

ECRI's *Strategic Insights for Ambulatory Care* newsletter is being offered to CAPIC insureds at no cost. If you are interested in visiting any of the links in this edition, please contact Brad Dunkin, Assistant Vice President, at BDunkin@CAPphysicians.com.



July 16, 2024

Strategic Insights for Ambulatory Care is a biweekly service provided by ECRI and the Cooperative of American Physicians (CAP). We welcome your comments; please send them to AmbulatoryCareRM@ecri.org.



Spotlight on Diagnostic Excellence

An **estimated 2.59 million** diagnostic errors occur annually in the United States among patients with dangerous diseases, with nearly 800,000 resulting in serious harm or death. In addition, missed and delayed diagnoses are significant contributors to liability. These ECRI resources can help organizations build systems to support diagnostic excellence for high-risk conditions:

- Taking Action: Strategies to Support Early and Accurate Cancer Diagnoses [read more](#)
- Diagnostic Excellence in Dementia Care [read more](#)
- Infographic: The Road to the Correct Diagnosis [read more](#)



[View all Diagnostic Safety resources](#)

What's New?

New In-Person Course | Human Factors Engineering: Systems Thinking to Enhance Patient Safety

During this two-day live training, ECRI's human factors engineers will provide the foundational knowledge to understand and conduct proactive assessments and reactive near miss and adverse events assessments from a true systems perspective. Applications for CEUs have been made. [Register now!](#)

Patient Safety & Relations

WHO Issues First-Ever Report on the Global State of Patient Safety

What's the news. The World Health Organization (WHO) has published its first-ever WHO Report on Patient Safety, the [Global Patient Safety Report 2024](#), which offers a comprehensive overview of patient safety around the world and provides insights for policymakers, healthcare leaders, researchers, and patient safety advocates. The report includes case studies showcasing how different countries are learning and developing patient safety solutions in unique contexts.

Why it matters. Patient safety is essential to effective, safe healthcare, and yet only about one-third of countries have fully incorporated patient safety into their national strategies for achieving universal health coverage, according to WHO.

How ECRI can help. The resource collection [Risk Management Fundamentals](#) lists ECRI's resources covering patient safety, risk, and quality; engaging physician practices in patient safety; and more.

Worker & Environmental Safety

Less Than 10% of Physicians Responsible for Disruptive Behavior

What's the news. Less than 10% of physicians practicing at 193 participating hospitals have received a report of unprofessional behavior, according to a [study published June 6, 2024, in JAMA Network Open](#). The reports were submitted to the Coworker Concern Observation Reporting System, administered by the Vanderbilt Center for Patient and Professional Advocacy. Surgeons were the most likely to receive reports, and nonsurgeon nonproceduralists were the least likely; there was no significant difference between pediatric and nonpediatric providers. Examples of disruptive behavior varied, and included a physician who called a nurse a "bossy cow" for reminding him of the need to conduct a preprocedural time-out, and threatening a

nurse who advocated waiting for a patient's spouse to arrive at the hospital to sign consent forms rather than signing the forms herself.

Why it matters. Disruptive practitioner behavior is about more than hurt feelings. When a provider creates an environment in which others find it difficult to safely do their work, it must be treated as a critical patient safety issue.

How ECRI can help. The guidance article [Disruptive Practitioner Behavior](#) covers types of disruptive behavior, its possible consequences for healthcare organizations, and interventions organizations can use to lessen or mitigate disruptive behavior.

Legal & Regulatory

Doctor Accused of Stealing PHI of Children Receiving Gender-Affirming Care

What's the news. A Texas doctor has been indicted for illegally obtaining protected health information (PHI) for pediatric patients not under his care and without authorization, according to a [June 17, 2024, press release](#) from the United States Attorney's Office. Intending to act as a whistleblower against a major Texas children's hospital for providing transgender care to pediatric patients, the accused doctor turned over the names of pediatric patients, their attending physicians, and treatment codes to a media contact; however, transgender care for minors was legal at the time, and the hospital announced in 2022 that it would stop providing such care, according to a [June 18, 2024, Associated Press article](#).

Why it matters. Maintaining the security of PHI is a matter of patient safety, not just regulatory compliance. The HIPAA privacy rule, issued by HHS under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, is a set of federal standards for safeguarding individuals' PHI maintained or transmitted in any form or medium. As required by the HIPAA security rule issued by HHS in 2003, covered entities and business associates must implement reasonable and appropriate administrative, technical, and physical safeguards for protecting the PHI they create, maintain, or transmit.

How ECRI can help. The guidance articles [The HIPAA Privacy Rule](#) and [The HIPAA Security Rule](#) discuss the fundamentals of each rule and major areas of concern for risk managers responsible for covered healthcare providers.

FBI, HHS Warn of Phishing Scheme Targeting Healthcare Organizations

What's the news. The U.S. Federal Bureau of Investigation (FBI) and the Department of Health and Human Services HHS are warning healthcare organizations of hackers engaging in a social engineering campaign, using phishing schemes to steal login credentials to access and divert automated clearinghouse payments to US controlled bank accounts, according to a [June 24, 2024, joint advisory](#). HHS and FBI urge healthcare leaders to implement recommended mitigations to protect

organizations against attacks, including implementing multifactor authorization for every account, training for IT help desk employees, and checking phone logs for contact with certain phone numbers.

Why it matters. Phishing attacks can lead to HIPAA violations through data breaches, financial fraud, reputational damage, and more. They also take many forms, such as targeted campaigns through email or phone, so it is vital to educate employees about the importance of security policies and procedures.

How ECRI can help. The guidance article [Cybersecurity in Ambulatory Care](#) can help risk managers better understand their organizations' current approaches, identify opportunities for improvement, and clearly define their roles in cybersecurity within their organizations.

HHS Final Rules Establishes Disincentives for Information Blocking

What's the news. The U.S. Department of Health and Human Services released a final rule establishing disincentives for healthcare providers that have committed information blocking, according to a [June 24, 2024, HHS press release](#). The final rule exercises HHS's authority under the 21st Century Cures Act to establish disincentives for healthcare providers who engage in practices that they knew were unreasonable and likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information, except as required by law or covered by a regulatory exception, HHS says.

Why it matters. Patients have a right to access their own health information. Patient access to health information, as required by law, allows coordinated, efficient, and informed patient care.

How ECRI can help. The article [The Information Blocking Rule](#) summarizes the primary requirements of the Information Blocking Rule, which was promulgated pursuant to the 21st Century Cures Act.



ECRI and ISMP Headquarters, 5200 Butler Pike, Plymouth Meeting, PA 19462, 610.825.6000