ASTP Assistant Secretary for Technology Policy

Safety Assurance Factors for EHR Resilience (SAFER) Guides 2024 Update

David R. Hunt, MD, FACS
Medical Director, Patient Safety
ASTP/ONC Office of Policy (OPOL)

Assistant Secretary for Technology Policy
U.S. Department of Health and Human Services

December 5, 2024

Disclaimers

- Dr. Hunt has no financial relationships or affiliations with ineligible companies and has no conflicts of interest to disclose.
- Some materials contained in this presentation are based on the provisions contained in 45 C.F.R. Parts 170 and 171. While every effort has been made to ensure the accuracy of this restatement of those provisions, this presentation is not a legal document. The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state and local laws may also apply.

Sir Cyril Chantler

Medicine used to be simple, ineffective and relatively safe.

Now it is complex, effective and potentially dangerous.

The role and education of doctors in the delivery of healthcare.

Hollister Lecture delivered at the Institute of Health Services Research, Northwestern University, Illinois, USA. October 1998. *Lancet* 1999;353:1178–81.

NATIONAL

Cyberattack led to harrowing lapses at Ascension hospitals, clinicians say

JUNE 19, 2024 · 5:00 AM ET

HEARD ON MORNING EDITION

By Rachana Pradhan, Kate Wells

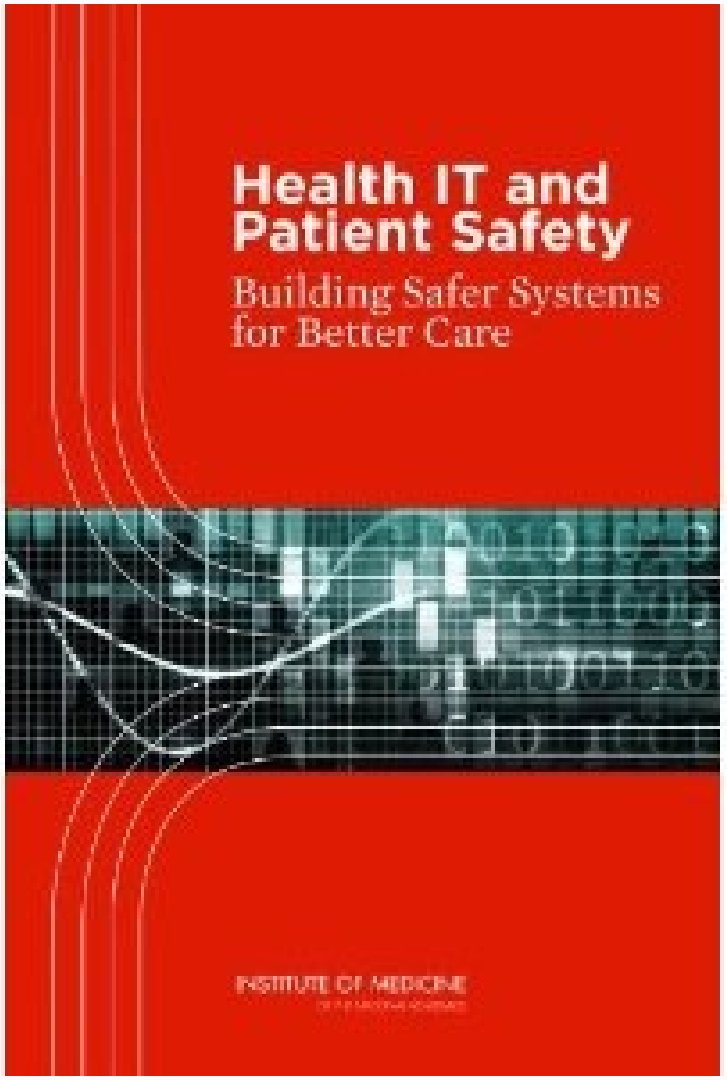
FROM KFF Health News

U.S. Department of Health and Human Services

Office of Inspector General

Adverse Events in Hospitals: A Quarter of Medicare Patients Experienced Harm in October 2018

ASTP

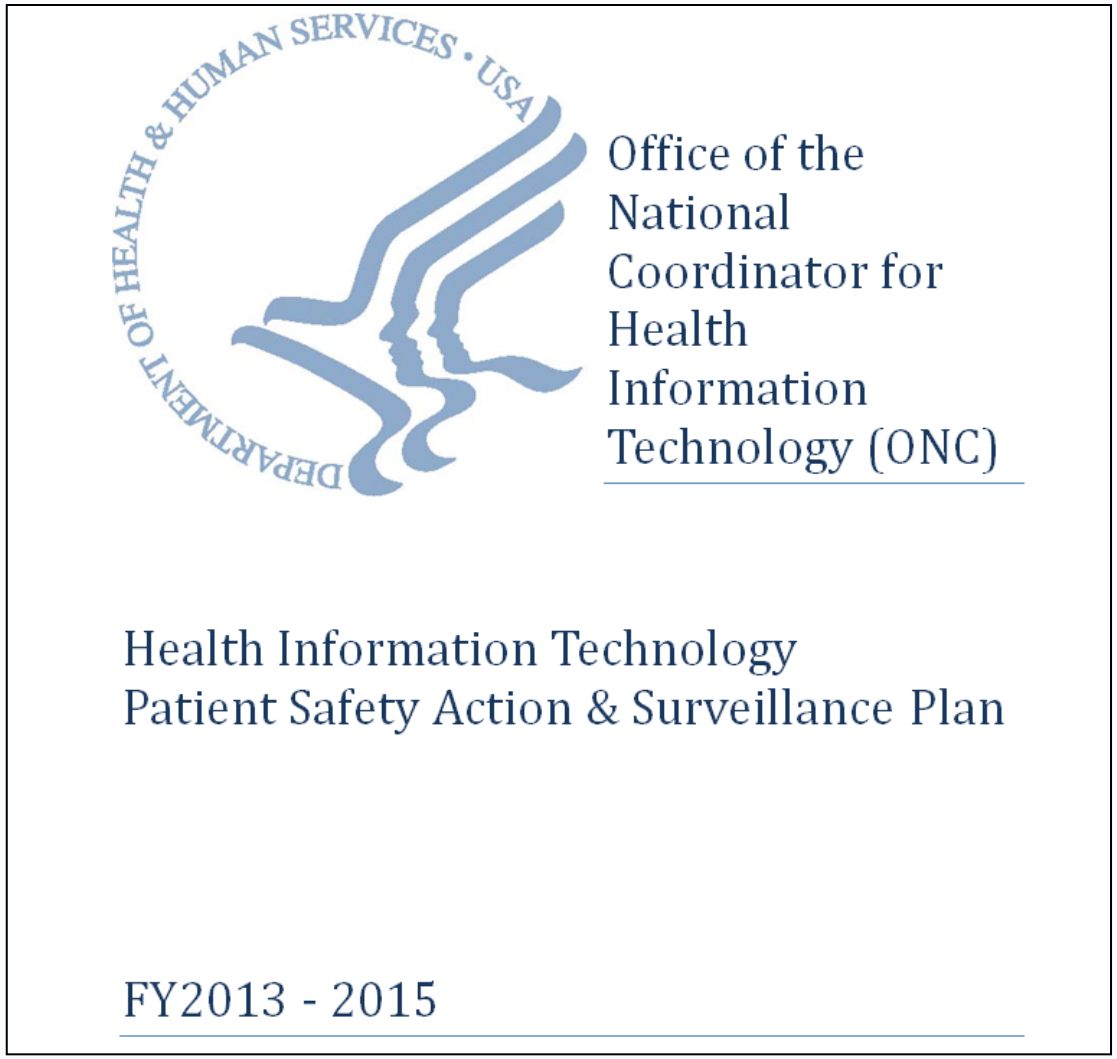


- **Health IT can improve patient safety** in some areas such as medication safety; however, there are **significant gaps** in the literature regarding **how health IT impacts patient safety overall**

- Safer implementation and use begins with viewing health IT as part of a larger **sociotechnical** system

- **All stakeholders need to work together** to improve patient safety

Goals:

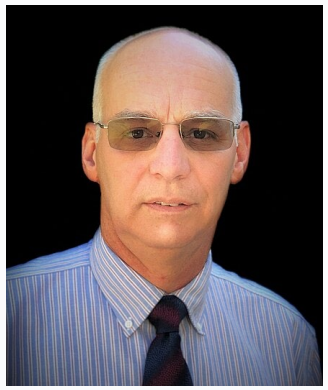


- Use Health IT to Make Care Safer
- Improve the Safety and Safe Use of Health IT

Patient Safety Action & Surveillance Plan

- **Learning**: Increasing the quantity and quality of data and knowledge about health IT safety
- **Improving**: Targeting resources and corrective actions to improve health IT safety and patient safety
- **Leading:** Promoting a culture of safety related to health IT

SAFER Guides



Dean Sittig, PhD

University of Texas School of Biomedical Informatics; UT-Memorial Hermann Center for Healthcare Quality and Safety

Hardeep Singh, MD

Houston VA Center for Innovations in Quality, Effectiveness and Safety, and Baylor College of Medicine

Joan Ash, PhD

Prof. and Vice-Chair Informatics at Oregon Health & Science University

Kathy Kenyon, JD

ONC (2009-2015) Senior Policy Analyst

Initial Stakeholder Engagement

- American College of Physicians
- American Health Information Management Association
- American Hospital Association
- American Medical Informatics Association
- American Society for Healthcare Risk Management
- Association of Medical Directors of Information Systems
- CDC's Laboratory Health IT Panel
- Health Information Management Systems Society
- Institute for Healthcare Improvement
- Medical Group Management Association
- Patient Safety Organizations
- The Scottsdale Institute
- Summer Institute for Nursing Informatics
- Texas Medical Association
- The Joint Commission

SAFER Guides

https://www.healthit.gov/topic/safety/safer-guides

Foundational Guides

- High Priority Practices
- Organizational Responsibilities

Infrastructure Guides

- Contingency Planning
- System Management

Clinical Process Guides

- Computerized Provider Order Entry with Decision Support
- Test Results Reporting and Follow-Up
- Clinician Communication
- Patient Identification

SAFER Guides Update 2024

Primary Authors

- **Trisha Flanagan, RN, MSN, CPPS,** Health Informatics Nurse, Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey Veterans Affairs Medical Center, Houston TX
- **Hardeep Singh, MD, MPH,** Co-Chief, Health Policy, Quality and Informatics Program, Center for Innovations in Quality, Effectiveness and Safety and Professor of Medicine at the Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine, Houston, TX
- **Dean F. Sittig MS, PhD, FACMI, FAMIA, FHIMSS, FIAHSI,** Professor of Biomedical Informatics, Department of Clinical and Health Sciences, McWilliams School of Biomedical Informatics, University of Texas Health Science Center at Houston, TX and Informatics Review LLC, Lake Oswego, OR

Support staff for the primary authorship team

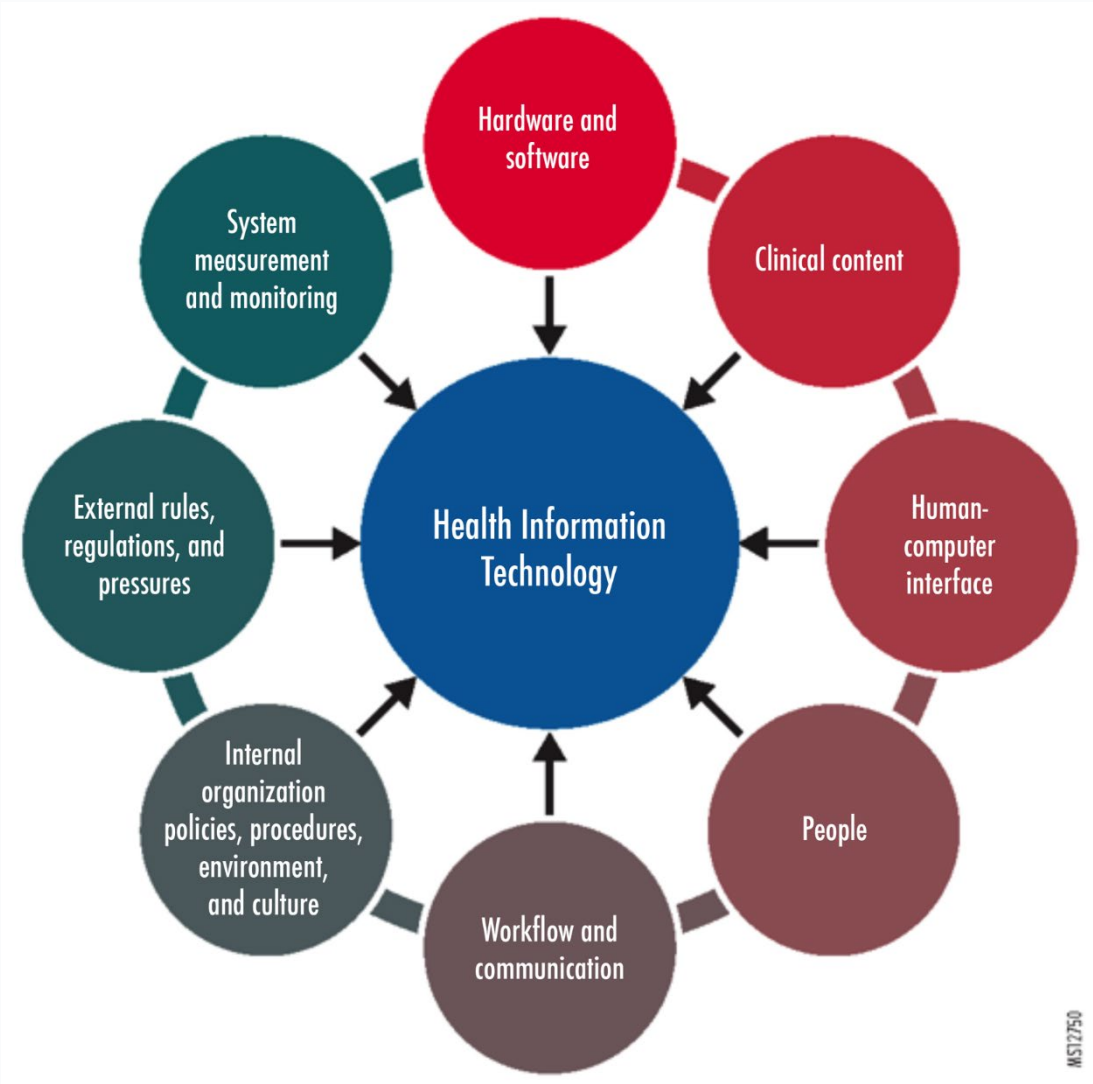
- **Rosann Cholankeril, MD, MPH,** Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine
- **Sara Ehsan, MBBS, MPH,** Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine Additional authors who contributed to at least one guide:
- **Jason S. Adelman, MD, MS,** (Patient ID) Chief Patient Safety Officer & Associate Chief Quality Officer, Executive Director, Patient Safety Research, Co-Director, Patient Safety Research Fellowship in Hospital Medicine, New York-Presbyterian Hospital/Columbia University Irving Medical Center, New York, NY
- **Daniel R. Murphy, MD, MBA,** (Clinician Communication, Test Results) Chief Quality Officer, Baylor Medicine, Houston, TX
- **Patricia Sengstack, DNP, NI-BC, FAAN, FACMI,** (Organizational Responsibilities) Senior Associate Dean for Informatics, Director, Nursing Informatics Specialty Program, Vanderbilt University School of Nursing, Vanderbilt University, Nashville, TN

SAFER Guides Update 2024

Additional contributors who provided feedback on various guides or parts of guides

- Miriam Callahan, MD (Patient ID)
- David C. Classen, MD (CPOE, AI recommendation)
- Anne Grauer, MD, MS (Patient ID)
- Ing Haviland (Patient ID)
- Amanda Heidemann, MD (All Guides)
- I-Fong Sun Lehman, DrPH, MS (Patient ID)
- Christoph U. Lehmann, MD (AI recommendation)
- Christopher A. Longhurst, MD, MS (AI recommendation)
- Edward R. Melnick, MD (Clinician Communication)
- Robert E. Murphy, MD (Organizational Responsibilities)
- Ryan P. Radecki, MD, MS (AI recommendation)
- Raj Ratwani, PhD (AI recommendation)
- Trent Rosenbloom, MD (Clinician Communication)
- Lisa Rotenstein, MD (Clinician Communication)
- Hojjat Salmasian, MD, PhD (All Guides)
- Richard Schreiber, MD (CPOE)
- Danny Sands, MD (Clinician Communication)
- Debora Simmons, PhD, RN (Organizational Responsibilities)
- Carina Sirochinsky (Patient ID)
- Neha Thummala, MPH (Patient ID)
- Emma Weatherford (Patient ID)
- Adam Wright, PhD (CPOE)
- Andrew Zimolzak, MD, MMSc (Test Results, Clinician Communication)

Socio-Technical Model for Health IT



Adapted by permission from BMJ Publishing Group Limited. Sitting DF and Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care.* 19(Supplement 3): i68-74, October 2010; doi: 10.1136/qshc.2010.042085

Anatomy of a SAFER Guide

- Category (e.g. High Priority Practices)
- Instructions
- Principle
- Recommended Practices
- Rationale for Practice
- Strength of Recommendation
- Actors
- Examples
- References

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

The *Checklist* is structured as a quick way to enter and print your self-assessment.

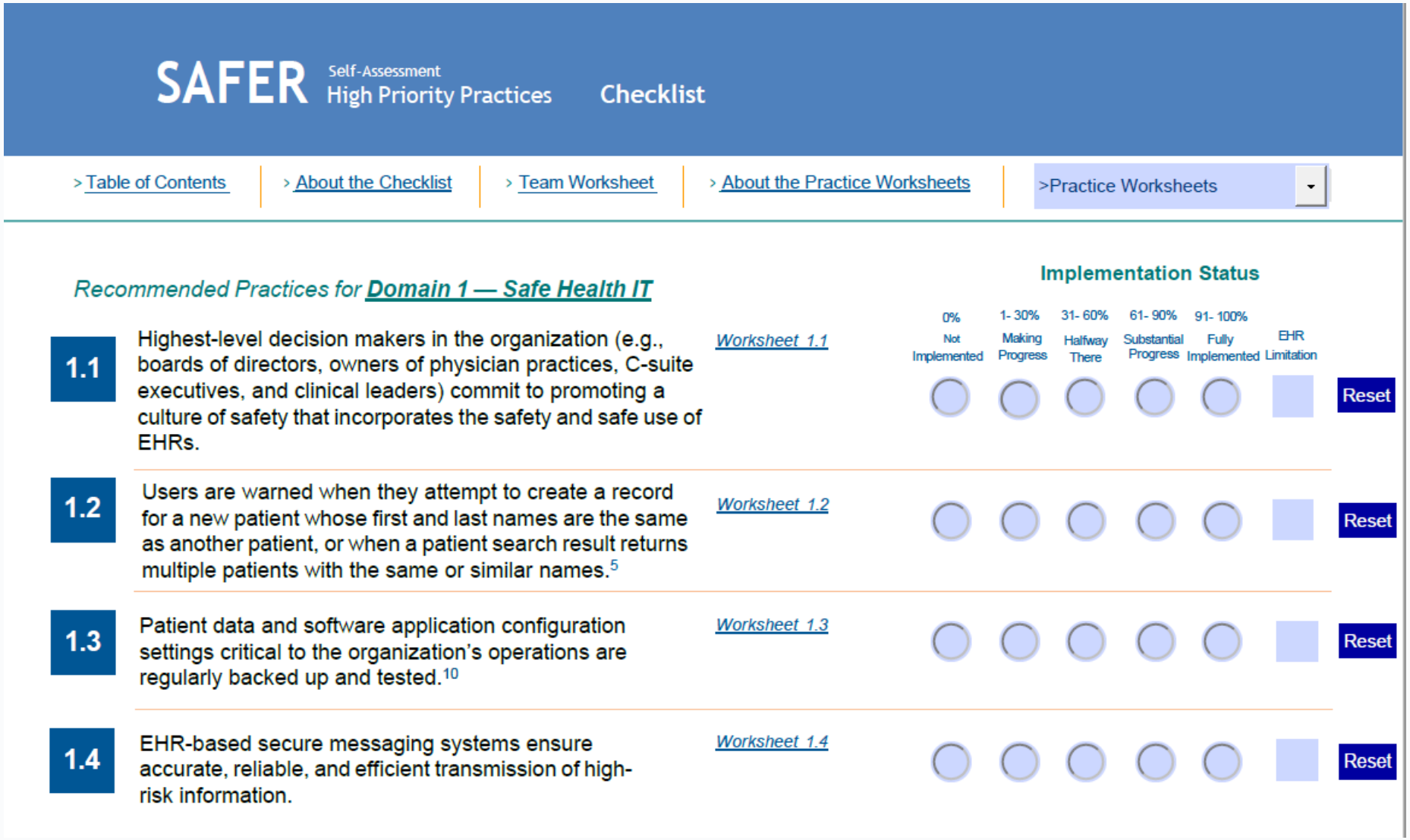
Select the level of implementation achieved by your organization for each Recommended Practice. Your Implementation Status will be reflected on the Recommended Practice Worksheet in this PDF. The implementation status scales are as followed:

Not Implemented – (0%)	Making Progress (1 - 30%)	Halfway there (31 – 60%)	Substantial Progress (61-90%)	Fully Implemented (91-100%)
The organization has not implemented this recommendation.	The organization is in the early or pilot phase of implementing this recommendation as evidenced by following or adopting less than 30% of the implementation guidance.	The organization is implementing this recommendation and is following or has adopted approximately half of the implementation guidance.	The organization has nearly implemented this recommendation and is following or has adopted much of the implementation guidance.	The organization follows this recommendation, and most implementation guidance is followed consistently and widely adopted.

The organization should check the following box if there are some limitations with the current version of their EHR that preclude them from fully implementing this recommendation.

☐ **EHR Limitation** - The EHR does not offer the features/functionality required to fully implement this recommendation or the implementation guidance.

SAFER Guides 2024

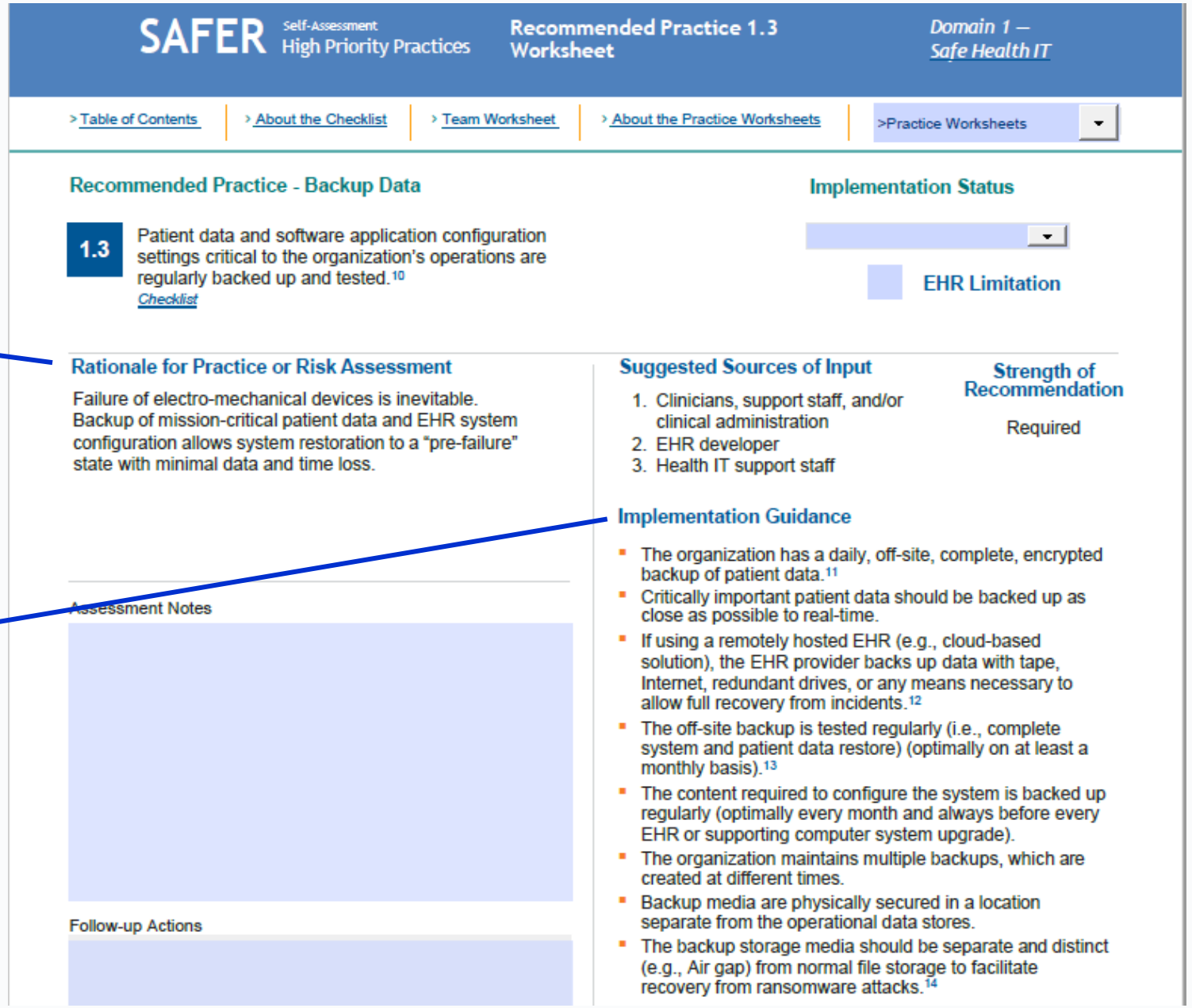


ASTP

SAFER Guides 2024

Rationale section provides guidance about "why" the safety activities are needed

The Implementation Guidance section lists potentially useful practices or scenarios to inform your assessment and implementation of the specific Recommended Practice.



SAFER Self-Assessment High Priority Practices | Recommended Practice 1.3 Worksheet | Domain 1 – Safe Health IT

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

Recommended Practice - Backup Data

Implementation Status

1.3 Patient data and software application configuration settings critical to the organization's operations are regularly backed up and tested.[10]
Checklist

EHR Limitation

Rationale for Practice or Risk Assessment

Failure of electro-mechanical devices is inevitable. Backup of mission-critical patient data and EHR system configuration allows system restoration to a "pre-failure" state with minimal data and time loss.

Suggested Sources of Input

1. Clinicians, support staff, and/or clinical administration
2. EHR developer
3. Health IT support staff

Strength of Recommendation

Required

Implementation Guidance

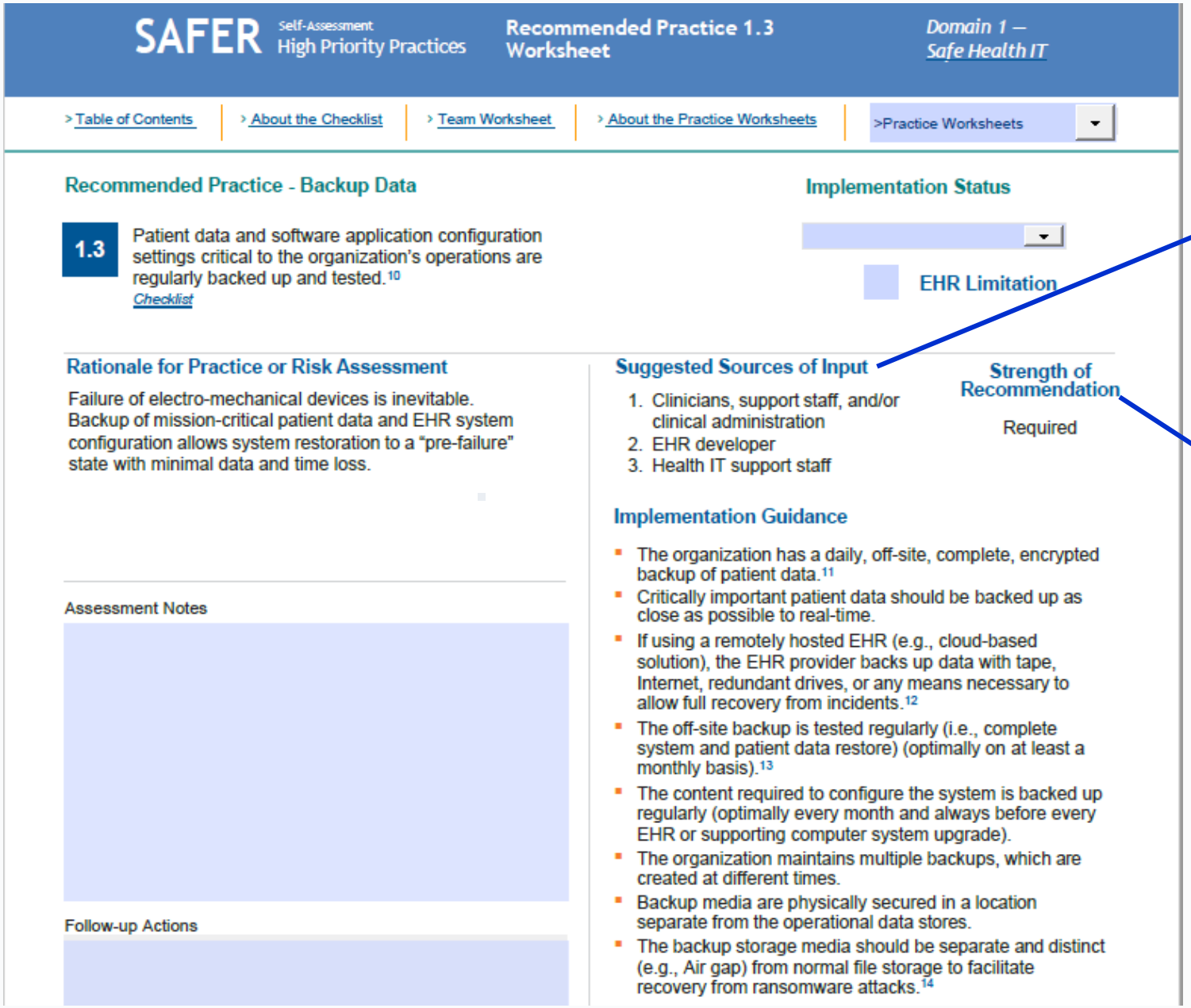
- The organization has a daily, off-site, complete, encrypted backup of patient data.[11]
- Critically important patient data should be backed up as close as possible to real-time.
- If using a remotely hosted EHR (e.g., cloud-based solution), the EHR provider backs up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.[12]
- The off-site backup is tested regularly (i.e., complete system and patient data restore) (optimally on at least a monthly basis).[13]
- The content required to configure the system is backed up regularly (optimally every month and always before every EHR or supporting computer system upgrade).
- The organization maintains multiple backups, which are created at different times.
- Backup media are physically secured in a location separate from the operational data stores.
- The backup storage media should be separate and distinct (e.g., Air gap) from normal file storage to facilitate recovery from ransomware attacks.[14]

Assessment Notes

Follow-up Actions

ASTP

SAFER Guides 2024



SAFER Self-Assessment High Priority Practices | Recommended Practice 1.3 Worksheet | Domain 1 – Safe Health IT

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

Recommended Practice - Backup Data

Implementation Status

1.3 Patient data and software application configuration settings critical to the organization's operations are regularly backed up and tested.[10]
Checklist

EHR Limitation

Rationale for Practice or Risk Assessment

Failure of electro-mechanical devices is inevitable. Backup of mission-critical patient data and EHR system configuration allows system restoration to a "pre-failure" state with minimal data and time loss.

Suggested Sources of Input

1. Clinicians, support staff, and/or clinical administration
2. EHR developer
3. Health IT support staff

Strength of Recommendation

Required

Implementation Guidance

- The organization has a daily, off-site, complete, encrypted backup of patient data.[11]
- Critically important patient data should be backed up as close as possible to real-time.
- If using a remotely hosted EHR (e.g., cloud-based solution), the EHR provider backs up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.[12]
- The off-site backup is tested regularly (i.e., complete system and patient data restore) (optimally on at least a monthly basis).[13]
- The content required to configure the system is backed up regularly (optimally every month and always before every EHR or supporting computer system upgrade).
- The organization maintains multiple backups, which are created at different times.
- Backup media are physically secured in a location separate from the operational data stores.
- The backup storage media should be separate and distinct (e.g., Air gap) from normal file storage to facilitate recovery from ransomware attacks.[14]

Assessment Notes

Follow-up Actions

The *Suggested Sources of Input* section indicates categories of personnel who can provide information to help evaluate your level of implementation.

Strength of Recommendation section provides an estimate of the strength of evidence available in the scientific literature, or states that it is "required" due to a federal rule, regulation, or conditions of participation, for each recommendation.

ASTP

Select Recommendations from High Priorities Guide

Recommended Practice - Safety Culture

1.1 Highest-level decision makers in the organization (e.g., boards of directors, owners of physician practices, C-suite executives, and clinical leaders) commit to promoting a culture of safety that incorporates the safety and safe use of EHRs.

Select Recommendations from High Priorities Guide

Recommended Practice - Backup Data

1.3 Patient data and software application configuration settings critical to the organization's operations are regularly backed up and tested.[10]

Checklist

Implementation Guidance

- The organization has a daily, off-site, complete, encrypted backup of patient data.[11]
- Critically important patient data should be backed up as close as possible to real-time.
- If using a remotely hosted EHR (e.g., cloud-based solution), the EHR provider backs up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.[12]
- The off-site backup is tested regularly (i.e., complete system and patient data restore) (optimally on at least a monthly basis).[13]

Select Recommendations from High Priorities Guide

Recommended Practice - Artificial Intelligence

1.5

Artificial Intelligence (AI)-enabled application developers, EHR vendors, and healthcare organizations using AI-enabled systems or EHRs with enhanced AI features or functions share responsibility (based on their ability and resources available) for ensuring AI safety. This shared responsibility includes appropriate clinical, technical, and administrative governance, policies, procedures, people, and technologies to ensure AI is monitored and that its use is safe, secure, private, ethical, and equitable.[20]

Research

JAMA | Original Investigation

Effect of Restriction of the Number of Concurrently Open Records in an Electronic Health Record on Wrong-Patient Order Errors

A Randomized Clinical Trial

Jason S. Adelman, MD, MS; Jo R. Applebaum, MPH; Clyde B. Schechter, MD, MA; Matthew A. Berger, MD; Stan H. Reissman, MSW; Raja Thota, MS; Andrew D. Racine, MD, PhD; David K. Vawdrey, PhD; Robert A. Green, MD, MPH; Hojjat Salmasian, MD, MPH, PhD; Gordon D. Schiff, MD; Adam Wright, PhD; Adam Landman, MD; David W. Bates, MD, MSc; Ross Koppel, PhD; William L. Galanter, MD, PhD, MS; Bruce L. Lambert, PhD; Susan Paparella, MSN, RN; William N. Southern, MD, MS

JAMA | Viewpoint | AI in Medicine
November 27, 2024

Recommendations to Ensure Safety of AI in Real-World Clinical Care

Dean F. Sittig, PhD; Hardeep Singh, MD, MPH

Abstract | Full Text

JAMA. 2024; 10.1001/jama.2024.24598

This Viewpoint provides recommendations for health care organizations (HCOs) and clinicians to facilitate the use of artificial intelligence (AI)-enabled systems, including electronic health records with AI features, in routine clinical care and provides pragmatic guidance for HCOs and clinicians at all stages of AI implementation.

- Shared Responsibility
- Ensure quality of AI performance
- Record & Monitor AI performance
- Training programs for clinicians
- Mitigating Postimplementation Risks

https://jamanetwork.com/journals/jama/fullarticle/2827434

ASTP

The great French Marshall Lyautey once asked his gardener to plant a tree. The gardener objected that the tree was slow growing and would not reach maturity for 100 years. The Marshall replied, “In that case, there is no time to lose; plant it this afternoon!”

Thank You!

davidr.hunt@hhs.gov

Reach out via phone or web

202-690-7151

Feedback Form: https://www.healthit.gov/form/healthit-feedback-form

Stay connected, follow us on social media channels

@onc_healthIT

https://www.youtube.com/user/HHSONC

Subscribe to our weekly eblast at healthit.gov for the latest updates!