AMERICAN MEDICAL ASSOCIATION PRIVATE PRACTICE PHYSICIANS SECTION

Resolution: 2
(A-24)

Introduced by: Alex Shteynshlyuger, MD

Subject: Change Healthcare Security Lapse—The FBI Must Investigate

Referred to: PPPS Reference Committee
(xxxx, MD, Chair)

---

Whereas, the Change Healthcare security compromise has as yet unknown long-term repercussions on the healthcare industry, with hundreds of thousands of affected third parties; and

Whereas, the issue affects national self-interest, of significant relevance to third parties, including physicians, hospitals, and other healthcare providers as well as consumers, with close to half of the United States population affected, according to Change Healthcare; and

Whereas, the mission of the Federal Bureau of Investigation is to protect the American people and uphold the Constitution of the United States; and

Whereas, United Healthcare has a self-interest in minimizing its own culpability and the severity of the security breach which may preclude other parties from instituting adequate safeguards to prevent similar security incidents in the future; therefore be it

Resolved, that our American Medical Association issue a formal public request that the Federal Bureau of Investigation investigate Change Healthcare's cybersecurity incident and issue a public report and the cause of the security breach, determining whether it is preventable and how (Directive to Take Action); and be it further

Resolved, that our AMA convene a workgroup on legal issues arising from the Change Healthcare breach, including but not limited to resultant interruption of business practices, increase in the costs of electronic transactions, increase in liability and financial losses and report back at Interim 2024 on the feasibility to pursue legal action on behalf of private practice physicians and possibly in collaboration with the American Hospital Association (Directive to Take Action).

Fiscal Note: TBD

Received: 4/29/2024

## RELEVANT AMA POLICY

### Indemnity for Breaches in Electronic Health Record Cybersecurity D-315.977

Our AMA will advocate for indemnity or other liability protections for physicians whose electronic health record data and other electronic medical systems become the victim of security compromises.

Citation: Res. 221, I-15

### 3.3.3 Breach of Security in Electronic Medical Records

When used with appropriate attention to security, electronic medical records (EMRs) promise numerous benefits for quality clinical care and health-related research. However, when a security breach occurs, patients may face physical, emotional, and dignitary harms.

Dedication to upholding trust in the patient-physician relationship, to preventing harms to patients, and to respecting patients' privacy and autonomy create responsibilities for individual physicians, medical practices, and health care institutions when patient information is inappropriately disclosed.

The degree to which an individual physician has an ethical responsibility to address inappropriate disclosure depends in part on his or her awareness of the breach, relationship to the patient(s) affected, administrative authority with respect to the records, and authority to act on behalf of the practice or institution.

When there is reason to believe that patients' confidentiality has been compromised by a breach of the electronic medical record, physicians should:

(a) Ensure that patients are promptly informed about the breach and potential for harm, either by disclosing directly (when the physician has administrative responsibility for the EMR), participating in efforts by the practice or health care institution to disclose, or ensuring that the practice or institution takes appropriate action to disclose.

(b) Follow all applicable state and federal laws regarding disclosure.

Physicians have a responsibility to follow ethically appropriate procedures for disclosure, which should at minimum include:

(c) Carrying out the disclosure confidentially and within a time frame that provides patients ample opportunity to take steps to minimize potential adverse consequences.

(d) Describing what information was breached; how the breach happened; what the consequences may be; what corrective actions have been taken by the physician, practice, or institution; and what steps patients themselves might take to minimize adverse consequences.

(e) Supporting responses to security breaches that place the interests of patients above those of the physician, medical practice, or institution.

(f) Providing information to patients to enable them to mitigate potential adverse consequences of inappropriate disclosure of their personal health information to the extent possible.

Citation: Issued 2016