FEATURE

Patient Monitoring in the Digital Age

Evaluate the risks and benefits of hands-off patient care

By Kelly Rollins, CISA, and Emily Carrere, CFE

The use of virtual hospital services (VHS) has become a growing trend in the healthcare industry. VHS programs provide opportunities for healthcare organizations to expand their services and provide 24/7 patient care, without a nurse being present in each patient room. However, these programs also create new operational and IT risks for the organization.

While like telehealth/telemedicine in some ways, virtual hospital services (VHS) differ in that they allow hospitals to use both remote and in-person monitoring for comprehensive and digitally enabled care. VHS includes the entire provision of care for the patient's stay in the hospital and is considered a real-time remote patient monitoring tool.

VHS is initiated by the bedside hospital care team to be carried out by teams at control centers and/or offsite locations (i.e., bunkers). These remote locations include human caregivers consisting of virtual providers, nurses, and various types of technicians, who use real time communication with bedside caregivers to provide patients with the best care.

This article will focus on three specific VHS programs: telesitter, telemetry monitoring and electronic intensive care unit (eICU); however, the same risks and considerations can be applied to other VHS programs.

Benefits of VHS programs

VHS programs are forecasted to grow, so it is important to understand the various benefits these programs can bring to an organization:

- Potential cost savings
- Improved care quality and patient safety
- Decreased negative outcomes, including minimized infection threats
- Operational efficiencies with higher patient volumes
- Support with nationwide staffing shortages and reduced workload for bedside caregivers
- Enhanced provider and patient communication
- Expanded access to specialty care providers
- Increased patient monitoring capabilities

Potential risks and audit considerations

Prior to conducting an audit of VHS programs, you should consider operational and IT risks that could impact the approach, scope, and timing of your audit.

Operational risks

Licenses, training and education

When conducting an audit in the VHS space, it's important to first understand the licensing, training, and education requirements for your healthcare organization. If remote providers or staff do not have proper training, education, or licensing, there is an increased risk to the organization for HIPAA violations or malpractice suits. You should review whether employees are required not only to complete education on the services provided, but also complete annual evaluations to confirm they are competent in performing their job duties.

Audit procedure examples

- Review job descriptions to ensure expectations have been established and include patient confidentiality as part of the job description.

VHS programs are forecasted to grow, so it is important to understand the various benefits these programs can bring to an organization.

A telesitter may complete a sitter assessment that would be housed in the patient's electronic medical record.

Definitions:

Bunker – an offsite or centralized (i.e., out of patient room) location where VHS services are performed and monitored.

Electronic intensive care unit (eICU) – ICU nurses remotely assist with bedside monitoring in ICU units.

Electronic protected health information (ePHI) – protected health information that is produced, saved, transferred or received in an electronic form. EPHI management and security are covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

Remote providers – providers in another location who assist bedside.

Telesitter – remote technicians monitor patients for adverse events via mobile cameras in patients' rooms. (Note: AvaSure's AI-augmented virtual sitting technology is branded TeleSitter®.)

Telemetry monitoring – cardiac monitoring for patients with cardiac complications.

- Validate that annual competency checks/evaluations have been completed.
- Confirm that remote contract providers have completed hospital-specific training and are licensed in the states in which they are providing services.

Informed consent and privacy

Another aspect to consider is informed consent. If patient consent is not received, the organization is at a greater risk for liability from medical errors.

Audit procedure examples

- Obtain regulatory and organizational requirements for patient consent (for example, language included, when it should be obtained, and retention requirements) and validate that the consent forms being used comply with those requirements.
- Ensure correct version of informed consent is used and determine who is responsible for substantiating consent.
- Review medical records to ensure proper patient consent.

Documentation review

Your audit should include a review of the documentation completed for each VHS service, which is commonly a flowsheet or note template. For example, a telesitter may complete a sitter assessment that would be housed in the patient's electronic medical record (EMR) and would contain documentation of encounters with the patient (for example, when the patient left the room or was discharged).

Audit procedure examples

- Determine documentation requirements, considering specific regulatory and reimbursement requirements.
- Verify that the current and approved documentation is contained in the EMR for every encounter.
- Review medical records to ensure all required documentation was obtained.

Designation and communication

Communication between the bunker and bedside is vital to ensuring complete patient care coordination. The key to testing this is observation. You should ask similar questions

in both spaces to ensure controls are operating effectively and consistently.

Audit procedure examples

- Verify that staff know the criteria to designate a patient for VHS services.
- Verify that staff know how orders should be placed, received and documented.
- Confirm communication occurs when patients are given medications that may alter their vitals, if patients are being transferred or discharged, and if devices are available for use.
- Confirm there is a backup communication process in case of telecommunications interruption.

Parameters and monitoring

Without proper patient-specific monitoring parameters in place (for example, heartrate parameters should be based on a patient's condition, not a generic baseline), remote monitoring alerts may be ineffective. This could result in technicians being less responsive to alerts and overlooking vital communication between bunker and bedside. Among other hazards, such inconsistent monitoring could increase a patient's fall risk.

Audit procedure examples

- Review system log-on process performance.
- Identify how parameters are determined, who is responsible for implementing them, and how changes are made.
- Review processes to communicate parameter limits to appropriate personnel.
- Perform onsite walkthroughs to assess how patients are monitored during bunker shift change to ensure continuous patient monitoring.

IT Risks

Given the reliance VHS programs have on technology, it is critical to have a thorough understanding of the IT environment prior to beginning an audit of VHS programs. This includes hardware/devices, software applications and user access.

Applications and devices

While the IT risks might be similar across VHS programs, the applications and devices utilized to support these programs could vary. As such, it is important to work with business process owners and/or the IT department during the audit planning process to develop an inventory of the applications and devices that support the VHS programs within the scope of your engagement.

During this process, auditors should work with the IT department to determine if any of the applications identified in your inventory are technically medical devices with control limitations that need to be considered in the testing plan. For example, medical devices might not support multiple user logins or have robust audit logging/monitoring capabilities. Auditors might consider performing a distinct audit of medical devices and ePHI HIPAA compliance.

Once the inventory of applications and devices is compiled, consider the following risk areas.

User Access

As applications and devices are being utilized to support patient care, it is important to ensure access is limited to authorized personnel based on business need and that user access reviews are conducted periodically.

Audit procedure examples

- Ensure roles and responsibilities for managing access to VHS applications and devices have been defined, documented, and communicated. Determine who is responsible for managing access (for example, business process owners, IT, and/or vendors) and ensure they understand their role in the process.
- For applications, determine the hosting location—is the application being hosted locally by your organization or is it being hosted by the vendor? If vendor-hosted, request and review an independent assessment report, such as SOC, HITRUST or ISO.
- Determine if the application is integrated with your organization's active directory system and how

Given the mobility of VHS hardware assets, it is important to ensure devices are stored in secured locations.

While the IT risks might be similar across VHS programs, the applications and devices utilized to support these programs could vary.

authentication and authorization are managed. Consider performing a detailed review of the user listings.

- Evaluate vendor access to applications and devices if applicable.

Audit logging and monitoring

As VHS programs are centered around patient monitoring activities, work with the business process owners to determine what audit logging and monitoring functionality should be enabled. This includes understanding if video recordings are taking place during patient encounters and if so, how those recordings are being stored and maintained in VHS applications and devices. If patient encounters are not being recorded via video, business process owners might heavily rely on detailed audit logs for monitoring purposes—this increases the need to ensure that strong audit logging and monitoring controls are enabled.

Audit procedure examples:

- Evaluate whether audit log retention aligns with business needs.
- Determine how audit logs are being reviewed, including the frequency, who performs the review, and evidence to support the process.
- Ensure appropriate audit log configurations are enabled.
- Determine who can access, modify and delete audit logs and evaluate the appropriateness of the process.
- Discuss vulnerabilities to cyberattacks and resulting data breaches with the security officer.

Configuration

Configuration management is important to ensure applications and devices are configured appropriately, and access to modify configuration settings is limited.

Audit procedure examples

- Determine if any VHS applications or devices are configured to record patient encounters (for example, patient video or audio is being recorded)—if so, ensure this has been approved by your legal and compliance teams, including the HIPAA privacy and security officer(s).
- Identify critical configuration settings and ensure access to modify these settings is restricted to authorized personnel.
- Determine what type of alerts should be enabled and ensure notifications are being sent to appropriate individuals in an effective manner (for example, alerts are not sent to an unmonitored email address).
- Conduct physical walkthroughs to observe the applications and devices in use and determine if configuration settings are accessible to end users.

Asset management and physical security

While applications play a critical role in supporting VHS programs, the physical hardware used to support these applications and facilitate VHS processes is equally critical—this includes cameras, monitors, telemetry devices, etc. It is important to ensure effective processes are in place to

Key Takeaways

- Ensure an effective communication plan has been established in VHS programs.
- Confirm employee certifications and trainings are up to date.
- Be aware of alert fatigue and its potential impacts on program effectiveness.
- Understand the difference between applications vs. devices and the associated regulatory requirements.
- Ensure roles and responsibilities have been defined and documented.
- Understand device recording capabilities and seek legal guidance from general counsel and the privacy officer.
- Review vendor contracts and independent assessments.

Ensure roles and responsibilities for managing access to VHS applications and devices have been defined, documented, and communicated.

manage and secure hardware in the healthcare provision/bedside and monitoring/bunker locations.

Audit procedure examples

- Determine who is responsible for managing hardware assets (monitoring team, facility personnel, vendor, or a combination of these groups). Ensure roles and responsibilities are defined, documented, and communicated to all groups involved in VHS program management.
- During physical walkthroughs, determine where hardware assets are stored and what security mechanisms are in place to safeguard the storage locations (for example, badge readers, pin-codes, key locks). Given the mobility of VHS hardware assets (for example, cameras on wheels or remote telemetry boxes), it is important to ensure devices are stored in secured locations and HIPAA encryption requirements are met.
- If badge readers are utilized to secure monitoring locations and/or locations in which hardware assets are stored, consider a badge access review to ensure only appropriate personnel have access.

Vendor management

If your organization uses third parties to support VHS programs/processes, it is critical to ensure contractual agreements exist and include required supporting documentation such as business associate agreements and nondisclosure agreements.

Audit procedure examples

- Ensure vendor roles and responsibilities are clearly defined, documented, and communicated to VHS program team members.
- Review contracts and supporting documents and confirm with your legal team that they are complete based on the services provided.
- If vendor support includes software as a service with a hosted application, request and review independent attestation reports (for example, SOC report, HITRUST, ISO Certification).

Conclusion

An audit can help your organization minimize the risks of new or expanding virtual hospital services while maximizing the benefits of this evolving service structure. **NP**

Kelly Rollins, CISA, IT Director, and Emily Carrere, CFE, Senior Auditor, work for Ochsner Health based out of New Orleans, La. You can reach Kelly at Kelly.Rollins@ochsner.org and Emily at Emily.CarrereTrevino@ochsner.org.

Kindness is the language which the deaf can hear and the blind can see.
– Mark Twain