Top Cyber Risks to Include in Your Audit Plan - Update

HCCA – Compliance Institute
April 9, 2019

Johan Lidros CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, ITIL-F
President Eminere Group

Presenter

- Johan Lidros, Founder and President of Eminere Group
- Over 20 years of experience providing information technology security, compliance and governance services in the healthcare industry in Europe and in the United States
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, etc.) and has participated in several related committees
- Certifications: CISA, CISM, CGEIT, ITIL-F, CRISC, HITRUST CCSFP

Table of Contents

Introduction

- Information technology (IT) is critically important for healthcare organizations.
- The complexity and rate of change of technology can dramatically impact risk and compliance.
- The latest IT and cyber threats can challenge a healthcare provider's ability to deliver quality outcomes.
- Improvements in IT Governance can help prepare organizations for IT audit challenges
- A wealth of best practices and industry standards are available to help healthcare organizations improve their cyber-security, IT Audit and IT Risk compliance.

Objectives

- **You will learn:**
  - The latest key IT and Cyber Risks you need to monitor and audit;
  - How to discuss IT and Cyber Risks with management, and
  - How to turn IT and Cyber Risks into opportunities.
- **We will share:**
  - Trending IT governance and security best practices;
  - Accepted industry standards, and
  - Sources for further research.
- **We welcome your questions – don't save them for the end!**

Table of Contents

Health IT - Definition

- **The term "Health IT" is broadly used currently and refers to an array of technologies to store, share, and analyze health information.**

"Health IT systems compromise the hardware and software that are used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention or disease."

Office for the National Coordinator of Health Information Technology

Typical Health IT Systems

Health IT Systems	Example
Administrative/billing or practice management system	• Coding/billing system • Master patient index • Registration/appointment scheduling system
Automated dispensing system	• Medication dispensing cabinet
Computerized medical devices	• Infusion pumps with dose-error-reduction capability • Patient monitoring systems (e.g., cardiac, respiratory, fetal)
Electronic health record (EHR) or EHR component	• Bar-coded medication administration • Clinical decision support system • Clinical documentation system (e.g., progress notes) • Computerized provider order entry • Pharmacy system
Human interface device	• Keyboard, • Monitor/display/Touchscreen • Mouse • Speech recognition system
Laboratory information system	• Microbiology system • Pathology system • Test results
Radiology/diagnostic imaging system	• Picture archiving and communication system

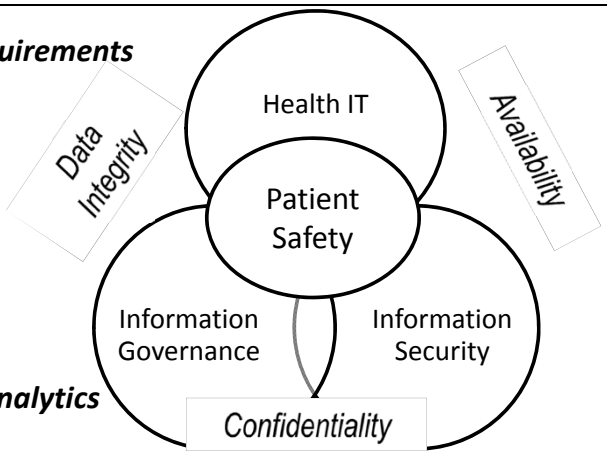
Key Drivers Impacting Health IT

Regulatory requirements

PII/EPHI Theft

Telehealth

Big data and Analytics



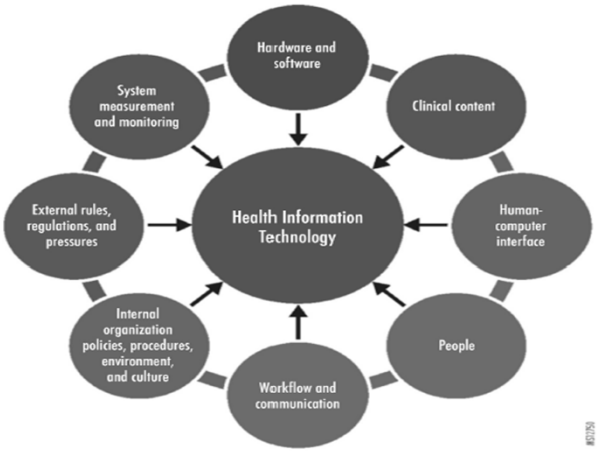
Cloud

Patient interaction

Social media

Portable devices

Health IT – Enterprise Impact



Healthcare IT Characteristics

- **Diversified IT environment**
- **Medical Devices and IT System coming together**
- **EMR and HIE are changing the IT environment**
- **Location of healthcare services provided**
  - On-site
  - Telehealth
  - Internet of Things
- **Cloud is getting common and more outsourcing**
- **Many regulatory requirements**
- **Constantly new and changing threats/risks related to the use of technology**
- **The "value" of information**
- **Immature IT/Information Security**

Typical IT Risks

Risk List	Risk List	Risk List
1. Vendor Management	13. Data Warehouse and Other Data Repositories	25. PCI-DSS Compliance
2. Change Management	14. Internal and External Intrusion	26. Problem and Incident Management
3. Identity and Access Management	15. IT Governance / IT Security Governance	27. Resources and IT Skills
4. EPHI Inventory and IT Asset Management	16. Business Continuity (Downtime)	28. Roles and Responsibilities
5. Network Availability	17. Disaster Recovery and Backup Management	29. Facility/Utility Systems
6. Electronic Communication (Email, Texting, Faxing)	18. Disposal of Electronic Media	30. Grants w. IT Security Requirements / Research
7. IT Risk Management	19. Security Incident Management	31. Cybersecurity
8. Medical Devices	20. Information/Data Governance	32. IT Cost
9. Phone Systems	21. Patch management	33. Affiliated Organizations
10. Security Awareness	22. Physical Security and IT Environmental Controls	34. Telehealth
11. Internet Usage and Social Media	23. End-User Devices (Workstations, Tablets, Laptops, USBs, Smart phones, etc.)	35. Privacy/GDPR/State Privacy, etc.
12. Audit Trail and Logs	24. IoT	

Health IT Risks – ECRI 2018

1. **Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients**
2. **Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk**
3. **Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants**
4. **Missed Alarms May Result from Inappropriately Configured Secondary Notification Devices and Systems**
5. **Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury**
6. **Unholstered Electrosurgical Active Electrodes Can Lead to Patient Burns**
7. **Inadequate Use of Digital Imaging Tools May Lead to Unnecessary Radiation Exposure**
8. **Workarounds Can Negate the Safety Advantages of Bar-Coded Medication Administration Systems**
9. **Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care**
10. **Slow Adoption of Safer Enteral Feeding Connectors Leaves Patients at Risk**

13

AHIA 2017 IT Audit Survey

Audit Area	%
Network security	60.5%
Identity and Access management	55.3%
Electronic medical record system	44.7%
Business continuity/disaster recovery	44.7%
IT general controls	44.7%
Financial systems	42.1%
Change management	42.1%
HIPAA Security	42.1%
Patch management	39.5%
PCI compliance	39.5%
Mobile device security/BYOD	39.5%
Vendor management	36.8%
Biomedical devices	34.2%
Cloud security	34.2%
Pre- or Post-implementation review	34.2%
HIPAA Privacy	34.2%
Security Incident Management	31.6%

14

Most Common Audit Areas

- **Identity and Access Management**
- **EMR Core System**
- **IT General Controls**
- **HIPAA**
- **Financial Systems**
- **Vendor Management**
- **Business Continuity and Disaster Recovery**
- **Network Security**
- **PCI**
- **Mobile Device Management**
- **Patch Management**
- **Cybersecurity**
- **New Systems**

Additional Key Risks to Audit

- **Health IT**
  - Internet of Things
  - Telehealth
  - Apps (internet of things)
  - Risk Management
  - Medical Devices
- **Data Warehouse**
- **HIE**
- **Information Governance**
- **IT Governance**
- **Patient Communication/Portal**
- **Backup Management**
- **Security Awareness Training**
- **Emergency Management/BCP/DR**
- **Departmental IT**
- **GDPR/State privacy…**

Added Value Audits – Hidden Opportunities

- **Life Cycle Management**
  - Application/Tool functionality
  - Tools
  - Cost
  - Age
  - Utilization
  - Budget/capacity/acquisition processes
- **Identity and Access management**
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)

17

IT Audit Plan Considerations

- **Comprehensive IT Risk Assessment**
- **Build Long Term IT Audit Plan**
- **Regular Audit of Key Control Areas**
  - Value added internal benchmarks
  - Trends
- **Framework Based**
  - Standard benchmark
- **Pro-Active Audits/Value Added Work**
  - Pre-implementation
  - Committees
- **Value – Cost – Investment – i.e. Performance**
- **Audit Tools – Key Component for Effective and Efficient IT Risk Management**

18

Table of Contents

- Introduction
- Key IT and Cyber Risks to Audit
- Board and Management Communication
- Best Practices and Additional Resources
- Wrap-up and Q&A

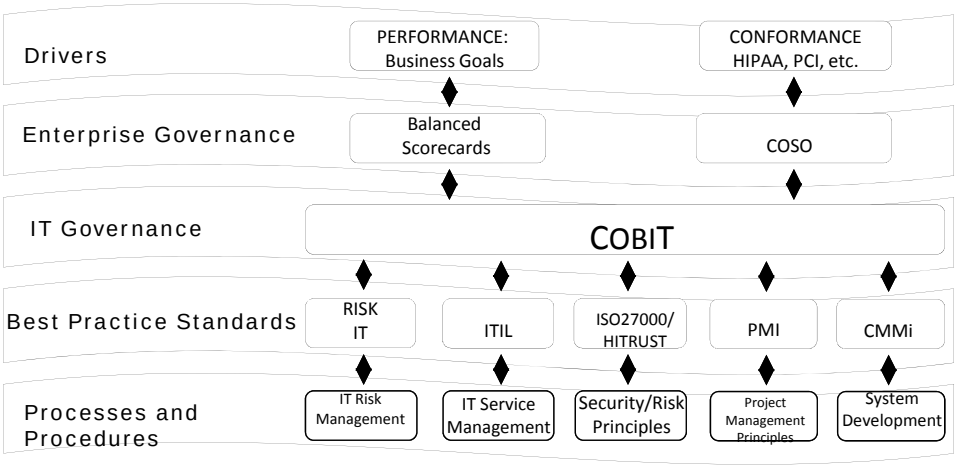
Discussion Areas Management/Board

- Health IT
- IT Governance
- Information Governance
- Information Security
- IT Standards
- Measurements and Metrics

Actions to Reduce Risk

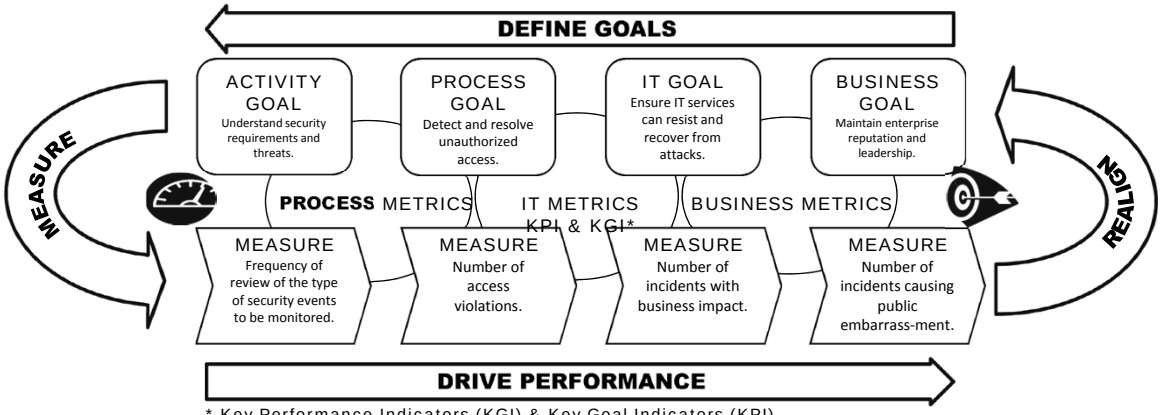
- **Leadership**
  - Information governance
  - Multidisciplinary Involvement
  - Vendor selection and Involvement
  - Change management
  - Monitor system effectiveness
- **Safety culture and process improvement**
  - Comprehensive system analysis/risk assessments/failure mode and effects analysis
  - Shared involvement and responsibility
  - System implementation and upgrades

IT Governance Framework



IT Goals and Metrics - Key Performance Indicators & Key Goal Indicators

You cannot manage what you do not measure!



* Key Performance Indicators (KGI) & Key Goal Indicators (KPI)

Legend	
Risk Rating	Trend
Low	Risk increasing
Medium	Risk decreasing
High	No change

Board / Executive IT Risk Dash Board

Capability	Key Risks	Risk Level	Risk Mgm Plan	Regulatory Findings	Trend
IT Risk Management	IT risks are not defined IT risks are not managed to acceptable levels		7	5	△
Information & Asset Inventory	Processes and procedures for classifying, labelling and handling information and assets are not managed Identification and assignment of ownership for assets containing sensitive information has not been performed.		6	3	▭
Information Protection	Processes for monitoring and tracking sensitive information throughout its lifecycle is not established Failure to restrict collection of personal information for only necessary purposes		~35	~22	△
Information Security Program Management	The information security program is not aligned with business requirements Policies and procedures have been established for information security		13	13	▭
Identity & Access Management	Priviliged access is used to compromise data Terminated user access is not removed appropriately		37	34	
Threat & Vulnerability Management	Internal and external vulerabilities go unmanaged Internal and external security threats go unmanaged		~120	~76	△
Third Party Security	Security risks are not identified with third parties Security risks are not managed to acceptable levels with third parties		39	39	△
IT Operations	Information security practices are not integrated into IT operations (change mgm, incident mgm, etc.) IT operations are not performing their Information security responsibilities		~26	~19	▭
Business Continuity & Disaster recovery	Disaster recovery processes and procedures are not defined Ability to recover from an outage has not been tested		38	34	△
Phyiscal & Environmental Controls	Physical perimeter controls at IT facilties are not established IT environmental controls (power, temp, etc.) to support IT operations are not sufficent		20	14	▭
Organization Security & Awareness	Users do not perform their security responsibiliteis Users do not understand their security responsibilities		5	4	▭
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance isssues are not implemented Compliance with legislative, regulatory or contractual obligations are not identified		~12	~2	▭

Regular Security Reporting

- **Risk Management Program**
  - Status management program – see example next page – Dash board
  - Number of risk assessments performed – Defined assessments and analysis per IT and organization projects, to include change control.
  - Time to remediate issues – The time between identification and remediation.
- **Vulnerability Management**
  - Issues by Status – When a vulnerability is identified on a system the first time, it is a new data point that should inform and, depending on the situation, drive an action.
  - Remediation Time - Measure the length of time from identification to remediation and is a measure of the efficiency of the patch and remediation cycle.
  - Mean time to Patch – The time between identification of a needed patch and the installation of the required patch.
- **Exceptions**
  - The number of information security policy exceptions requested and granted
- **Incident Management**
  - Number of Events - Events are activities or indicators that warrant further investigation and can be indicators of incidents.
  - Number of Incidents - Incidents occur when a material event or events have occurred and require a formal response activity.
- **Specific Initiatives**
  - CMS Quality Measurements

CMS Quality Measurements - Examples

Quality Area	Quality Requirements	CMS Reference	Goal	Current Status	Accountable	Responsible
Information System Assets (Medical Devices, Server, End User Computing Devices, Databases, Software, Data)	Identify and classify all information system assets Verify assets and classification annually and obtain data owner approval	CP-2(8) SE-1	100% of All Information System Assets Classified annually and approved by data owner	70% of all Information System Assets Classified	Data Owner	CISO

Table of Contents

- **Introduction**
- **Key IT and Cyber Risks to Audit**
- **Board and Management Communication**
- **Best Practices and Additional Resources**
- **Wrap-up and Q&A**

Resources

- **AHIMA**
  - Information Governance Framework http://www.ahima.org/topics/infogovernance
- **AAMI**
  - TIR57: Principles for medical device security—Risk management www.aami.org
  - TIR97: Principles for medical device - Post-market security management for device manufactures (in development)
  - AAMI Medical Device Cybersecurity – A guide for HTM professional
- **Bipartisan Policy Center**
  - Patient Safety and Information Technology: Improving Information Technology's Role in Providing Safer Care https://bipartisanpolicy.org/library/patient-safety-and-information-technology-improving-information-technologys-role-in-providing-safer-care
- **The Center for Internet Security (CIS)**
  - Critical Security Controls for Effective Cyber Defense https://www.cisecurity.org/controls/
  - Regular updates OS security standards. .
- **Center for Disease Control and Prevention (CDC) and HHS**
  - Healthcare Organization and Hospital Discussion Guide for Cybersecurity https://www.cdc.gov/phpr/healthcare/documents/healthcare-organization-and-hospital-cyber-discussion-guide.pdf
- **Cloud Security Alliance**
  - Cloud Controls Matrix version September 2017 https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
  - Top Threats to Cloud Computing: Deep Dive
  - OWASP Secure Medical Device Deployment Standard
- **CRICO**
  - Malpractice-Risks-Associated-with-Electronic-Health-Records https://www.rmf.harvard.edu/Clinician-Resources/Article/2017/Malpractice-Risks-Associated-with-Electronic-Health-Records?
- **CMS**
  - Recommendations to Providers Regarding Cyber Security January 13, 2017
  - Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers September 2016 https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Core-EP-Rule-Elements.html
  - CMS Acceptable Risk Safeguards (ARS) – Security and Privacy
- **ECRI Institute**
  - Patient Safety Annual Top 10 studies of patient safety risks
  - Recall information devices

Resources

- **FDA**
  - Management of Cybersecurity in Medical Devices – Guidance for Industry and FDA Staff https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- **FFIEC**
  - Information Security Booklet Released September 2016
  - Cyber security assessment framework https://www.ffiec.gov/cyberassessmenttool.htm
- **Healthcare Industry Cybersecurity Taskforce (HHS)**
  - Report on improving cybersecurity in the healthcare industry https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
- **Healthcare & Public Sector Coordinating Council (HSCC) with HSCC Joint Cybersecurity Working Group (JCWG)**
  - MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN https://healthsectorcouncil.org/the-joint-security-plan/
  - Healthcare Industry Cybersecurity Practices https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx
- **HHS – Agency for Healthcare Research and Quality**
  - 2017 NATIONAL HEALTHCARE QUALITY AND DISPARITIES REPORT
  - https://www.ahrq.gov/research/findings/nhqrdr/chartbooks/patientsafety/index.html?utm_source=ahrq&utm_medium=en3&utm_term=&utm_content=3&utm_campaign=ahrq_en8_15_2017#_blank
- **HITRUST**
  - Privacy
  - NIST CSF
  - The addition of the Center for Internet Security Critical Security Controls (CIS CSC)
  - Precision Medicine Initiative (PMI)
  - OCR Audit Protocol
  - FEDRAMP Support for Cloud and IaaS Service Providers
  - FFIEC IT Examination Handbook for Information Security.
- **Joint Commission.**
  - Sentinel event alert #54: safe use of health information technology. Oakbrook Terrace, IL: Joint Commission; 2015; Available from: www.jointcommission.org/safehealthit .
  - Sentinel event alert #42: Safely implementing health information and converging technologies. Joint Commission; 2008; Available from: www.jointcommission.org/safehealthit
- **MDiSS Medical Device Innovation, Safety and Security Consortium**
  - MDISS Tool – security risk assessment medical devices Tool MDRAP https://mdrap.mdiss.org

Resources

- **NACD – National Association of Corporate Directors**
  - 2017 Cyber Risk Oversight http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html
- **NIST**
  - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity version 1.1 January 2017
  - Cybersecurity Resource Center Beta https://beta.csrc.nist.gov/
  - Guide for Cybersecurity Incident Recovery https://beta.csrc.nist.gov/publications/detail/itl-bulletin/2017/02/guide-for-cybersecurity-incident-recovery/final
  - Baldridge Cybersecurity Excellence Builder https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf
- **ONC – Health IT**
  - Report of the evidence on Health IT Safety and interventions May 2016
  - SAFER Guides - https://www.healthit.gov/safer/
  - EHR Contracts Untangled SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT September 2016 https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf
  - How to Identify and Address Unsafe Conditions Associated with Health IT
  - The Role of Health IT Developers in Improving Patient Safety in High Reliability Organizations
- **ONC and OCR Office of Civil Rights (OCR)/HHS**
  - Security Risk Assessment – Small and Medium Entities https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
- **OCR**
  - HIPAA Audit Program (Privacy, Breach and Security)
- **Security Culture Framework https://securityculturefamework.net/**

Regulatory Requirements - Changes

- **CMS - Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers.**
  - Must be in compliance with Emergency Preparedness regulations to participate in the Medicare or Medicaid program.
- **Effective date, on November 16, 2017.**
  - Testing
  - Cyber event
  - https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Core-EP-Rule-Elements.html

Health IT – Identify and Assess

- **How to Identify and Address Unsafe Conditions Associated with Health IT**
  - Office for the National Coordinator of Health Information Technology


The Office of the National Coordinator for Health Information Technology

Anticipating Unintended Consequences of Health Information Technology and Health Information Exchange

How to Identify and Address Unsafe Conditions Associated with Health IT

November 15, 2013

Authors
ECRI Institute:
Cynthia Wallace, CPHRM
Karen P. Zimmer, MD, MPH, FAAP
Lorraine Possanza, DPM, JD, MBE
Robert Giannini, NHA, CHTS-IM/CP
Ronni Solomon, JD

Prepared for
The Office of the National Coordinator for Health Information Technology
Washington, DC

Prepared by
Westat
1600 Research Boulevard
Rockville, MD 20850-3129
(301) 251-1500

Contract No: HHSP23320095655WC
Task Order: HHSP23337003T

SAFER Guides

33

SAFER – Checklist

SAFER Self Assessment High Priority Practices | Checklist

> Table of Contents | > *About* the Checklist | > Team Worksheet | > *About* the Practice Worksheets | > Practice Worksheets

Recommended Practices for Phase 2 — Using Health IT Safely

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
11	The status of orders can be tracked in the system.	*Worksheet 11*	○	○	○	reset
12	Clinicians are able to override computer-generated clinical interventions when they deem necessary.	*Worksheet 12*	○	○	○	reset

34

SAFER Guides

Recommended Practice

12 Clinicians are able to override computer-generated clinical interventions when they deem necessary.[47,48]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Computers cannot practice medicine. Disallowing clinician overrides of computer-generated interventions implies that computers have access to more accurate data and greater medical knowledge and expertise than clinicians. This is rarely true.

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Hard stop alerts (i.e., the user must take an action before proceeding) are used only for the most egregious potential errors. Hard stop alert overrides are closely monitored and reviewed often.[47]
- The alert override rate (i.e., the number of point-of-care alerts that clinicians override divided by the total number of point-of-care alerts generated) is monitored, and alerts with high override rates are reviewed.

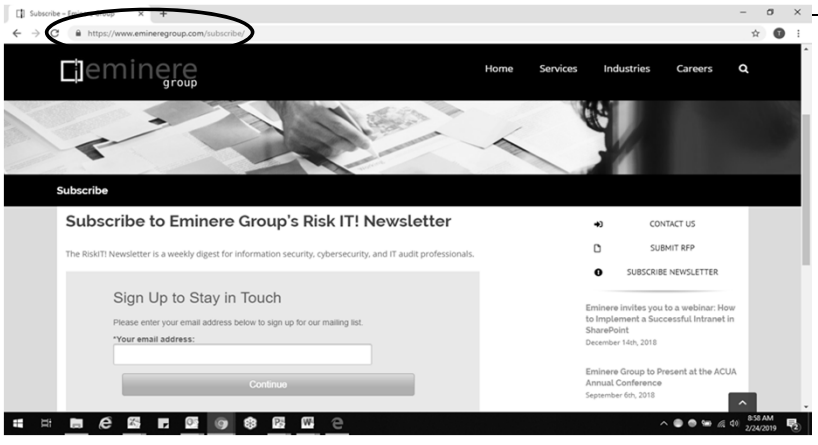
See the *Computerized Provider Order Entry with Decision Support Guide* for related recommended practices.

Assessment Notes

Follow-up Actions

35

Another Resource: RiskIT! Weekly Newsletter



https://www.emineregroup.com/subscribe/

36

Table of Contents

- **Introduction**
- **Key IT and Cyber Risks to Audit**
- **Board and Management Communication**
- **Best Practices and Additional Resources**
- **Wrap-up and Q&A**

Conclusion

- **Risk based Long Term Audit Plan**
  - Health IT
  - Key Controls
  - Operational efficiency
- **Drive Measurements and Metrics**
  - Board and Management discussions
  - Audits
- **Several good practices and standards exist to guide you in most areas**

Questions?

39

For questions please contact

- **Johan Lidros**
  - johan.lidros@emineregroup.com
  - (813) 832-6672 x-9101
  - (813) 355-6104 (cell)

- **Tom Smith**
  - tom.smith@emineregroup.com
  - (813) 832-6672 x-9112
  - (501) 837-4001 (cell)

40