International Journal of Paramedicine

Published by the National EMS Management Association (USA)

CASE REPORTS

PRIVATE HEALTH INFORMATION LEGAL PROTECTIONS IN EMERGENCY MEDICAL SERVICES: A NEW JERSEY CASE STUDY THAT INFORMS UNITED STATES' PROTECTIONS

Ryan S. Houser, MHA, MPH, MS, EMPS, NREMT[1*]

**Corresponding Author:* ryan.houser@rutgers.edu

Author Affiliations: 1. Rutgers Law School - Newark Campus, Newark, NJ, USA

Recommended Citation: Houser, R. A Survey of Private Health Information Legal Protections in Emergency Medical Services: A New Jersey Case Study that Informs United States' Protections. *International Journal of Paramedicine*, (Pre-Issue Version; 2022, November 17). Retrieved from https://internationaljournalofparamedicine.com/index.php/ijop/article/view/2330

Keywords: EMS; policy; public health; legal protection; personal information

Received: February 10, 2022
Revised: September 2, 2022
Accepted: September 10, 2022
Pre-Issue Release: November 17, 2022
Publication: TBD

Copyright ©: 2022 by the National EMS Management Association

Funding Support: There is no funding to report.

Competing Interests: The author certifies they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

Acknowledgement: Ryan Houser is a CLiME Research Fellow focusing on health disparities. Ryan was previously a dual-fellow at Georgetown University within the Center for Global Health Science and Security and O'Neill Institute For National And Global Health Law – Georgetown University Law Center.

Pre-Issue Galley

ABSTRACT

Recent communications between counsel for an Emergency Medical Service (EMS) provider in New Jersey and the state Department of Health (DOH), Office of Emergency Medical Services (OEMS), claimed that the DOH was providing illicit access to private health information (PHI) based within the providers electronic patient care report (ePCR). While the response from the DOH indicated that the information sharing was completed in accordance with all state and federal laws, the concerns raised by the law firm are not novel. EMS systems are often trusted by their patients to protect their PHI obtained as a necessity during their lifesaving operations. The collection and use of data from EMS systems nationwide are crucial to improving operations, provider safety, and patient care; however, there is a competing interest in protecting patients' privacy and respecting their Constitutionally protected rights. There are important legal and policy perspectives that should guide the prospect of personally identifiable EMS data sharing with law enforcement. With 64% of state health departments considering themselves hybrid entities, the concerns within New Jersey are likely shared throughout the United States. There are mechanisms that must remain in place to protect the rights and privacy of patients who need to trust these protections to engage with the system while also ensuring that the minimum necessary information to support the legitimate police powers of the state to protect health and safety is maintained.

INTRODUCTION

In November of 2021, a New Jersey Emergency Medical Service (EMS) law firm sent correspondence to the state's Office of EMS (OEMS) claiming that OEMS provided administrator access to the state's Emergency Medical Record (EMR) system, ImageTrend, to the New Jersey State Police, Fatality Analysis Report System personnel, potentially in violation of numerous laws. While the response correspondence (1) from the Department of Health indicated that the information sharing was completed in accordance with all state and federal laws, the concerns raised by the law firm are not novel. The same concerns about privacy and information sharing

with law enforcement were raised when efforts were introduced to increase inter-agency data sharing as the nation responded to the opioid epidemic. The collection and use of data from EMS systems nationwide are crucial to improving operations, provider safety, and patient care. There are important legal and policy perspectives that should guide the prospect of personally identifiable EMS data sharing with law enforcement. This paper will review the New Jersey incident, applicable protections within the state, and the similarities between other entities throughout the United States that could yield similar concerns.

NEW JERSEY'S HISTORY

In 2014, the state police's Drug Monitoring Initiative partnered with the state to combine data resources to combat the opioid epidemic in the state. The state's Attorney General's Office and the Department of Health Data Privacy Officer created a Data Use Agreement which allowed for the bi-directional data sharing of law enforcement and EMS data through the Department of Health (NJDOH) and the Department of Law and Public Safety (NJDLPS).(2) The data use agreement outlines the specific data that can be shared to respect patient privacy and ensure only the minimum data needed to accomplish the public health efforts is obtained.(3)

In January of 2018, to ensure better collection of public health data, New Jersey enacted an EMS Data Law(4) which mandates that all EMS agencies in the state, whether volunteer or licensed by OEMS, submit electronic patient care reports (ePCR) to the DOH in a format that is compliant with the National Emergency Medical Services Information System (NEMSIS). This service increases the amount of data and information available to the state for important public health measures and tracking, which also increases the vulnerabilities to widespread detrimental impacts from a breach or authorized access.

LEGAL PERSPECTIVES

To protect the rights of individuals contacting the health system, certain laws have been established to protect the right to privacy of patients. These laws and statutes at the federal or state level are meant to provide a framework from which information sharing is permissible to support legitimate government interests while narrowly tailoring the sharing to ensure that privacy safeguards remain in place. This section will scope the various applicable federal and state standards that protect PHI and privacy, which would be implicated in personally identifiable EMS data sharing with law enforcement.

Health Insurance Portability and Accountability Act

As the world moved to more electronic-based information systems, the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") established, for the first time, a national set of standards for protecting certain health information. The standards defined the use and disclosure of an individual's health information or protected health information (PHI). Covered entities or organizations subject to the

Privacy Rule, including health care providers, regardless of size, who electronically transmit health information in connection with certain transactions,(5) were bound by these standards to ensure that through the risk of civil money penalties, PHI was properly protected while permitting the necessary flow of health information that supports the promotion of high-quality healthcare and protects the health and well-being of the general public. The goal of the Privacy Rule was to create a balance that permits the crucial uses of information while protecting the privacy of those in need of medical care and healing.

Permitted uses and disclosure of information without the authorization and permission of the individual include public health activities. Under the HIPAA Privacy Rule, HIPAA-covered entities, such as EMS providers, may disclose information to a public health authority such as a Department of Health. HIPAA allows these public health authorities to share information with other government agencies, which may include law enforcement entities that are collaborating with the public health authority for various public health purposes such as combating the opioid epidemic or any other purpose of preventing or controlling disease, injury, or disability.(6) The sharing of this PHI can be disclosed without authorization to the public health authorities authorized to receive this information.(7) Additional programs are included in the Fatality Analysis Reporting System (FARS), funded by the National Highway Traffic Safety Administration (NHTSA). Under FARS, EMS data repositories may be searched for federal reporting data. NHTSA can obtain individually identifiable information concerning the victims of motor vehicle crashes, which may be maintained in a state's EMS data repository, according to the Federal Office of Civil Rights. The Department of Health is a hybrid entity under HIPAA as defined by 45 CFR § 164.103. Meaning, the department is a single legal entity performing covered and non-covered functions. The public health branch of the Department of Health in New Jersey is not a HIPAA-covered portion of the Department of Health in which OEMS is housed.(1) A hybrid entity is permitted to designate its healthcare components as covered by HIPAA and its other non-health components as non-covered, which may include the state's EMS authority.

PHI can be shared where required by law.(8) Most states require their EMS to provide patient data to their OEMS; the provision of this data would be considered required by law. Additionally, OEMS will fall under the HIPAA permittance of EMS providers to disclose PHI to a health oversight agency for oversight activities authorized by law.(9) Under HIPAA's Privacy Rule, two de-identification methods can be used to ensure information shared cannot identify, or if there is no reasonable basis in which a covered entity can believe the shared information can identify an individual. HIPAA permits covered entities to use these standards to determine that information is not PHI. Under § 164.514(b)(1), expert determination, entities apply statistical or scientific principles when de-identifying information. A person with the knowledge of the generally applicable principles would "determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information."(10) This leads to a very small risk that the anticipated receiving entity could identify an individual. Under the Safe Harbor method, removing 18 types of identifiers leads to no actual knowledge that residual information can identify an individual.(11)

Amendment IV

Under the 4th amendment, the Constitution provides the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."(12) Under recent court decisions, the Supreme Court has held that the 4th amendment protects people from warrantless searches of historical cell-site location due to an individual's reasonable expectation of privacy despite information being in the possession of a third party. See *Carpenter v. United States*.(13) The similar arguments made in this case provide additional protections for the future searches of health information in private databases such as PHI within and ePCR created by an EMS entity. Law enforcement being granted full, unwarranted access to PHI within an ePCR platform could amount to a violation of amendment IV in the absence of permissions based on the various legally acceptable access that have been discussed.

Amendment X

Due to the federalist structure of the United States Constitution under the 10th Amendment, "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."(14) Under this amendment, the states have been recognized to have police powers, which provide them the authority to make laws for public safety and health. The exercises of police power must remain within the induvial rights guaranteed by the Constitution. The constitution does not provide an expressed right to privacy; however, various court decisions have interfered the broadly interpreted liberty guaranteed by the 14th amendment(15) to guarantee a fairly broad right of privacy that has come to encompass decisions about child rearing, procreation, marriage, and termination of medical treatment. Additionally, other amendments have included certain aspects of privacy such as the privacy of beliefs,(16) privacy against the quartering of soldiers,(17) privacy against unreasonable searches and seizures,(18) privilege against self-incrimination, providing protections for personal information,(19) and an enumeration of certain rights in the Bill of Rights which "shall not be construed to deny or disparage other rights retained by the people."(20) Outside of any infringements of these rights, the government has general deference to create laws to promote general health and safety. Even within these protections, the government can promote police powers, however, with a heightened level of scrutiny applied to ensure that the actions achieve a compelling government interest through narrowly tailored means to that interest and be the least restrictive means available. There is a general protection of privacy which inspires the other protections provided in this section, but the states do have a legitimate interest under their police powers to make and enforce all laws necessary to preserve public health, safety, and general welfare, which may include the collection of aggregated data which informs public health interventions even if this includes a collaboration with a law enforcement entity.

Federal Computer Fraud and Abuse Act

The CFAA was enacted to prohibit intentionally accessing a computer without authorization or in excess of authorization. This law provides that either fines or imprisonment

are possible under violations of the act in which an actor intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains protected information.(21) Any improper access to EMRs would constitute a violation of the CFAA in addition to the other laws discussed in this section.

Title XIX of the Social Security Act

This federal law established the regulations for the Medicaid program. The law includes provisions that govern the acquisition, use, and disclosure of Medicaid enrollees' PHI.(22) EMS entities frequently assist patients with Medicaid and thus collect their PHI, which would be protected under Title XIX.

State Law

New Jersey State Constitution: Under Article 1 § 7 of the state constitution, similar to the protections in Amendment IV of the United States' Constitution, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."(23)

N.J.S.A. 56:8-164(a): This statute provides descriptions of prohibited actions relative to the display of social security numbers.(24) This statute prohibits a public entity from intentionally communicating a person's social security number. ePCRs frequently contain patient social security numbers as a means of identification.

N.J.S.A. 56:8-163(a): This statute requires similar public entities that compile or maintain electronic records that include personal information such as PHI to disclose any breach in the data or access by an unauthorized person.(25)

N.J.S.A. 2A:38(A)-3(c): Under this statute, anyone who is damaged as a result of the "purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network" "may sue the actor therefor in the Superior Court and may recover compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation."(26)

Data Use Agreement: Under the authority of N.J.S.A. 262H-1 the Department of Health can enter a DUA, which allows the DOH to collect patient data necessary to carry out the work of the DOH.(27) The DOH can collaborate with other state agencies on issues within the state that affect public health.(28) The state of New Jersey also has statutes that require EMS providers to report certain information to the DOH.(29,30) This information is meant to assist the DOH in recording and tracking data concerning the types of medical emergencies for which EMS is requested, response times of EMS entities, patterns in timing and location of the requests for EMS aid, the nature of services provided, and patterns in dispatch and response activities.

Case Law: The state of New Jersey has recognized a private right of action for the invasion of privacy, within HIPAA standards, due to the disclosure of medical records to an unauthorized third party. See Smith v. Datla, 451 N.J. Super. 82 (App. Div. 2017)(32).

This case found that "physicians were under a common law duty to maintain the confidentiality of patient records and information" and that liability could ensue from any breach.(32) Additionally, in State v. Donis, 157 N.J. 44 (1998), the courts maintained the need to protect privacy and prevent unreasonable searches and seizures.(33)

Other States: Many state EMS authorities are likely not covered under HIPAA(34) as they may not be a "covered entity."(35) Merely receiving PHI does not automatically turn an organization into a covered entity which could result in a gap of protections for health information.(34) Nearly all ambulance services within the United States are covered entities under HIPAA since they provide health care services in a direct treatment capacity and are engaged in HIPAA-standard electronic transactions where they bill insurers for services provided. This ensures that any information provided to EMS providers is protected. However, these EMS entities share information with EMS Authorities for trend tracking and public health needs, but the sharing of this information opens a gap in protection as EMS authorities do not "provide health care or function as a health plan or health care clearinghouse and are therefore not covered entities under HIPAA."(34) Even if there are states themselves that are covered entities, components of the state that do not function in any healthcare provider, plan, or clearing house role, can avoid HIPAA coverage if the state is a hybrid entity. Similar to New Jersey, the Texas Department of State Health Services designated itself a HIPAA hybrid entity.(36) The Texas DSHS indicated they have been "very careful to designate its covered and non-covered functions under HIPAA to ensure that its public health, regulatory and health oversight functions are not affected."(36) However, the voluntary compliance yields a potential avenue for misuse of data in the case of a bad actor. Research has found that thirty-two states (64%) classify themselves as hybrid entities, with 14 considering themselves covered (28%) and four (8%) saying they were neither covered nor hybrid.(37)

Policy Perspectives

There is a great need for trust to be instilled in the public safety system. Any actions that could harm patients by releasing information to unauthorized persons, especially law enforcement, could erode trust and discourage healthcare access. Any undocumented migrants or patients with criminal records may be discouraged from contacting EMS if they know their information may be obtained by law enforcement entities. This places patients needing medical care in a position from which they may have to balance their health against other competing interests, creating a potential for a novel public health crisis for populations already at risk and discriminated against. EMS entities have a stated mission of treating all patients in need without discrimination based on any status. Using the information obtained during their lifesaving work makes EMS a potential pawn in practice for illicit access to PHI.

Greater inter-agency data sharing, however, is crucial to the awareness of certain public health crises such as the opioid epidemic. The dataset that is shared by NJDOH to NJDLPS is meant to "support situational awareness in order to lessen and prevent the threat to the public of overdoses due to the possible opioid use or abuse, identify those who are being disproportionately affected, as well as to administer emergency care."(1)

The various dashboards and analytics performed by the state of New Jersey with the public health data, partially obtained from EMS ePCRs, helps to create a more comprehensive picture of the impact of the opioid crisis within the state and to better inform strategies to combat the epidemic.

RECOMMENDATIONS

The need to ensure privacy protections of PHI while also allowing appropriate aggregate data is available to fully understand the public health crises that exist is an increasingly difficult and novel challenge as the data becomes more electronic in nature. States must investigate new technical solutions which reduce the degree and risk of data exchanges necessary to make decisions with evidence-based data. Within the necessary legal frameworks associated with data protections and privacy rights of patients, technology can be adapted to ensure that access is tailored narrowly to the request from the state. General research and program evaluations have different data requirements than FARS, with varying levels of identifiable information that is necessary. Maintaining legal confidentiality and privacy requirements can be achieved through operational system frameworks that limit any permissible access.

Engaging the public is also an important part of the public health initiatives of the state. When an informed understanding of the basic privacy safeguards and purposes of the data sharing is provided to the public, including the EMS agencies from which the data is obtained, the public may become advocates for the initiatives rather than skeptical, unengaged participants. This is an important role for EMS providers, who are the main point of contact for patients when they enter the healthcare system. Educating on the purpose of data collection and the protections in place will ensure that EMS providers are trusted while caring for patients. EMS leadership should also remain diligent with their Electronic Health Record platforms to identify potential sources of concern, as was the case in New Jersey. Although, the incident was ultimately deemed to be valid access. As advocates for our patients, advocacy should also include protecting their health information from unwarranted intrusion.

The protection of patient information and requirements for providers also extends beyond HIPAA. On August 25, 2022, a jury in California awarded $31 million to family members of victims of a January 2020 helicopter crash.(38) This award was a result of the improper release of photos of the crash site and victims which were captured by first responders who responded to the scene. This case should serve as a reminder for EMS providers that patient privacy and confidentiality are paramount to the profession, alongside proper care provided and subsequent documentation. The family members of the crash victims brought a claim under emotional distress and invasion of privacy of the surviving family members.(38) The court found that although a majority of the photos were never publicly released, the sharing of photos to a select few who were not on scene and without any reason to view the photos was damage enough. This case should remind providers that they are responsible for all parts of patient privacy and not just HIPAA. Almost all states in the United States have several laws prohibiting invasion of privacy with potential compensatory and punitive damages that providers should be aware of.(38) This case brought about the ""Kobe Bryant Act" which makes it a misde-

meanor crime (punishable by up to a $1,000 fine) for first responders in California to share photos of a deceased person at a crime scene for any purpose other than official law enforcement purposes."(38) This mirrors closely the privacy rights permitted under HIPAA, but also extends non-HIPAA covered entities like general first responders including firefighters and police officers, plugging a gap in protection in relation to police, fire, and EMS "taking, sharing, and disseminating patient information of patients or victims of crimes."(38)

EMS agencies and providers need to be aware of any alleged improper conduct which must be investigated. While taking crime scene photos is permissible for law enforcement and even EMS if for legitimate patient treatment purposes, there are strict rules which govern how the pictures are taken and with whom they may be shared. Any dissemination of sensitive photos with anyone who is not in a "need to know" basis is inappropriate and possibly illegal.(38) Even non-"public" disclosures such as to social media and disclosures to even one person who has no right to see the confidential material is improper. While there is no private right of action under HIPAA, HIPAA regulations that generally favor patient privacy are instilled as the standard of care by which all EMS providers will be judged in a civil suit brought under state laws.(38) The best way for EMS providers to be protected is through policies and training which instill the ideals discussed that are highlighted in the Kobe Bryant case. The case should serve as an important lesson for EMS providers to recognize the complexities of patient privacy and the duties that extend beyond HIPAA.

CONCLUSION

One of the major challenges within the legal field is balancing certain rights against certain legitimate governmental interests. The sharing of PHI has legitimate purposes for the government, which has an interest in understanding the public health crises to mitigate any threats to protect the life and safety of its citizens. However, the practice of sharing PHI can directly implicate certain privacy rights as conferred by the United States Constitution and other state Constitutions or supplemental statutes. There are mechanisms that must remain in place to protect the rights and privacy of patients who need to trust these protections in order to engage with the system while also ensuring that the minimum necessary information to support the legitimate police powers of the state to protect health and safety is maintained.

REFERENCES

1. Clancy, T. (2021). NJDOH Data Sharing Return Correspondence, https://www.nj.gov/health/ems/ems-toolbox/Inquiry Response to Data Sharing.pdf.
2. Seplaki, T. (2018) New Jersey's EMS Response to the Opioid Epidemic. *Journal of Emergency Medical Services*, https://www.jems.com/administration-and-leadership/new-jersey-s-ems-response-to-the-opioid-epidemic/.
3. Data Use Agreement Between NJDOH and NJDLPS. (2019). https://www.state.nj.us/health/ems/documents/ems-toolbox/DLPS%20-%20DOH%20Data%20Use%20Agreement%20(fully%20executed)%20(Nov%202019).pdf?fbclid=IwAR0n-8v5yfDapybE7YePxHwFPQwJPojS0HUUX9sIONgcNOVDukwEAC-l2ajA.

4. N.J.S.A. 26:2K-66
5. 45 C.F.R. §§ 160.102, 160.103; see Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). see 45 C.F.R. Part 162
6. 45 CFR 164.512(b)(1)(i)
7. 45 CFR 164.512
8. 45 CFR §164.512 (a).
9. 45 CFR 164.512(d)
10. 45 CFR §164.514(b)
11. 45 CFR § 164.514(b)(2)
12. U.S. Const. amend. IV
13. 585 U. S. ____ (2018)
14. U.S. Const. amend. X
15. U.S. Const. amend. XIV
16. U.S. Const. amend. I
17. U.S. Const. amend. III
18. U.S. Const. amend. IV
19. U.S. Const. amend. V
20. U.S. Const. amend. IX
21. 18 U.S.C. § 1030(a)(2)
22. 42 U.S.C. §§1396-1396v
23. N.J. Const. art. I, § 7
24. NJ Rev Stat § 56:8-164 (2013)
25. NJ Rev Stat § 56:8-163 (2013)
26. NJ Rev Stat § 2A:38A-3 (2020)
27. N.J. Stat. § 26:2H-1
28. N.J. Stat. § 26:1A-15
29. N.J. Stat. § 26:2K-67
30. N.J. Stat. § 26:2K-68
31. Smith v. Datla, 451 N.J. Super. 82, 164 A.3d 1110 (App. Div. 2017)
32. Lee v. Park, No. 17-1421 (3d Cir. Dec. 20, 2017)
33. State v. Donis, 157 N.J. 44, 723 A.2d 35 (N.J. 1998)
34. PAGE, WOLFBERG & WIRTH LLC. (2021) HIPAA Concerns About Releasing Information for NEMSIS. https://nemsis.org/wp-content/uploads/2021/03/Legal-Opinion-on-Sharing-EMS-Data-NEMSIS_2021-1.pdf
35. 45 CFR § 160.103.
36. Texas Health and Human Services. (2022) Important message about HIPAA to providers and entities that use the Vital Statistics applications from the Department of State Health Services, https://dshs.texas.gov/hipaa/vsmessage.shtm.
37. Association of State and Territorial Health Officials. (2205). HIPAA Privacy Rule Implementation in State Public Health Agencies: Successes, Challenges, and Future Needs, https://biotech.law.lsu.edu/cdc/astho/HIPAA5FINAL.pdf
38. What EMS providers can learn from the Kobe Bryant Crash Photos Jury Verdict. Page Wolfberg & Wirth LLC. (2022, September 8). Retrieved September 9, 2022, from https://www.pwwemslaw.com/news/what-ems-providers-can-learn-kobe-bryant-crash-photos-jury-verdict.