Self-Assessment Questionnaire: Establishing a Health Information Technology Safety Program

Initial assessment by: _____

Date: _____

In consultation with: _____

_____

_____

Date of previous assessment: _____

The success of a health information technology (IT) safety program hinges on the ability of system users to recognize, react to, and report health IT-related events for analysis and action (e.g., vendor reporting, PSO reporting, vendor modifications). Two overarching factors support a health IT safety program: the organization's culture of safety and the ability to "do the right thing, even if it's not standard procedure," Christoph Lehmann, MD, FACMI, FAAP, professor of pediatrics and biomedical informatics, Vanderbilt University School of Medicine, said to participants at the September 16, 2016, meeting of the *Partnership for Health IT Patient Safety*.

Once an event is identified and reported to the appropriate parties, it can be analyzed and solutions can be developed. A health IT safety program also allows for feedback, which meeting participants identified as a key component to the safe and effective implementation and use of health IT. The provision of feedback about health IT-related issues and the actions taken within a provider organization can be accomplished in different ways; for example, two methods mentioned during the meeting were communication by managers to staff and the distribution of information on a dashboard. Vendors typically distribute information in regular or special publications, as appropriate.

A health IT safety program within a provider organization requires support from all levels of the organization, including leadership and patients, as well as vendors. Executive walkrounds and proactive patient queries can help crystallize staff members' reported concerns or demonstrate the effects of implemented solutions. Such proactive knowledge can help prioritize safety interventions and vendor actions.

Use this self-assessment questionnaire in conjunction with the following resources to review and further develop an effective health information technology (IT) safety program. Then, use the attached action plan template to track resulting projects, initiatives, and reviews.

- ECRI Institute guidance article: Health information security standards https://www.ecri.org/components/HRC/Pages/LawReg19_1.aspx
- ECRI Institute PSO Deep Dive: Patient education https://www.ecri.org/Pages/Patient-Identification-Deep-Dive.aspx

- Office of the National Coordinator for Health Information Technology (ONC) SAFER guide: organizational responsibilities https://www.healthit.gov/sites/safer/files/guides/safer_organizationalresponsibilities_sg002_form_0.pdf

		Yes	No	N/I*	N/A	Comments
	Foundation					
1	Does the organization rely on a standard definition of health IT safety?					
	a. Does this definition include safe use of the technology?					
	b. Does this definition include the equipment itself?					
	c. Does this include using health IT to improve safety?					
2.	If there is no freestanding health IT safety program, is the health IT safety program integrated into other existing and maintained programs (e.g., patient safety, quality, risk, or others)?					
3.	Is the organization alert for health IT safety events as well as events in which health IT safety plays a role?					
4.	Does the health IT safety program incorporate the electronic health record (EHR), all networked equipment, and all technologies used?					
5.	Does the health IT safety program address or support IT security measures?					
	a. Does the health IT safety program address or support equipment security measures?					
	b. Does this program address personal device use (e.g., bring-your-own-device policies)?					
6.	Is the health IT safety program or program component reviewed regularly					

* N/I stands for "Needs Improvement"

		Yes	No	N/I*	N/A	Comments
	for effectiveness?					
7.	Is education provided to staff as a part of the health IT safety program?					
	a. Does this education occur upon hire and whenever new upgrades, systems, modifications, or other system changes occur?					
	b. Is this education documented?					
	c. Does this education include the importance of awareness, reporting, and security practices?					
8.	Does the organization use evidence-based assessments, such as those included in the ONC SAFER guides?					
9.	Are human-factors specialists part of health IT evaluations and health IT safety and usability considerations?					
10,	Are clinicians engaged in health IT safety practice development and assessment?					
11.	Are proactive failure modes and effects analyses (FMEAs) conducted for health IT-related issues?					
12.	Are designated resources regarding health IT safety identified and made available to staff?					

Using Leadership Roles to Champion Health IT Safety

13.	Are sufficient resources dedicated to health IT safety?					
14.	14. Are experts available as part of health IT safety program resources?					
15.	15. Do executives and senior leaders participate in walkrounds?					
	a. Do these walkrounds include consideration of health IT safety-related issues?					

		Yes	No	N/I*	N/A	Comments
	b. Do these walkrounds include consideration of workflow (i.e., are leaders asked to be aware of the potential for—and reasons behind—workarounds and to attempt to resolve the need for them)?					
16.	Is a member of the executive team or senior leadership accountable for and engaged in health IT safety?					
17.	Is patient feedback sought regarding health IT system use or concerns?					
	a. Is this feedback brought to the attention of the health IT safety committee?					
	b. Is this feedback, when appropriate, brought to the attention of the vendor?					
	c. Is it used to analyze and implement improvements to the health IT system?					
18.	Does the organization have a surveillance mechanism (automatic or manual) in place to identify and flag health IT–related issues (e.g., patient queries, failure modes and effects analysis, root-cause analysis, walkrounds, PSO reporting, feedback loops, or vendor-provided safety information)?					
19	Does this method of identifying health IT-related issues include—					
	a. Review of relevant adverse-event report data by a designated staff member?					
	b. Coordination as appropriate with internal IT staff and the vendor?					
	c. Reviewing equipment failures?					
	d. Identifying and reviewing the source of use errors or workaround?					
	e. Encouraging staff to report technology hazards, such as difficult interfaces or confusing elements that may lead to potential errors or workarounds?					

		Yes	No	N/I*	N/A	Comments
	f. Review of safety committee findings?					
	g. Tracking compliance with equipment inspection and preventive maintenance schedules?					
	h. Monitoring downtime and the impact it has on health IT-related issues?					
	i. Reviewing relevant patient complaints and concerns?					
	j. Looking for workarounds?					
	k. Raising awareness of vendor-reported issues?					
	l. Are health IT-related events reported to the appropriate individual (e.g., risk manager, IT staff, vendor, medical director)?					
20.	Does the organization analyze the frequency and severity of identified health IT–related safety problems?					
	a. Does this evaluation include review of the factors contributing to the health IT–related safety problem?					
	b. Does this evaluation include comparing typical work practices (i.e., actual practices, including potential workarounds) with current standards and procedures (i.e., recommended or ideal practices)?					
21.	Are the findings of analyses communicated to the appropriate individuals (e.g., the safety committee, risk manager, IT leadership, chief medical informatics officer, designated safety representative, department leaders, vendors)?					
22.	When conducting a root-cause analysis (RCA) for a safety event, are health informatics personnel, IT, and clinicians part of the process?					
23.	Does the organization share its learnings—					

		Yes	No	N/I*	N/A	Comments
	a. Within the reporting facility?					
	b. Across the organization?					
	c. With the vendor?					
	d. Outside the organization?					
	e. Through a relationship with a patient safety organization (PSO)?					
24.	Does the organization use data from its PSO for further learning?					
25.	Does an event trigger a search for previous or other potential similar events?					

Engaging Providers, Staff, and Patients

26.	Are clinicians aware of and engaged in health IT safety practices?					
27.	Do patients have access to their information?					
	a. Do they have a way to indicate the information's validity or error?					
	b. Are potential security issues with patient access to information addressed?					
	c. Are staff aware of the risk of IT security breach from:					
	d. Computer viruses?					
	e. Phishing, spamware, or other malware attacks?					
	f. Equipment theft or loss?					
	g. Intentional or unintentional HIPAA [Health Insurance Portability and Accountability Act] violations?					
28.	Is the reporting of health IT safety events, near misses, or hazardous conditions encouraged and supported?					
29.	Is feedback provided to those who do					

	Yes	No	N/I*	N/A	Comments
report?					
a. Is a dashboard used to provide feedback?					
b. Are safety-reporting feedback and updates provided to staff members?					

Action Plan

Assessment Completed By: _____ **Date:** _____

Question No.	Action Required	Responsibility	Target Date	Action Completed	
				Date	Initials

Question No.	Action Required	Responsibility	Target Date	Action Completed	
				Date	Initials