

PAGE, WOLFBERG & WIRTH LLC

ATTORNEYS & CONSULTANTS

PARTNERS

JAMES O. PAGE (1936-2004)
DOUGLAS M. WOLFBERG 1,2
STEPHEN R. WIRTH 1

DANIEL J. PEDERSEN 1
RYAN S. STARK 1

OF COUNSEL

KENNETH E. BRODY 1
G. CHRISTOPHER KELLY 3
CHRISTINA M. MELLOTT 1

5010 EAST TRINDLE ROAD, SUITE 202
MECHANICSBURG, PA 17050

TELEPHONE (717) 691-0100
FACSIMILE (717) 691-1226

WWW.PWWEMSLAW.COM

ASSOCIATES

MATTHEW W. KONYA 1

CONSULTANTS

LISA W. BERNHARD, CPA
STEVEN M. JOHNSON

1 MEMBER, PENNSYLVANIA BAR

2 MEMBER, NEW YORK BAR

3 MEMBER, TENNESSEE BAR

January 22, 2021

University of Utah, School of Medicine
295 Chipeta Way
P.O. Box 581289
Salt Lake City, Utah 84158-1220

Re: HIPAA Concerns About Releasing Information for NEMSIS

The University of Utah School of Medicine (“University”) administers the National Emergency Medical Services Information System (NEMSIS), a nationwide database used for improving emergency medical services (EMS) through the standardization, aggregation, and utilization of EMS data at a local, state, and national level. Some EMS stakeholders have raised concerns under the Health Insurance Portability and Accountability Act (HIPAA)¹ about sharing EMS patient care report data (“EMS data”) with entities involved in facilitating NEMSIS. The University asked Page, Wolfberg, & Wirth (PWW), to address those HIPAA concerns.

Nothing in HIPAA restricts the sharing of the EMS data necessary to populate and administer the NEMSIS database. First, HIPAA permits all EMS agencies to share their EMS data, including protected health information (PHI),² with state EMS authorities, offices, and bureaus (referred to as “State EMS Authorities” or “State EMS Authority”). Second, EMS Authorities who are covered by HIPAA are permitted to share EMS data with Federal agencies and contractors that administer NEMSIS, such as the University. Finally, HIPAA may not even apply to the sharing of EMS data with the University for two reasons. First, many State EMS Authorities are not covered by HIPAA. Second, the limited information being shared to NEMSIS contains only a single identifier – a ZIP Code – and therefore may not constitute PHI under HIPAA.

¹ Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936).

² PHI is defined as any individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity. 45 CFR § 160.103.

Disclaimer

This opinion is limited to issues of federal law, specifically the Health Insurance Portability and Accountability Act (HIPAA).

Analysis of HIPAA Issues

1. HIPAA Permits Release of PHI from Ambulance Services to EMS Authorities

Ambulance services are permitted to share EMS data – including PHI - with EMS Authorities under two HIPAA regulations. First, PHI can be shared “where required by law.”³ Because most states require their ambulance services to provide patient data to their State EMS Authority (or contractor of that Authority), the provision of this data would be considered to be “required by law.” Second, HIPAA permits health care providers to disclose PHI to a “health oversight agency” for oversight activities authorized by law.⁴ A health oversight agency is an agency or authority of a state that is authorized by law to oversee the health care system.⁵ State EMS Authorities are agencies of a state authorized by law to oversee emergency medical services in their states. They are authorized to receive EMS data from ambulance services in their role as health oversight agencies. While there only needs to be one HIPAA regulation that permits a covered entity to make a disclosure of PHI, here there are two regulations – 45 CFR § 164.512(a) & 164.512(d) - that permit EMS agencies to share PHI with their State EMS Authority.

2. Most State EMS Authorities Are Likely Not Covered by HIPAA

Most State EMS Authorities are likely not covered by HIPAA and therefore HIPAA does not apply to their uses and disclosures of EMS data. In order to be covered by HIPAA, an individual or organization must meet the definition of a “covered entity”⁶ under the law. Merely receiving PHI does not automatically turn an organization into a covered entity. That organization must fall under one of the types of specifically defined covered entities in HIPAA.

There are three primary types of covered entities under HIPAA:

1. **Health care providers** who transmit health information in a HIPAA-standard electronic transaction (such as health claims submission to insurance);
2. **Health plans** (i.e., insurers, etc.); and
3. **Health care clearinghouses** (i.e., entities which convert non-standard data into HIPAA-compliant electronic information, and vice versa).⁷

³ 45 CFR §164.512 (a).

⁴ 45 CFR 164.512(d).

⁵ 45 CFR § 160.103.

⁶ 45 CFR § 160.103.

⁷ Id.

Nearly all ambulance services in the United States are “covered entities” under HIPAA because they provide health care services in a direct treatment capacity and they also engage in HIPAA-standard electronic transactions - billing insurers for their services. However, most EMS Authorities do not provide health care or function as a health plan or health care clearing house and are therefore not covered entities under HIPAA.

While a state itself may be a “covered entity” because it has components that function as a health plan, health care provider, or health care clearinghouse, other components that do not function in one of these roles can avoid HIPAA coverage if the state is a “hybrid entity.”⁸ A hybrid entity is a single legal entity that performs both HIPAA covered activities and HIPAA non-covered activities. A hybrid entity designates its health care component(s) as covered by HIPAA and its other non-health components as non-covered. For example, a municipality that provides EMS and bills insurance for those services is a “covered entity” because it is a health care provider that transmits claims (a HIPAA standard transaction). But the municipality may choose to become a hybrid entity and designate its EMS operation as a health care component that is covered by HIPAA, and its street sweepers, parks, and other non-health departments as non-covered components not subject to HIPAA. The same is true for State EMS Authorities that are not health care providers, health plans or health care clearinghouses. A state may designate its EMS Authority as a non-covered health care component.

Under the arrangement between the University and the U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA), Office of Emergency Medical Services, the flow of information goes from EMS agencies to the State EMS Authority to the University, often through a vendor. If the State EMS Authority is not a covered entity, HIPAA does not apply to the disclosure of information, PHI or otherwise, from the EMS Authority to the University. In fact, the Department of Health and Human Services expressly recognized in its commentary to the regulations that HIPAA may not apply to subsequent disclosure of that PHI after a covered entity makes an authorized disclosure.⁹ After an ambulance service properly reports EMS data to its EMS Authority, any concerns under HIPAA about an EMS Authority disclosing the information are rendered moot if the State EMS Authority is not covered by the HIPAA.

3. HIPAA Permits Release of PHI to “Public Health Authorities,” and the University, as a NHTSA Contractor, Qualifies as a “Public Health Authority”

Covered entities are expressly permitted by HIPAA to share PHI with “public health authorities” for certain purposes, including the “conduct of public health surveillance, public health investigations, and public health interventions.” A public health authority is:

⁸ 45 CFR §164.504(c).

⁹ 67 Federal Register 53221 (August 14, 2002).

[A]n agency or authority of the United States, a state, a territory, a political subdivision of a State or territory or Indian tribe, or a person *or entity acting under a grant of authority from or contract* with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.¹⁰

NHTSA is a federal agency with oversight and responsibilities regarding the transportation and safety of all roads and vehicles and the agency is required to gather all information relevant to that function. Moreover, the Federal Department of Health and Human Services Office for Civil Rights (OCR) formally recognized NHTSA as a public health authority under HIPAA in a February 22, 2013 letter from OCR Director Leon Rodriguez. NHTSA is clearly a “public health authority” in that capacity.

NHTSA was mandated to develop the NEMSIS program and NHTSA contracted with the University to accomplish that task. Specifically, the Contract between NHTSA and the University (the NEMSIS “Contractor”) states that the University “shall operate the NEMSIS TAC, the National EMS Database, and all related systems to ensure uninterrupted collection, management and reporting of EMS data received from State EMS Offices while NHTSA transitions various NEMSIS TAC functions and activities to the Federal government.”¹¹ Thus, the University is a contractor of a federal agency (NHTSA) for purpose of administering a nationwide EMS database.

HIPAA deems contractors of government agencies to be “public health authorities” where they are involved in public health activities on behalf of governmental agencies. The University, in its capacity as NEMSIS project administrator, satisfies the definition of “public health authority” under the HIPAA Privacy Rule. Therefore, the University is permitted to directly receive such EMS data under HIPAA. The release of information – including any PHI - to the University for NEMSIS is permitted by HIPAA regardless of whether the EMS Authority is a covered entity or not.

4. The Information Received by the University From State EMS Authorities Are Likely Not “PHI” Under HIPAA

The limited information sought by NHTSA and the University for the NEMSIS program may not even be “PHI” under the definition in HIPAA. In order to be PHI, information must be “individually identifiable health information”. The Privacy Rule states: “Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”¹²

¹⁰ 45 CFR §164.501 (emphasis added).

¹¹ Contract DTNH2215C00030, Section C.3 General Requirements.

¹² 45 CFR §164.514(a).

It is highly unlikely that a ZIP Code - the *only* “identifier” that is released from State EMS Authorities to NEMSIS - would be able to identify an individual. All other identifiers, including name, street and city address, date of birth, etc., are redacted from the EMS data before it is released to NEMSIS. This makes it highly unlikely that the information disclosed to NEMSIS is “individually identifiable health information.” As such, it is highly unlikely a State EMS Authority is providing PHI to NEMSIS. If the information is not considered to be PHI, the information is not subject to HIPAA and any concerns under the law are moot.

5. Even if the EMS Authority is a Covered Entity and the EMS Data are Considered to be PHI, the Data can be “De-identified” and no Longer Subject to HIPAA

Even if the information provided to the University is considered to be PHI with the ZIP code, HIPAA permits covered entities (if the State EMS Authority is considered to be a covered entity) to use either of two “de-identification” standards to determine that information is not PHI.

First, a covered entity (if a state EMS office is considered a covered entity) may determine that health information is not “individually identifiable health information” if a person with knowledge of generally accepted statistical and scientific principles:

Determines 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.¹³

In this context, we believe that any person with knowledge of generally accepted statistical and scientific principles would quite likely conclude that the disclosure of health information with only ZIP Codes would pose a very small risk – if any – that the information would allow the identification of individual patients or the compromise of individual health information.

Alternatively, a covered entity may determine that health information is not individually identifiable health information if certain “identifiers” are removed. This provision of the regulation lists eighteen (18) specific identifiers, including ZIP Code. HIPAA states that the initial three digits of a ZIP Code are not considered identifying information if:

The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people is changed to 000.¹⁴

¹³ 45 CFR §164.514(b).

¹⁴ 45 CFR §164.514 (b)(2)(i)(B)(1) & (2).

This would require the State EMS authority to make this adjustment to the ZIP Code field in the information it provides to NEMSIS.

6. *No Business Associate Agreement or Authorization Necessary*

A “Business Associate Agreement” (“BAA”) is required under HIPAA when a third party performs a service on behalf of a covered entity. Here, the University is not providing a service on behalf of the State EMS Authorities, it is merely collecting information from those Authorities. As a result, no BAA is required between the State EMS Authorities and NEMSIS for the State EMS Authorities to be able to release the information to the University. While the University could choose to enter into BAAs with State EMS Authorities to reassure the states for purposes of HIPAA compliance, it would not be required.

We also note that HIPAA does not require a state EMS Authority to obtain any type of authorization, permission, consent, or waiver from individual ambulance services to permit the State EMS Authority to release information to the University. Authorizations for the use and disclosure of PHI are signed by patients, not covered entities. Further a waiver is not required when the information is expressly allowed to be released in accordance with HIPAA. It is inaccurate to assert that HIPAA requires any express authorization – from anyone – for the submission of this data by a State EMS Authority to NEMSIS.

Conclusion

HIPAA in no way restricts the sharing of the EMS data necessary to administer the NEMSIS database. In fact, HIPAA permits EMS agencies to share their EMS data, including protected health information (PHI), with State EMS authorities, and EMS Authorities (covered or not) are permitted by HIPAA to share EMS data with Federal agencies and contractors that administer NEMSIS, including the University. Moreover, HIPAA may not even apply to some entities and information involved in the NEMSIS chain.

Please feel free to contact us should you require any additional assistance with respect to this matter.

Very truly yours,

Signed

The Attorneys at Page, Wolfberg & Wirth