Pharmacy Cyber Intrusion Preparedness Toolkit

Updated as of May 13, 2021

Introduction

Vizient has created a toolkit to provide pharmacy member guidance to prepare for a cyber intrusion. Events of this type have been steadily increasing over the past number of years and this has accelerated during the COVID-19 pandemic. Thoughtful planning and mitigation strategies can serve to strengthen readiness, resilience, effective response and recovery in the instance of an attack.

For questions regarding this content, please contact us at pharmacyquestions@vizientinc.com.

Considerations

Identify system vulnerabilities	
☐	Create a list of software applications used in the delivery of patient care including, but not limited to: • Operational: carousel, ADC, IV room compounding, EHR, RFID, temperature monitoring, repackaging, inventory management, compounding logs, assessment of risk documents, diversion mitigation, electronic room access. • Clinical: patient monitoring, laboratory data, patient selection/identification, profile management, high-risk medication management, antimicrobial stewardship, PN ordering, order sets, protocols, drug information, hand-off communication, intervention documentation, REMS programs, medication error/ADE reporting • Administrative: staffing schedule, policies and procedures, payroll system, training & education, staff on-boarding, communications, 340B split billing
☐	Assess vulnerability risk for each software application based on downtime duration. • ≤ 24 hours • 1-7 days • 1-4 weeks • ≥ 4 weeks
☐	Assess organizational change control process to evaluate inclusion of downtime procedures.

Contingency planning	
☐	Evaluate contingency plan for each software application/downtime duration match.
☐	Establish a departmental downtime manual.
☐	Create a paper backup system for each potential vulnerability point inclusive of a replenishment strategy.
☐	Consider purchase of a standalone PC or laptop and local access printer (not connected to network).
☐	Ensure routine backup procedures for all systems, including standalone PCs or laptops.
☐	Build redundancies into systems where able (e.g. medication and supply ordering applications, printed references).
☐	Establish education plans for the use of paper systems for clinicians not familiar with these processes (e.g. “how to write a complete medication order”, “how to write a paper prescription”, “how to use a paper MAR”).
☐	Establish a communication strategy for the notification of staff and internal and external customers which can be modified to address the scope and projected duration of the event.
☐	Ensure alternative communications capabilities between departments (e.g. fax machines, pagers, cell phones, secure texting)
☐	Collaborate with nursing in developing a process for communicating admission, discharge and transfer of patients to ensure accurate patient locations.
☐	Ensure a mechanism for the communication of prescriber orders in need of clarification prior to nursing administration.
☐	Establish and maintain a list of key vendors and contact numbers.
☐	Assess high risk medications that should not be available via critical override with consideration for patient specific dispensing from pharmacy.

☐	Estimate and anticipate surge in need for paper prescription pads during downtime; include plans for replenishment.
☐	Anticipate needs for auxiliary labels, batch labels, master formulation records (sterile & non-sterile), and production logs.
☐	Create a plan for internal ordering (e.g. clinic floor stock).
☐	Anticipate support for patient assistance program management.
☐	Develop strategies to ensure compliance with REMS programs.
☐	Ensure contingency billing documentation system is defensible upon audit.
☐	Design back up communication systems to be compliant with HIPAA.
☐	Develop an alternative staffing model to meet patient care needs while safeguarding staff resiliency.
☐	Establish time sheets or similar strategies to document staff hours worked.
☐	Plan to support departments with whom pharmacy interacts (e.g. nursing/MARs; prescribers/order sets; radiology/orders; laboratory/results/orders)
☐	Avoid reliance on work-arounds which risk PHI security breaches or cross contamination of systems (e.g. infecting home computers)
☐	Anticipate multidisciplinary pharmacy-related needs (e.g. ICU flow sheets, floor stock order forms, controlled substance forms, missing medication form, medication reconciliation form).
☐	Consider alternative staffing models, security needs and emergency ops team.
☐	Develop strategies to minimize staff fatigue / burnout.
☐	Establish post-event evaluation processes, addressing identified gaps and lessons learned.