter error message restricting access to an external site to demonstrate the whitelisting is enabled at the network layer. Also, you determine that the Epic browser whitelist setup and support guide confirms that external whitelisting outside of Epic on the network is an acceptable method for preventing access to external sites from within Epic.

Although the EP report indicated that this control is not enabled, your technical security auditing determined that the control is enabled adequately.

Future audits

Your audit of Epic security and mitigating controls will probably identify additional ePHI platforms, applications and supporting infrastructure that were not labeled as ePHI systems. Many of these systems are in the areas of data analytics, ancillary medical systems, connected medical devices and patient portals.

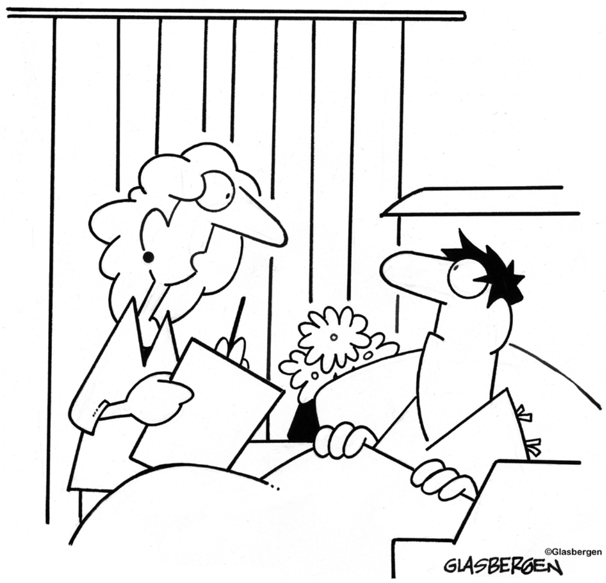
Use this valuable information for planning future audits. Your organization is responsible to identify other environments, connections or mitigating controls that an Epic scan cannot identify. You need to add these systems and devices to your ePHI audit plan and perform additional audits to confirm that the identified threats and security requirements are addressed.

Summary

To continue to provide assurance to your management and board of the protection of the ePHI that your organization has been trusted with, you need to understand the ITGCs, as well as the maturity of the security controls identified within your Epic EP.

By completing an Epic security assessment utilizing the Epic EP, you help ensure security compliance and add value by providing important input into your organization's annual HIPAA risk assessment process. **NP**

Paul Hinds specializes in cybersecurity, privacy and IT risk. He works with healthcare and life sciences companies providing internal audit, risk management, IT security and privacy services. Paul can be reached at Paul.Hinds@northwestern.edu and (224) 723-4817.



"Of course we're a good hospital! Could we charge $500 for an aspirin if we weren't?"

Nobody learned anything by hearing themselves speak.
- Richard Branson