

PAGE, WOLFBERG & WIRTH LLC

ATTORNEYS & CONSULTANTS

JAMES O. PAGE
1936-2004

DOUGLAS M. WOLFBERG ○ Δ
STEPHEN R. WIRTH ○

CHRISTINA M. MELLOTT ○
DANIEL J. PEDERSEN ○

○ MEMBERS, PENNSYLVANIA BAR
Δ MEMBER, NEW YORK BAR

5010 EAST TRINDLE ROAD, SUITE 202
MECHANICSBURG, PA 17050

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

www.pwwemslaw.com

DOUGLAS M. WOLFBERG
dwolfberg@pwwemslaw.com

June 26, 2007

PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION

VIA ELECTRONIC AND FIRST CLASS MAIL

N. Clay Mann, PhD, MS
Professor, Associate Director for Research
University of Utah School of Medicine
Intermountain Injury Control Research Center
295 Chipeta Way
P.O. Box 581289
Salt Lake City, Utah 84158-1220

Re: Release of Information by State EMS Agencies to NEMSIS Under the Health Insurance Portability and Accountability Act (HIPAA)

Dear Dr. Mann:

On behalf of the National EMS Information System (NEMSIS), we have been asked by the University of Utah (the "University"), which contracts with the National Highway Traffic Safety Administration (NHTSA) to administer NEMSIS, to provide an opinion regarding the release of information for the purpose of creating a national EMS information database. It is our understanding that some state EMS agencies have raised HIPAA concerns about the release of information to NEMSIS, and that this is compromising the ability to assemble the type of database originally envisioned under the NEMSIS project.

We begin with a summary of our conclusions, followed by a more detailed analysis of the basis for our conclusions.

Summary

For reasons described in more detail below, we believe that state EMS agencies may share EMS data and other health information with the University for purposes of the NEMSIS database, without either party violating HIPAA, and without causing the ambulance services, EMS organizations or others from where these data originate to violate HIPAA. In summary, the reasons for this conclusion are: (1) state EMS offices are likely not “covered entities” under HIPAA and therefore are not even bound by the HIPAA regulations; (2) the University, by virtue of being a NHTSA contractor for purposes of administering NEMSIS, is a “public health authority,” to which disclosures of protected health information (PHI) are expressly permitted under HIPAA; and (3) the information being shared quite likely satisfies the standards for “de-identified” health information, and its release would not be regulated by HIPAA in any event.

Background

The University of Utah entered into a “cooperative agreement” with NHTSA for purposes of gathering EMS data. The University of Utah, under the terms of the agreement, is specifically tasked with assisting NHTSA in creating a National EMS Information System (NEMSIS). Such a database is of great importance to better assist the federal government in understanding the EMS system, as well as assess and analyze the types of incidents that require EMS, and to optimize EMS delivery and resources throughout the United States. According to the cooperative agreement, the University of Utah is required to assist in gathering data from state EMS agencies for this purpose.

Analysis

1. HIPAA Applies Only to “Covered Entities,” and Most State EMS Offices Likely are Not Covered by HIPAA

There are two primary regulations under HIPAA that could impact the release of health information in this context – the Privacy Rule and the Security Rule. However, to be subject to these regulations, one must be a “covered entity” – otherwise, these extensive rules are inapplicable. (*45 C.F.R. §160.103.*)

There are three primary types of covered entities – (1) health care providers who transmit health information in a HIPAA-standard electronic transaction; (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). (*45 C.F.R. §160.103.*) Most ambulance services are considered “covered entities” under HIPAA because they provide health care services in a direct treatment capacity *and* because they also engage in HIPAA-standard electronic transactions, most commonly, billing insurers and others for their services.

While a state itself may be a “covered entity,” departments or agencies of the state, such as state EMS agencies, that are not health plans, health care providers or health care clearinghouses can nevertheless avoid coverage under HIPAA as “hybrid entities” (*45 CFR §164.504(c)*). A hybrid entity is a covered entity that also provides “non-covered” functions. For example, a municipality that provides ambulance services might be a “covered entity” regarding its EMS operation, but its street sweepers or parks department employees would not be subject to HIPAA, since the municipality would be a “hybrid entity” under HIPAA. The same would be true for the departments of state government that do not meet the definition of health care provider, health plan or health care clearinghouse.

Under the terms of the arrangement between the University and NHTSA, the flow of information is supposed to go from state EMS agencies to the University. Assuming that both parties in this exchange are non-covered entities, HIPAA is inapplicable, and there are no HIPAA restrictions that prevent non-covered entities from sharing information – even health information - with one another. State EMS agencies are permitted to receive EMS data and health information from individual ambulance services within their jurisdictions. *45 CFR §164.512 (d)*. Under this provision, PHI can be shared “where required by law,” and most states obligate their ambulance services to provide data to their state EMS agency.

In addition, HIPAA expressly permits the sharing of EMS data and other health information for “health oversight activities,” without the authorization of the patient. *45 CFR 164.512(d)*. The state EMS agencies are specifically responsible for general oversight of the EMS system, and are permitted to receive protected health information from individual covered entities. The state EMS agencies (in their role as health oversight agencies), however, are generally not covered entities, and are not restricted under HIPAA in how they may use or disclose PHI obtained from covered entities. In other words, where HIPAA permits the lawful disclosure of PHI from a covered entity to a non-covered entity, it does not regulate the “downstream” re-disclosure or subsequent disclosure of that information by the non-covered entity.

The U.S. Department of Health and Human Services (DHHS), in the preamble to the final HIPAA regulations, expressly recognized that once a disclosure of PHI is made, the Privacy Rule may quite likely not afford any additional protections against re-disclosure. In fact, DHHS specifically stated that “health information may no longer be protected by the Privacy Rule once it is disclosed by the covered entity.” *67 Federal Register 53221 (August 14, 2002)*.

Therefore, state EMS agencies are permitted to use and disclose the EMS data and related health information that they receive from their individual ambulance services and EMS agencies, and that disclosure by the state EMS agency to NEMESIS would not

constitute a violation of HIPAA, either by the state EMS office or the individual EMS agencies.

2. *HIPAA Expressly Permits Release of Information to “Public Health Authorities,” and the University, as a NHTSA Contractor, Qualifies as a “Public Health Authority” for NEMSIS Purposes*

The University is a contractor of a federal agency, specifically NHTSA, for purposes of assembling a nationwide EMS database. As discussed above, only “covered entities” are subject to HIPAA, and covered entities (such as ambulance services) are expressly permitted to share information with “public health authorities,” for certain purposes, including the “conduct of public health surveillance, public health investigations, and public health interventions.” *45 CFR §164.512 (b)*. A national EMS database such as NEMSIS is clearly a public health tool designed for public health surveillance and investigation.

It is important to review the specific HIPAA definition of the term “public health authority,” because the precise wording of the definition is critical to this analysis:

Public health authority is an 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.

45 CFR §164.501 (emphasis added).

NHTSA is a federal agency with oversight and responsibilities regarding the transportation and safety of all roads and vehicles, and is mandated to gather and synthesize all relevant information relevant to that function. NHTSA is clearly a “public health authority” in that capacity. In fact, the “Cooperative Agreement” executed by NHTSA states that NHTSA is required to:

Develop and maintain the Federal Level Database for NEMSIS, including data collection, data storage and data distribution. This would include a web-based reporting mechanism for the EMS community and the general public to obtain descriptive reports on EMS across the nation.

“Cooperative Agreement,” Part IV “Scope of Work,” Section A.5 (Page 4-5).

Further, NHTSA is mandated to develop the NEMSIS program and NHTSA contracted with the University to accomplish that task:

Specifically, the purpose of this Cooperative Agreement is to provide technical assistance and support to state and local Emergency Medical Services and NHTSA's EMS Division and NCSA toward full implementation of NEMSIS, including the National EMS Database.

"Cooperative Agreement," Part II "Purpose," Paragraph 2 (Page 3)

Based upon its role as a "Public Health Authority," NHTSA is expressly permitted, under HIPAA, to receive PHI without patient authorization and without permission of the individual ambulance services from which the data originated. In addition, the HIPAA Privacy Rule expressly considers contractors of government agencies to be considered "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, clearly satisfies the definition of "public health authority" under the HIPAA Privacy Rule. Therefore, the University, as a NHTSA contractor that has been specifically engaged to assist NHTSA in the accumulation and processing of the data outlined in the "Cooperative Agreement" and "Scope of Work," is also permitted to directly receive such information. The release of EMS data and other health information by *any* entity (whether a covered entity or a non-covered entity) to the University for this purpose does not constitute a violation of HIPAA. Therefore, even if a state EMS agency was covered by HIPAA, the release of this EMS data to NEMSIS would be permissible.

- 3. The Data Sought by NEMSIS From State EMS Agencies Are Not "Individually Identifiable," and its Disclosure is Therefore Not Prohibited Under HIPAA, Even if HIPAA Did Apply*

The information sought by the NHTSA and the University for the NEMSIS program is not considered "PHI" under the definition contained within HIPAA. PHI and "individually identifiable health information" are inherently related ("PHI" itself is defined in part as "individually identifiable health information"), so if information is not considered "individually identifiable health information," then it can no longer be considered "PHI." If, in turn, it is no longer PHI, the information is not subject to HIPAA and its release cannot violate the HIPAA regulations. 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.

45 CFR §164.514(a). It is highly unlikely that a zip code alone (the only “identifying” feature that is used in the collection of the EMS data) would be able to “identify an individual.” As a result, the information that would be released by the state EMS agency to NEMSIS likely does not even rise to the level of “individually identifiable health information,” and would therefore not be considered “PHI.”

4. *The Information Sought by NEMSIS could be Classified as “De-identified” and Therefore Not Subject to HIPAA*

In the event that the zip code may be construed to be an “identifier” to the extent that the information remains “individually identifiable health information,” the Privacy Rule still has provisions in place to deal with “de-identification” of PHI. A covered entity (if a state EMS office is even 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

45 CFR §164.514(b). 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 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. *45 CFR §164.514*. This provision of the regulation lists eighteen (18) specific identifiers, including zip code. With respect to zip code, the Privacy Rule indicates 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.

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

Whether or not the requested information is “de-identified” under the definitions as outlined above may depend upon the precise mechanism in place to ensure that appropriate “de-identification” occurred. It is our understanding that the NEMSIS

Technical Assistance Center (TAC) suppresses any table cells with small case counts to even further protect against individual identification.¹

5. *Additional Observations*

Please allow us to comment on some additional HIPAA issues. A “Business Associate Agreement” (“BAA”) is required under HIPAA when a third party performs a service on behalf of a covered entity. The BAA contains safeguards to prevent improper release of information by the third party, except where such a release is permitted under HIPAA. Here, the non-covered entity (the University) would not be considered to be providing a service on behalf of a covered entity, and as a result, no BAA is required between the state EMS offices and NEMSIS for the state EMS agencies to be able to release the necessary information to the University. While NEMSIS could choose to enter into BA agreements with state EMS offices if this would reassure the states for purposes of HIPAA compliance, such a step would not be required.

We also note that HIPAA does not require a state EMS agency to obtain any type of authorization, permission, consent or waiver from individual ambulance services to permit the state EMS agency to release the information to the University. Authorizations for the use and disclosure of PHI are signed by patients, not covered entities, and such a waiver is not required in any event when the information is expressly allowed to be released in accordance with HIPAA. It is, quite simply, inaccurate to assert that HIPAA requires any express authorization – from anyone – for the submission of this data by a state EMS office to NEMSIS. It is counterintuitive to claim that HIPAA precludes the release of information when the information is being released for a purpose that is expressly permitted by HIPAA. To require an authorization or waiver before such a release occurs only further prevents the progress of gathering the information required under the NHTSA contract and the NEMSIS project.

Conclusion

Since the EMS data in question are: 1) being disclosed by state EMS agencies, which are likely not “covered entities” under HIPAA; (2) being released to a “public health authority,” which is expressly permitted under HIPAA; 3) not considered “individually identifiable health information”; and 4) “de-identified” in accordance with HIPAA standards, state EMS agencies are allowed to share EMS data with the University of Utah in conjunction with the NEMSIS program without giving rise to a violation of

¹ It is our understanding that the zip code is one of the 75 required elements in the NEMSIS database. The zip code is also one of the 18 listed “identifiers” in HIPAA, 45 *CFR* §164.514. However, we also recognize that certain “cell size restrictions” are used by NEMSIS to greater limit the possible use of zip code as an identifying feature. As long as this safeguard is consistent with the requirements outlined in the Privacy Rule, it appears as though the zip code would not be considered an identifying feature.

N. Clay Mann, PhD, MS
June 26, 2007
Page 8


HIPAA, either by state EMS agencies, or by the individual agencies that originally generated the data.

Disclaimer

This opinion is limited to issues of federal law, specifically the Health Insurance Portability and Accountability Act (HIPAA). We express no opinion on any state laws that may pertain to this issue.

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

Very truly yours,



Douglas M. Wolfberg