Risk Management SNAPSHOT

Current issues and hot topics in healthcare risk management.

CMS Warns About Medical Records Request Scam

Unauthorized release of medical records can result in HIPAA fines and damage to your organization's reputation. It is important to verify the authenticity of any requests for protected health information. CMS has recently released a warning about phishing attempts to gain access to medical records.

Medical Records Request Scam: Watch out for Phishing

CMS identified phishing scams for medical records. This may include scammers faxing you fraudulent medical records requests to get you to send patient records in response; see example (PDF)

When you review any requests, look for signs of a scam, including:

- Directing you to send records to an unfamiliar fax number or address
- Referencing Medicare.gov or @Medicare (.gov)
- Indicating they need records to "update insurance accordingly"

A scam request may include:

- Poor grammar, misspellings, or strange wording
- Incorrect phone numbers
- Skewed or outdated logos
- Graphics that are cut and pasted

If you think you got a fraudulent or questionable request, work with your Medical Review Contractor to confirm if it's real. Submit medical documentation through the Electronic Submission of Medical Documentation (esMD) system or CMS medical review contractor secure internet portals, when available.

For more information about HIPAA compliance, take a look at Medical Mutual's HIPAA checklist.

This article falls under LEGAL/REGULATORYin the Enterprise Risk Management (ERM) risk domains.

Risk within this domain incorporates the failure to identify, manage, and monitor legal, regulatory, and statutory mandates on a local, state, and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property.

White House Partners with Microsoft, Google on Cybersecurity for Rural Hospitals

With rising cybersecurity attacks focused on healthcare organizations, what is being done for our rural healthcare systems? The technology giants will offer free or low-cost cybersecurity tools to rural hospitals, which often have limited resources to combat the rising number of cyberattacks.

A recent news brief was put out by Healthcare Dive in early June titled White House partners with Microsoft, Google on cybersecurity for rural hospitals. The brief discusses how rural healthcare organizations are a focus for the White House and technology giants. Cyberattacks against the U.S. healthcare sector increased 128% from 2022 to 2023, according to the Office of the Director of National Intelligence. The programs from Microsoft and Google aim to enhance infrastructure, improving security and resilience at rural facilities.

This article falls under TECHNOLOGY in the Enterprise Risk Management (ERM) risk domains.

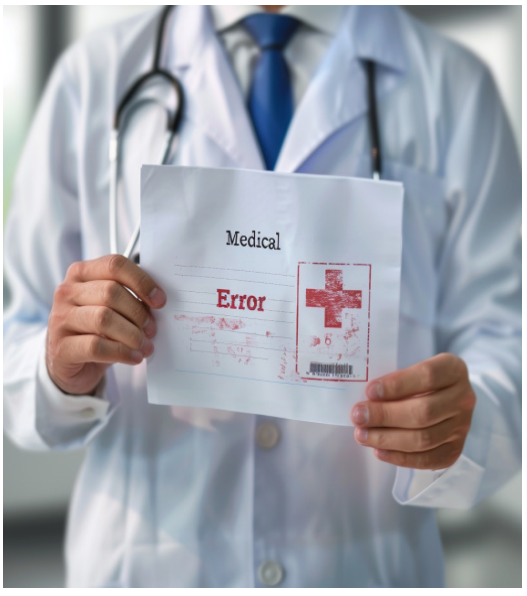
This domain covers machines, hardware, equipment, devices, wearable technologies and tools, but can also include techniques, systems and methods of organization. Health care has seen an escalation in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Electronic Health Records (EHR) and Meaningful Use, financial and billing systems, social media and cyber security; cyber risks can be significant.

ISMP Updates List of Error-Prone Abbreviations

In April 2024, ISMP updated the List of Error-Prone Abbreviations, Symbols, and Dose Designations. The list contains abbreviations, symbols, and dose designations that have led to patient harm and should not be used when communicating medical information.

Abbreviations, symbols, and certain dose designations are a convenience; a time saver; a means of fitting a word, phrase, or dose into a restricted space; and a way to avoid misspellings. However, they are sometimes misunderstood, misread, or misinterpreted, occasionally resulting in patient harm. Their use can also waste time tracking down their meaning, sometimes delaying patient care. The abbreviations, symbols, and dose designations were reported to ISMP through the ISMP National Medication Errors Reporting Program (ISMPMERP) and have been misinterpreted and involved in harmful or potentially harmful medication errors. They should NOT be used when communicating medical information verbally, electronically, and/or in handwritten applications. This includes inter-

© 2024 Medical Mutual Mutual Insurnace Company of Maine



nal communications; verbal, handwritten, or electronic prescriptions; handwritten and computer-generated medication labels; drug storage bin labels; medication administration records; and screens associated with pharmacy and prescriber computer order entry systems, automated dispensing cabinets, smart infusion pumps, and other medication-related technologies.

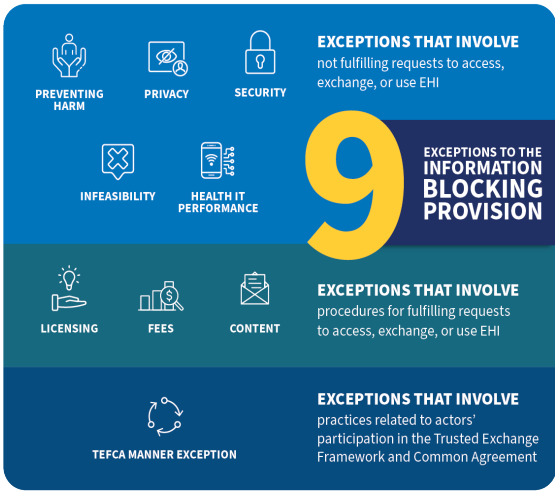
The updated list can be found here.

For additional information about medication safety, check out Medical Mutual's practice tip Medication Safety in the Office Practice.

This article falls under **Clinical/Patient Safety** *in the Enterprise Risk Management (ERM) risk domains.*

Risks associated with the delivery of care to patients, residents and other health care customers. Clinical risks include: failure to follow evidence based practice, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), health care equity, opportunities to improve safety within the care environments, and others.

HHS Finalizes the Information Blocking Disincentive Rule



On June 24, 2024, the U.S. Department of Health and Human Services (HHS), which oversees the federal law known as the Health Insurance Portability and Accountability Act (HIPAA), finalized a rule that would cost healthcare providers and facilities significant financial penalties for improper information blocking.

In a final follow-up to articles in past Snapshot newsletters, Blocking Information in Your EHR Might Cost You (February 2024) and Associations Starting to Speak Out on the Pending Information Blocking Rule Changes (May 2024), the U.S. Department of Health and Human Services (HHS) has finalized a rule which firmly establishes financial disincentives for health care organizations and providers who have committed information blocking.

You can read the press release here: HHS Finalizes Rule Establishing Disincentives for Health Care Providers That Have Committed Information Blocking

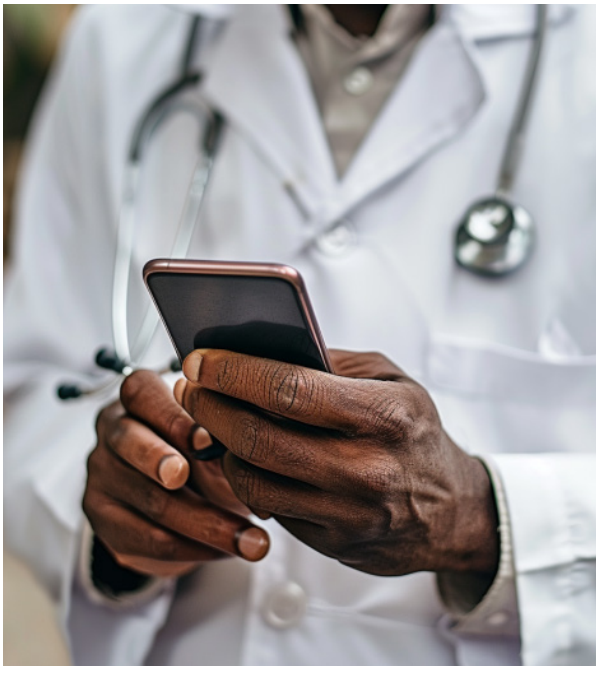
In recognition of the financial significance even one finding of information blocking could have, we recommend organizations and practices take the time to proactively review their current practices and electronic health record (EHR) settings. If changes need to be made, implement those as soon as possible and ensure good documentation is retained to show your intention.

© 2024 Medical Mutual Mutual Insurnace Company of Maine

This article falls under **LEGAL/REGULATORY** *in the Enterprise Risk Management (ERM) risk domains.*

Risk within this domain incorporates the failure to identify, manage, and monitor legal, regulatory, and statutory mandates on a local, state, and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property.

Use of Texting for Patient Orders



Communication between care team members outside of the electronic health record (EHR) can be tricky to manage. Although many organizations have integrated secure texting platforms (STP) to allow texting patient information more safely, communicating orders was not permitted outside of the EHR. Effective immediately, The Joint Commission has updated its position on this.

On June 5, 2024, The Joint Commission released a new position statement, Use of secure text messaging for patient information and orders. This statement follows the endorsement of CMS, which was released in February of this year QSO-24-05-Hospital-CAH. Recognizing that computerized provider order entry (CPOE) will remain the preferred method of order entry, Joint Commission-accredited healthcare organizations will now be allowed to use appropriately configured STPs to communicate patient information and orders, which transmit directly into the EHR.

Medical Mutual has a practice tip on Mobile Devices that can help you assess your current communication process.

This article falls under **TECHNOLOGY** *in the Enterprise Risk Management (ERM) risk domains.*

This domain covers machines, hardware, equipment, devices, wearable technologies and tools, but can also include techniques, systems and methods of organization. Health care has seen an escalation in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Electronic Health Records (EHR) and Meaningful Use, financial and billing systems, social media and cyber security; cyber risks can be significant.

© 2024 Medical Mutual Mutual Insurnace Company of Maine