Electronic Health Records

Detecting and Investigating Unauthorized Access to Electronic Health Records—A Case Study

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Content Summary

This booklet uses a case study to illustrate the strengths and weaknesses of a hospital's efforts to prevent, detect, and investigate unauthorized disclosure of personally identifiable patient health information. Failure to monitor employee access to this information allowed the scheme to continue for 3 years. Once the hospital got indications of the scheme, officials were able to use the electronic health record (EHR) audit log to support an investigation that led to guilty pleas and punishment for those responsible. Through the case study, providers and others will see opportunities to improve their own EHR program integrity measures.

Introduction

Electronic health record (EHR) technology, while providing the opportunity for increased efficiency and improved communication, can make it easier to commit fraud or abuse. It is easier and quicker to fabricate and alter records or sort, retrieve, and export them than with paper records. A 2012 case involving the sale of personally identifiable information taken from an EHR illustrates both EHR vulnerabilities and using an EHR system to detect and investigate illegal activities.

A Hospital Employee Is Recruited to Steal Patient Electronic Health Records

A hospital emergency room (ER) employee and his wife worked for a large not-for-profit hospital business with 22 locations in Florida.[1] The employee's job was to register patients, including those who arrived by ambulance, to the ER. He had access to patient information through the EHR system for locations across central Florida. In 2009, the employee met a manager of two chiropractic clinics who volunteered at the hospital. The manager recruited the hospital employee to participate in an illegal scheme involving EHRs. Specifically, the manager convinced the employee to use his EHR system access to identify ER patients involved in motor vehicle accidents. He obtained patient contact information and details on the circumstances of the accidents. He forwarded this information to the manager. The manager's employees then solicited the patients for chiropractic and legal services.[2] The manager paid the ER employee for his services.

A 2013 survey of hospitals and clinics with EHR systems in Minnesota found that only about 34 percent of hospitals and 57 percent of clinics performed monitoring and audits of unauthorized access because of alerts generated by their EHR systems.[4]

The employee engaged in this conduct from late 2009 until mid-2011. In July 2011, the hospital terminated the employee for having improperly accessed the health information of a physician fatally shot in one of the hospital's parking garages.[3] When the hospital terminated the employee, it did not examine the audit log's record of his other EHR access events and remained unaware of his other misconduct.

A Patient Complaint Leads to an Investigation

The hospital discovered the employee's additional misconduct in the most common way for cases of unauthorized access: a patient complaint.[5] After the hospital fired the employee, the manager recruited his wife to continue the scheme.[6] A month later, in August 2011, a nurse employed by the hospital complained that she received a solicitation call regarding her daughter. Her daughter was involved in a traffic accident and brought to the hospital's ER. The caller asked to speak to her daughter, recited details of the accident, and offered to provide a lawyer. After receiving the complaint, the hospital examined the EHR audit log entries for access to the patient's record. These records showed that the wife and another hospital employee improperly accessed information on this patient. The wife and the other employee denied it, but the hospital terminated them.

Patient complaints can be a good source of information about unauthorized access to EHRs.

Providers and others should take corrective action when they discover unauthorized access.

The hospital began a thorough examination of access to records in the EHR log to identify any other suspicious access events.[7] The log showed that someone accessed thousands of records from a computer terminal the employee used.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act, part of the American Recovery and Reinvestment Act of 2009, or ARRA)[8] requires reporting unauthorized disclosure of protected health information to the Secretary of the U.S. Department of Health and Human Services (HHS). Reporting breaches involving the records of 500 or more individuals is required "immediately." Under HHS rules this means without unreasonable delay and no later than 60 calendar days after discovery of a breach. HHS requires reporting other breaches within 60 calendar days after the end of the calendar year the breach occurred. HHS requires breaches involving the records of 500 individuals or more be disclosed through the media and posted on the HHS website.[9, 10]

The Hospital and Law Enforcement Use the EHR Audit Log to Identify the Culprit

After terminating the wife and the other employee in October 2011, the hospital referred the case to law enforcement. An agent with the Federal Bureau of Investigation (FBI) began working closely with the hospital to investigate the case. The hospital provided data from the EHR log to the agent. The data showed that from late 2009 through July 2011, someone using the ER employee's user name and password viewed summary information on more than 763,000 patients from one of the computer terminals used by the employee.[11] Using the log, the hospital showed that other ER representatives working during this period normally accessed 12,100 patient records. The EHR log showed not only that the number of access events was unusually high, but also that these events included the records of many patients admitted to ERs other than the one where the employee worked. From interviewing hospital employees, the FBI agent established how rare it was for an ER representative to have a legitimate business need to access records of patients admitted to another ER.[12] This proof showed that the access was unauthorized.

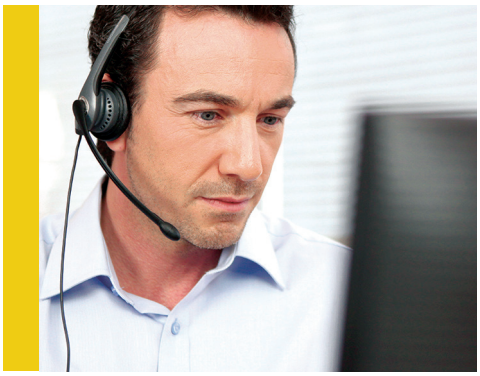
The EHR audit log showed that a user viewed health information of 763,000 patients and that the duties of the assigned position required access to 12,100 patient records.

Proving that unauthorized access occurred was easier than proving that the employee was responsible. Hospital employees shared system passwords, and the system permitted employees to log in to more than one computer at a given time.[13]

Providers should have policies that prohibit sharing passwords and simultaneously logging into the system from different terminals.

To eliminate the possibility that a person other than the employee used the password and the terminals to access the records, the hospital did a match between the audit log information and payroll records. This match showed that the unauthorized access occurred from terminals used by the employee clocked in during those times.[14]

To prove that the employee accessed the information, and wrongfully disclosed it to the manager of the chiropractic clinics, the investigating agent made further use of the EHR log, as well as traditional investigative tools. The audit log showed that the employee repeatedly accessed a particular type of screen that showed 10 patient records at a time, and that the employee viewed most screens for less than one second. Other screens he viewed for longer than one second contained either the record of a patient involved in a motor vehicle accident or a record that he accessed additional screens. This information was consistent with the employee seeking to identify patients involved in motor vehicle accidents and then using the system to obtain more information on these patients, including details about the accidents that he could sell to the chiropractic clinic manager. Using the log, the hospital identified more than 12,000 patients whose records were improperly accessed and were involved in a motor vehicle accident before admission to the ER.



From an examination of bank and telephone records, the FBI agent determined that the employee and his wife received checks from the manager. Telephone records showed that the employee talked to or exchanged texts with the manager.[15] The employee could not satisfactorily explain the payments or the contacts. Additionally, through witness interviews, the agent established that some of the patients the employee identified received telephone solicitations within days of their visit to one of the hospital system's ERs. The calls came to the contact telephone numbers that the patients provided to the hospital upon admission. The callers knew the details of the accidents as reported in the EHR. For example, on October 22, 2010, the audit log showed an ER-admitted patient was involved in a motor vehicle accident. On October 25, 2010, the employee viewed the records of this patient. After the employee viewed the information, the patient received a solicitation call from a person associated with an injury hotline operated by the clinic manager.[16] The log evidence and other proof pointed to the ER employee's guilt.

The Employee and His Co-Conspirators Are Charged and Plead Guilty

Providers and others can use information obtained from the EHR log to assist in prosecuting those who wrongfully disclose individually identifiable health information.

In August 2012, the United States Attorney's Office (USAO) charged the ER employee with conspiracy and wrongful disclosure of individually identifiable health information.[17, 18] The USAO also charged the employee's wife and the chiropractic clinic manager. Despite initial denials, the employee pleaded guilty just a little more than 2 months later. In his plea agreement, he admitted illegally obtaining access to the EHRs of more than 12,000 patients in order to sell the information to the chiropractic clinic manager. The judge sentenced him to 12 months and 1 day in Federal prison.[19, 20] The chiropractic clinic manager pleaded guilty to the same offenses and the judge sentenced her to 4 years. The employee's wife pleaded guilty to conspiracy and the judge sentenced her to 2 years probation and 25 hours of community service.[21] The maximum punishment for the conspiracy offense is 5 years.[22, 23] This case involved theft and fraud. When starting their employment with the hospital, the employee and his wife signed agreements to access EHRs only for legitimate job-related purposes.[24] When they accessed the records for illegitimate purposes, they were misrepresenting their intentions and perpetrating fraud.

Lessons Learned

Although the hospital in this case did not do a comprehensive investigation when it discovered someone had improperly accessed the doctor's EHR, it did undertake an investigation when a nurse later complained of another instance of unauthorized access. The hospital's response to the nurse's complaint illustrates ways providers and others can use the EHR system to determine the extent of unauthorized access and to identify those responsible. The case also suggests additional steps providers can take to make their efforts to prevent, detect, and investigate suspected EHR fraud, waste, and abuse more effective. These steps include adopting policies that:

- Prohibit sharing system passwords and logging in to the system from more than one computer terminal at a time; and
- Require, when a potential violation is identified, the following:
  - A thorough investigation;
  - When appropriate, well-publicized disciplinary action and referral to law enforcement; and
  - Additional corrective action in the form of measures to ensure no wrongful disclosure reoccurs.

In addition to adopting policies, providers should conduct:

- Ongoing monitoring of EHR access; and
- Audits of EHR access, periodically and when identifying abnormal patterns or receiving complaints.

All of these steps—internal monitoring and auditing, written policies, prompt responses to detected offenses, and corrective action—are elements of the compliance plan required by the Centers for Medicare & Medicaid Services (CMS) for certain managed care plans[25] and are recommended by the U.S. Department of Health and Human Services, Office of Inspector General for many types of providers.[26] Eventually CMS will require all Federal health care program providers to have a compliance program,[27] so any provider without one should develop and implement a robust compliance program now. Providers that already have a compliance program in place should review it to determine whether it addresses the concerns associated with EHRs.

Conclusion

This case study illustrates ways providers and others can use an EHR audit log to prevent, detect, and investigate EHR fraud. When a nurse complained about circumstances suggesting improper access, the hospital used the EHR audit log to confirm the violation and to detect the existence of numerous related violations. The log provided strong circumstantial evidence that led to guilty pleas and punishment for those responsible. Providers can learn from this experience to make their own compliance plans more effective in preventing, detecting, and investigating fraud, waste, and abuse associated with EHRs.

To see the electronic version of this booklet and the other products included in the "Electronic Health Records" Toolkit posted to the Medicaid Program Integrity Education page, visit https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the CMS website.

Follow us on Twitter #MedicaidIntegrity

References

1 Criminal Complaint at 2, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

2 Federal Bureau of Investigation. (2013, April 10). Davenport Man Sentenced to Four Years in Prison for Theft of Patient Information. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2013/davenport-man-sentenced-to-four-years-in-prison-for-theft-of-patient-information

3 Criminal Complaint at 9–10, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

4 Minnesota Department of Health. (2013, February). Minnesota Health Records Access Study (p. 19). Retrieved April 1, 2016, from http://www.health.state.mn.us/e-health/hras/hras021913report.pdf

5 Minnesota Department of Health. (2013, February). Minnesota Health Records Access Study (p. 19). Retrieved April 1, 2016, from http://www.health.state.mn.us/e-health/hras/hras021913report.pdf

6 Federal Bureau of Investigation. (2013, January 18). Former Florida Hospital Employee Sentenced to Federal Prison for Data Theft. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2013/former-florida-hospital-employee-sentenced-to-federal-prison-for-data-theft

7 Criminal Complaint at 9–10, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

8 American Recovery and Reinvestment Act. Pub. L. 111-5, Title XIII, 123 Stat. 115, 226. Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

9 Notification in the Case of Breach, 42 U.S.C. § 17932(d)(1), (e). Retrieved June 16, 2015, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap156-subchapIII-partA-sec17932.pdf

10 Notification to the Secretary, 45 C.F.R. § 164.408. Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-408.pdf

11 Criminal Complaint at 4–5, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

12 Criminal Complaint at 4–5, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

13 Criminal Complaint at 10, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

14 Criminal Complaint at 5–6, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

15 Criminal Complaint at 10–12, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

16 Criminal Complaint at 7–8, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

17 Florida Department of Financial Services. Enforcement Action Notification. Retrieved April 1, 2016, from http://www.myfloridacfo.com/Division/Fraud/EAN/PIP/documents/1-14-2013_12-217_EAN_P_EC.pdf

18 Wrongful Disclosure of Individually Identifiable Health Information, 42 U.S.C. § 1320d-6(a). Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partC-sec1320d-6.pdf

19 Federal Bureau of Investigation. (2012, October 22). Former Florida Hospital Employee Pleads Guilty to Data Theft. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2012/former-florida-hospital-employee-pleads-guilty-to-data-theft

20 Federal Bureau of Investigation. (2013, January 18). Former Florida Hospital Employee Sentenced to Federal Prison for Data Theft. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2013/former-florida-hospital-employee-sentenced-to-federal-prison-for-data-theft

21 U.S. Attorney's Office. Middle District of Florida. Orlando Branch Office. (2013, July 8). Representative search of office database. Retrieved April 1, 2016, via phone call to branch office.

22 Federal Bureau of Investigation. (2013, April 10). Davenport Man Sentenced to Four Years in Prison for Theft of Patient Information. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2013/davenport-man-sentenced-to-four-years-in-prison-for-theft-of-patient-information

23 Federal Bureau of Investigation. (2013, January 18). Former Florida Hospital Employee Sentenced to Federal Prison for Data Theft. Retrieved April 1, 2016, from https://www.fbi.gov/tampa/press-releases/2013/former-florida-hospital-employee-sentenced-to-federal-prison-for-data-theft

24 Criminal Complaint at 3–4, United States v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved April 1, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

25 42 C.F.R. § 438.608(b)(6). Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/CFR-2009-title42-vol4/pdf/CFR-2009-title42-vol4-sec438-608.pdf

26 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Physician Practices. 65 Fed. Reg. 59434, 59436. Retrieved April 1, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

27 Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6401(a)(3), (b)(1), 124 Stat. 119, 751, 752, (2010, March 23). Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf

Disclaimer

This booklet was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This booklet was prepared as a service to the public and is not intended to grant rights or impose obligations. This booklet may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

June 2016