Received: 11 October 2023 | Revised: 28 January 2024 | Accepted: 31 January 2024

DOI: 10.1002/emp2.13130

JACEP OPEN
JOURNAL OF THE AMERICAN COLLEGE OF EMERGENCY PHYSICIANS OPEN
A GLOBAL JOURNAL OF EMERGENCY MEDICINE
Open Access
WILEY

SPECIAL CONTRIBUTION

Ethics

Privacy and confidentiality of emergency department patient information: Contemporary considerations and challenges

Jay M. Brenner MD[1] | Michele Y. Delpier MD[2] | Jeremy R. Simon MD[3] | Joel M. Geiderman MD[4] | Catherine A. Marco MD[5] | John C. Moskop PhD[6] | On behalf of the American College of Emergency Physicians Ethics Committee

[1]Department of Emergency Medicine, SUNY-Upstate Medical University, Syracuse, New York, USA

[2]Dover, DE, Bayhealth Emergency Physicians, Syracuse, New York, USA

[3]Department of Emergency Medicine, Columbia University, Syracuse, New York, USA

[4]Department of Emergency Medicine, UCLA-Cedars Sinai, Syracuse, USA

[5]Department of Emergency Medicine, Penn State Health, Syracuse, USA

[6]Department of Medicine, Winston-Salem, Wake Forest University, Syracuse, USA

Correspondence
Jay M. Brenner, MD, SUNY-Upstate Medical University, Syracuse, NY, USA.
Email: brennerj@upstate.edu

Abstract

This article provides a brief review of moral and legal duties to respect confidentiality in emergency medicine. The article considers current challenges to confidentiality in emergency departments and proposes strategies to address them. It is offered as an update of the two-part review of confidentiality in emergency medicine in 2005 by Moskop et al published in 2005 in *Annals of Emergency Medicine*.

1 | INTRODUCTION

Respecting and protecting the confidentiality of patient information is widely accepted as an obligation of health care professionals. Explicitly recognized in the Hippocratic Oath,[1] confidentiality also features in multiple current codes of ethics, including the American College of Emergency Physicians (ACEP)'s *Code of Ethics for Emergency Physicians*.[2] Multiple statutes, regulations, and public policy statements in the United States and across the globe establish legal responsibilities to protect patient information.

In a 2005 review of confidentiality in emergency medicine, Moskop et al state that protecting confidentiality is both more difficult and more important in the emergency department (ED) than in other medical practice settings.[3,4] Maintaining confidentiality in the ED is difficult because treatment spaces are often open and crowding is endemic. Crowded ED environments may necessitate interacting with patients in proximity to others. Breaches of privacy may occur in the ED and can negatively effect patient satisfaction and comfort.[5,6] Others nearby may then overhear medical information. Despite these challenges, protecting the confidentiality of medical information in the ED is important because many patients present to the ED for treatment of sensitive conditions, such as sexual assault or mental illness. The Moskop et al is updated by examining issues that have newly arisen in the last 20 years and recommendations for preserving patient confidentiality in the ED are offered.

2 | CONCEPTUAL, MORAL, AND LEGAL FOUNDATIONS

We will follow the 2005 *Annals* article by starting with the conceptual, moral, and legal foundations of patient confidentiality.

Supervising Editor: Henry Wang, MD, MS

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.
© 2024 The Authors. *Journal of the American College of Emergency Physicians Open* published by Wiley Periodicals LLC on behalf of American College of Emergency Physicians.

2.1 | Basic concepts

To obtain effective care, patients or their representatives need to communicate pertinent medical information. Clinicians who receive such information have a responsibility to protect it from disclosure to others who have no right to it.[3]

Additionally, it is important to note at the outset that "privacy" has meanings in ethics and law, including *physical privacy, decisional privacy*, and *informational privacy*. Physical privacy refers to freedom from contact with other people or exposure of one's body to others. Decisional privacy refers to the freedom to make and act on personal choices without interference from others. Informational privacy refers to the ability to control the collection, use, and disclosure of personal information.[7,8] In this article, we will only use "privacy" in the sense of informational privacy.

2.2 | Moral foundations and limits of confidentiality

Cogent moral reasons support the responsibility of emergency physicians (EPs) to protect their patients' personal health information (PHI). The practice reflects recognition of the dignity and moral worth of patients. Furthermore, confidence that clinicians will respect the confidentiality of sensitive information encourages patients to communicate without reservation, thus helping clinicians make accurate diagnoses and recommend effective treatments. On the other hand, failure to protect the confidentiality of PHI may cause significant harm, including stigmatization and discrimination based on patients' medical conditions. Despite its moral significance, however, protecting the confidentiality of health information is not an absolute professional duty. It may sometimes be overridden by other duties, including duties to protect the patient or other parties from harm or to obey the law. When EPs encounter a conflict between apparent duties, they must evaluate the strength of the conflicting claims in order to determine their actual moral duty under the circumstances.[9,10]

2.3 | Legal foundations and limits of confidentiality

For more than a century, US court decisions and federal and state statutes have recognized professional responsibilities to protect the confidentiality of PHI. Professionals who disclose confidential information without adequate justification may be liable for damages if patients are harmed by that disclosure. Regulations implemented under the Health Insurance Portability and Accountability Act (HIPAA) impose additional duties on both individual clinicians and health care organizations to protect the confidentiality of PHI.[11] HIPAA itself uses the term Protected Health Information (Table 1).

HIPAA privacy regulations permit disclosure of PHI without patient consent for purposes of treatment, payment, and health care operations. They also permit disclosure of PHI for "twelve national priority purposes," including reporting of transmissible diseases, reporting of suspected patient abuse or neglect, suspected terrorist activities, and organ and tissue donation. The US Office of Civil Rights may impose monetary penalties and imprisonment for wrongful disclosure of HIPAA-protected PHI.

TABLE 1 Personal health information (PHI)-specific elements.

PHI-specific element
Names
Dates, except year
Telephone numbers
Geographic data
FAX numbers
Social security numbers
Email addresses
Medical record numbers
Account numbers
Health plan beneficiary numbers
Certificate/license numbers
Vehicle identifiers and serial numbers including license plates
Web URLs
Device identifiers and serial numbers
Internet protocol addresses
Full face photos and comparable images
Biometric identifiers (ie, retinal scan, fingerprints)
Any unique identifying number or code

In addition to the above-mentioned HIPAA exceptions to confidentiality duties, US common law permits or requires disclosure of PHI in several circumstances. Most notable among these disclosures is a "duty to warn" third parties of foreseeable risks to them posed by a patient, and a duty to disclose patient information to the authorized representatives of minor patients and of patients who lack decision-making capacity. This disclosure is necessary to enable representatives to make informed treatment decisions on behalf of patients. Many states, however, grant decision-making authority and confidentiality protections to minors for specific medical conditions, including pregnancy, substance use disorders, mental illness, and sexually transmitted diseases.[12,13]

2.4 | Challenges to confidentiality in the ED

2.4.1 | Perennial and past obstacles to ED confidentiality

The 2005 *Annals of Emergency Medicine* article also examines specific challenges for the protection of patient confidentiality that were commonly encountered in hospital EDs at that time.[4] Several of the challenges considered in that article remain in 2024. ED crowding, with its resultant lack of physical privacy in which to discuss PHI, has become endemic. As risks to the safety of ED patients and staff posed by violent patients or visitors have increased, so too has the risk to

confidentiality, and physical privacy, with observation by hospital security or law enforcement officers.[14,15] These risks may be mitigated as described below. Notably, HIPAA permits access to PHI by personnel who are necessary for treatment, payment, and health care operations activities, as security personnel certainly are.

Several other ED confidentiality issues examined in the 2005 article have since been largely resolved. The former practice of keeping "habitual patient files" to document patients suspected of seeking drugs has become obsolete in today's era of prompt access to electronic health records (EHRs) that include information about drug use and prescriptions. The practice of filming ED care for commercial reality TV programs has become less frequent after adoption of multiple professional society policy statements and multiple successful lawsuits for invasion of privacy. These developments discourage commercial filming unless both ED patients and staff provide prospective informed consent.

2.5 | Novel challenges to ED confidentiality

2.5.1 | Electronic communication

Communication in the health care setting has undergone major changes over the past two decades. Electronic communications, including social media, texting, and EHRs, pose novel challenges to confidentiality. This section will address the new challenges to patient confidentiality electronic communication pose and suggest strategies to mitigate the associated risks.[16,17]

2.6 | Social media

An early approach to social media in health care recommended avoiding or prohibiting its use completely to protect patient confidentiality. More recent approaches have endorsed its limited use when not directly related to a specific patient. For example, anesthesiologists used Twitter to share best practices of airway management during the COVID-19 pandemic.[18] Commentators have suggested that a "3Ps" rule be used prior to posting: a post should be a message one is comfortable being viewed by one's patients, professional colleagues, and public relations office.[19] It is best to assume that information on social media is public. Unencrypted electronic communications, including social media postings, must avoid including PHI. Even de-identified stories with vulgar or suggestive content may be distasteful and unprofessional and reflect poorly on an individual, department, or institution.

2.7 | Texting

Clinicians often use text messaging to send urgent patient care messages. Unfortunately, standard mobile networks are not sufficiently secure to protect patient confidentiality. As a result, many EHRs have created secure HIPAA-compliant text messaging, which has improved the reliability and efficiency of communication in the health care setting while protecting PHI. There are also independent HIPAA-compliant products and apps. One study identified barriers to the use of such apps, including lack of familiarity; a perception of the apps as unnecessary, burdensome, or intrusive; battery drainage; and low trust.[20] Another study identified the following opportunities for consideration: replacing pagers, ensuring archiving of text messages, requiring staff to use their own hospital-supplied device, and investing in robust Wi-Fi architecture.[21] Yet another study in 2017 confirmed that 20% of hospitals were providing staff with smartphones rather than pagers.[22] Finally, a recent study identified the risks and benefits of implementing a secure chat communication system instead of pagers in a group of 21 hospitalists. The benefits were ease of access, ability to send pictures, and ability to have a record of the conversation. The risks were implementation challenges, high volume of texts, and lack of shared understanding about appropriate texting.[23] One of the authors found the secure chat to be an effective and HIPAA-secure manner of initiating admission to the hospitalist service from the ED. In summary, while non-secure text messaging may be inappropriate for communicating about patients, secure text messaging may improve the coordination and efficiency of care. Many health systems also use secure portals to enable physician–patient communication rather than direct messaging or texting via personal devices.

2.8 | Electronic health records

The Health Information Technology for Economic and Clinical Health Act, part of the American Recovery and Reinvestment Act of 2009 required health care facilities to adopt an EHR. Hospitals were required to achieve "meaningful use" of the EHR by 2015. Today, virtually all US hospitals employ this technology.

Congress enacted a second statute with significant implications for EHRs, the 21st Century Cures Act, in 2016.[24] One provision of this statute, implemented in 2022, mandates that patients and their surrogate decision makers have free and immediate access to their EHRs, including clinical notes.[25] Both patients and clinicians report several benefits of open access to notes, including better understanding of their care and improved communication.[26,27] Clinicians, patients, and information technology professionals have also identified concerns about open and immediate access to EHR information, including inappropriate parental access to confidential medical information about their adolescent children and documentation of suspected of child abuse and neglect and domestic violence.[28,29]

Health care systems have developed and implemented a number of safeguards to address these concerns, including the following.

2.8.1 | Authentication and use of passwords

Password security is essential for maintaining confidentiality. Best practices for creating passwords exist and frequent password changes

are no longer considered ideal. Most important and obvious is that passwords should never be shared with anyone else. Multi-factor identification is useful in some environments but impractical for those who interact with the EMR frequently, such as EPs.

2.8.2 | Break-the-glass

Break-the-glass is a function that is triggered in the EHR when trying to enter a chart that is restricted for any of a variety of reasons (e.g., because the patient is a celebrity, VIP, or employee). What pops up may contain a warning and the question, "Are sure you want to enter this record?" Entry requires a second login. Entries are audited and reviewed. Improper entries may be punished by loss of employment, civil claims, and penalties under HIPAA.

2.8.3 | Mental health and substance use disorder notes

Mental health, psychotherapy, and substance use disorder (SUD) notes carry specific federal protections. These are sometimes protected via break-the-glass mechanisms or segregated so they can only be viewed by approved users. This can sometimes prevent ED providers from accessing useful information. Prescription drug monitoring programs, also password protected, can be used as an alternative for those with suspected SUD.

2.8.4 | Automatic log-outs and privacy screens

EHR systems are typically set to log out automatically after a short period of time so that another person cannot use the EHR under the first user's login. Another safeguard is the use of privacy screens that make the oblique viewing of screens difficult. While these safeguards may be viewed as a nuisance by some, they are necessary to ensure the confidentiality of the EHR.

2.8.5 | Patient access to EHRs

As noted above, the 21st Century Cures Act requires health care providers to provide open access to EHRs to patients. Providers, however, also have a responsibility to prevent harm to patients and to protect confidential patient information from disclosure to anyone who has no right to that information. The Act also, therefore, authorizes the Department of Health and Human Services (HHS) to identify activities that do not constitute information blocking. On behalf of HHS, the Office of the National Coordinator for Health Information Technology has defined eight exceptions to the rule prohibiting information blocking.[30] Included among those are a Preventing Harm Exception (limiting EHR access to protect patients and others from unreasonable risk of harm) and a Privacy Exception (restricting EHR access to protect patients' rights to confidentiality). To protect the confidentiality of adolescents' PHI, for example, one commentary reports implementation of a strategy to block parental access to their adolescents' EHRs. This strategy included review of the e-mail addresses linked to the patient portals for adolescents, efforts to link portal access to adolescent's e-mails, and restriction or deactivation of portal access to e-mail addresses linked to the adolescents' parents.[31]

2.9 | Confidentiality in the ED waiting room and hallways

Crowding in the ED has been and remains a significant obstacle to protecting patient confidentiality. Staff frequently must evaluate patients in the waiting room and other non-treatment areas such as hallways. Studies show that inadvertent disclosure of PHI in waiting rooms is frequent. Due to the close quarters and fast pace of the ED, confidentiality is often more difficult to protect than in other environments, such as a physician's office. Curtained areas and treatment cubicles offer some degree of privacy, but studies show that people still overhear a significant amount of confidential information. Under optimal conditions patients are seen in a closed room, but in times of increased demand and limited ED treatment space, there is often no private place to assess and treat patients. Strategies for protecting confidentiality when assessment and treatment patients in non-standard areas is unavoidable include reserved areas for private conversation, use of temporary barriers or dividers, and speaking in low volume when discussing sensitive information. Further studies are needed to determine how best to provide care for patients in waiting room and hallway environments while also respecting their rights to physical and informational privacy.[7,31–34]

2.10 | The duty to protect patients from others: Visitors, recording, and law enforcement

In most medical environments, the only people in the room with a patient are those who the patient agrees to have in the room. If there is an interruption or an inappropriate person enters the room, the interview, examination, or treatment can be paused. In the ED, the situation is often very different. In many circumstances, it is difficult to assure that no one can hear a conversation with a patient, even when the ED is not crowded. Aural and visual exposure of patients means that information about them is potentially available to anyone who is nearby. For this reason, access to the ED should have reasonable limits. Several circumstances raise particular concerns.

The first concern involves visitors. Many patients arrive in the ED with friends or family, or, or are joined by them soon after arrival. These visitors' presence may be welcome to the patient, but we cannot assume this. ED patients are vulnerable and may need to discuss information that they do not want visitors to know. At a minimum, EPs should ask whether patients are comfortable with visitors staying for the interview or exam. Staff should permit visitors to remain only if the patient allows it. If a visitor is asked to step out during an interview,

staff should make sure that they do not simply step behind a curtain or leave a room, but rather move out of hearing range of all discussions between patients and ED staff.

A second group that can breach patient confidentiality by their presence is law enforcement. Although police need a warrant to obtain evidence from a place where a person has an expectation of privacy, the ED is not such a place. Courts have sometimes ruled that the ED is a public place, a "continuation" of the street.[35] Nevertheless, police cannot obtain and review medical records in the ED without a warrant. Police may, however, use whatever observations they make about a patient's appearance, actions, possessions, or statements, and a judge will determine whether such evidence is admissible in court. It is possible that a stray comment or an overheard conversation could lead to a patient's arrest and conviction. This problem can be mitigated by policies that regulate police access to the ED. The problem of police overhearing something the patient expects to be kept confidential is more likely to arise when the patient is already in police custody in the ED. As with visitors, however, there is no need for the police to overhear a physician's interview with a patient who is in custody. Police can be asked to move far enough away so that the person in custody can speak quietly to the physician without being overheard.

A final group of people from whom patients should be protected are strangers. Although complete privacy is ideal, it is often impossible to interview patients out of hearing range of anyone else. The ubiquity of cell phones and the popularity of posting content from one's life online means that a patient may become part of another person's post, perhaps in an unflattering way. While this can happen in other environments as well, few of those are places where the subject is as vulnerable as in the ED. To protect the confidentiality of patients, hospitals should adopt rules against all unapproved photography and filming in the ED, with staff empowered to enforce those rules.

3 | CONCLUSION

This article reviews perennial and novel challenges to protecting patient confidentiality in EDs, including the use of social media, electronic communication and record-keeping, open ED layouts with close proximity of patients (and visitors) to one another, and chronic crowding. These circumstances pose ongoing, significant risks of breach of confidentiality to ED patients and professionals. The article proposes a variety of strategies to prevent violation of confidentiality in the ED.

REFERENCES

1. Reich WT, ed. Oath of Hippocrates. . *Encyclopedia of Bioethics*. Macmillan; 1995:2632.
2. American College of Emergency Physicians. Principles of ethics for emergency physicians. *Code of Ethics for Emergency Physicians*. Accessed December 20, 2022. https://www.acep.org/patient-care/policy-statements/code-of-ethics-for-emergency-physicians/
3. Moskop JC, Marco CA, Larkin GL, Geiderman JM, Derse AR. From hippocrates to HIPAA: privacy and confidentiality in emergency medicine—Part I: conceptual moral, and legal foundations. *Ann Emerg Med*. 2005;45:53-59.
4. Moskop JC, Marco CA, Larkin GL, Geiderman JM, Derse AR. From hippocrates to HIPAA: privacy and confidentiality in emergency medicine—Part II: challenges in the emergency department. *Ann Emerg Med*. 2005;45:60-67.
5. Olsen JC, Sabin BR. Emergency department patient perceptions of privacy and confidentiality. *J Emerg Med*. 2003;25(3):329-333. doi:10.1016/s0736-4679(03)00216-6
6. Lin YK, Lin CJ. Factors predicting patients' perception of privacy and satisfaction for emergency care. *Emerg Med J*. 2011;28(7):604-608. doi:10.1136/emj.2010.093807
7. Geiderman JM, Moskop JC, Derse AR. Privacy and confidentiality in emergency medicine: obligations and challenges. *Emerg Med Clin North Am*. 2006;24(3):633-656. doi:10.1016/j.emc.2006.05.005
8. Allen AL. Privacy in health care. In: Reich WT, ed. *Encyclopedia of Bioethics*. Macmillan; 1995:2064-2073.
9. Toader E, Damir D. Medical responsibility as moral and ethical foundation for the professional conduit. *Procedia—Social Behav Sci*. 2014;149:955-961. doi:10.1016/j.sbspro.2014.08.314
10. Blightman K, Griffiths SE, Danbury C. Patient confidentiality: when can a breach be justified? *Continuing Educ Anaesthesia Crit Care Pain*. 2014;14(2):52-56. doi:10.1093/bjaceaccp/mkt032
11. US Department of Health and Human Services. Summary of the HIPAA privacy rule. Accessed December 22, 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
12. Legal foundations Schleiter KE. When patient-physician confidentiality conflicts with the law. *Virtual Mentor*. 2009;11(2):146-148. doi:10.1001/virtualmentor.2009.11.2.hlaw1-0902
13. Lois A. Weithorn; When does a minor's legal competence to make health care decisions matter? *Pediatrics*. 2020;146(1):S25-S32. doi:10.1542/peds.2020-0818G
14. American College of Emergency Physicians. Violence in the emergency department. Accessed February 14, 2023. https://www.acep.org/administration/violence-in-the-emergency-department-resources-for-a-safer-workplace/
15. Marco CA, Schears RM, Geiderman JM, Derse AR, Moskop JC. Disruptive behavior among emergency department patients. *Am J Emerg Med*. 2022;59:176-177. doi:10.1016/j.ajem.2022.04.034
16. Ben-Assuli O. Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. *Health Policy*. 2015;119(3):287-297. doi:10.1016/j.healthpol.2014.11.014
17. Gostin LO, Halabi SF, Wilson K. Health data and privacy in the digital era. *JAMA*. 2018;320(3):233-234. doi:10.1001/jama.2018.8374
18. Gai N, So D, Siddiqui A, Steinberg BE. Dissemination of anesthesia information during the coronavirus disease 2019 pandemic through Twitter: an infodemiology study. *Anesth Analg*. 2021;133(2):515-525. doi:10.1213/ANE.0000000000005602
19. Liu HY, Beresin EV, Chisolm MS. Social media skills for professional development in psychiatry and medicine. *Psychiatr Clin North Am*. 2019;42(3):483-492. doi:10.1016/j.psc.2019.05.004
20. Byrd TF, Speigel PS, Cameron KA, et al. Barriers to adoption of a secure text messaging system: a qualitative study of practicing clinicians. *J Gen Intern Med*. 2023;38:1224-1231. doi:10.1007/s11606-022-07912-8
21. Liu X, Sutton PR, McKenna R, et al. Evaluation of secure messaging applications for a health care system: a case study. *Appl Clin Inform*. 2019;10(1):140-150. doi:10.1055/s-0039-1678607
22. O'Leary KJ, Liebovitz DM, Wu RC, et al. Hospital-based clinicians' use of technology for patient care-related communication: a national survey. *J Hosp Med*. 2017;12(7):530-535. doi:10.12788/jhm.2767
23. Lee JL, Kara A, Huffman M, et al. Qualitative analysis of team communication with a clinical texting system at a midwestern academic hospital. *Appl Clin Inform*. 2022;13(2):391-397. doi:10.1055/s-0042-1744389
24. 21st Century Cures Act, H.R. 34, 114th Cong. (2015).

25. Everson J, Healy D, Patel V. Experiences with information blocking in the United States: a national survey of hospitals. *J Am Med Inform Assoc*. 2023;30:1150-1157.
26. Wasseem N, Kircher S, Feliciano JL. Information blocking and oncology: implications of the 21st Century Cures Act and open notes. *JAMA Oncol*. 2021;7:1609-1610.
27. Leonard SM, Zackula R, Wilcher J. Attitudes and experiences of clinicians after mandated implementation of open notes by the 21st century Cures Act. *J Med Intern Res*. 2023;25:e42021.
28. You JG, Potter JE, Mishuris RG. Electronic health record adolescent confidentiality in a safety net setting. *Appl Clin Inform*. 2023;14:878-882.
29. Sinha S, Bedgood M Puttagunta R, Kataria A, et al. Variation in pediatric and adolescent electronic health data sharing practices under the 21st century Cures Act. *J Am Med Inform Assoc*. 2023;30:2021-2027.
30. HealthIT.gov. Office of the National Coordinator for Health Information Technology. Information blocking exceptions. HealthIT.gov/CuresRule
31. SoRelle Ruth MPH. Maintaining patient privacy: a tough task in the ED. *Emergency Med News*. 2003;25(3):40-41.
32. Innes K, Jackson D, Plummer V, Elliott D. Care of patients in emergency department waiting rooms—an integrative review. *J Adv Nurs*. 2015;71(12):2702-2714. doi:10.1111/jan.12719
33. Blank FS, Santoro J, Maynard AM, Provost D, Keyes M. Improving patient safety in the ED waiting room. *J Emerg Nurs*. 2007;33(4):331-335. doi:10.1016/j.jen.2006.10.016
34. Knowles J. The importance of clinician-patient confidentiality in the emergency department. *Clin Advisor*. 17:385-396. doi: 10.1016/S0733-8627(05)70066-3
35. Song JS. Policing the emergency room. *Harv Law Rev*. 2021;134:2646-2720.

How to cite this article: Brenner JM, Delpier MY, Simon JR, Geiderman JM, Marco CA, Moskop JC. Privacy and confidentiality of emergency department patient information: Contemporary considerations and challenges. *JACEP Open*. 2024;5:e13130. https://doi.org/10.1002/emp2.13130