ODMAP and Protected Health Information Under HIPAA: Guidance Document

March 2020

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

ODMAP and Protected Health Information Under HIPAA: Guidance Document

Table of Contents

TOPIC **PAGE**

ODMAP BASICS 3

HIPAA AND THE PRIVACY RULE 5

INTERACTION BETWEEN ODMAP AND THE PRIVACY RULE 10

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

ODMAP BASICS

What is ODMAP?

ODMAP stands for the Overdose Detection Mapping Application Program. The Washington/Baltimore High Intensity Drug Trafficking Areas (W/B HIDTA) developed ODMAP and launched it as a pilot program in January 2017.[1] Participation in ODMAP is available at no cost to federal, state, local and tribal law enforcement, other licensed first responders, criminal justice personnel, emergency rooms and hospital personnel, and other public health entities serving the interests of public safety and public health as part of W/B HIDTA's official mandate.[2] Agencies using ODMAP are termed "participating agencies" because in order to access ODMAP, each agency must enter into a participation agreement with W/B HIDTA agreeing, among other things, to adhere to ODMAP's operating policies and procedures.

What are the Washington/Baltimore High Intensity Trafficking Areas?

The High Intensity Drug Trafficking Areas (HIDTA) program is a federal program administered by the Office of National Drug Control Policy that is designed to provide resources to federal, state, local, and tribal agencies to coordinate activities to address drug trafficking in specific areas of the country. As of January 2020, there are 33 individual HIDTA regions within the United States, Puerto Rico and the Virgin Islands.[3] W/B HIDTA was designated in 1994 and serves Maryland, the District of Columbia, Virginia, and parts of West Virginia.[4]

How does ODMAP work?

ODMAP is a mapping application tied to a database containing overdose incident information. W/B HIDTA provides no cost access to the application to participating agencies. Using a mobile phone or computer interface with the program, users from participating agencies report information about an incident involving an actual or suspected drug overdose. In addition to manual data entry, participating agencies can work with W/B HIDTA to implement an application programming interface (API). An API allows overdose information contained within an already-functioning database to be automatically uploaded to ODMAP.[5] Using an API allows participating agencies to contribute data without adding manual reporting processes to field workers. The data reporting area of ODMAP is called "Level 1."

---

[1] ODMAP Overview, *The History of ODMAP*, available at http://www.odmap.org/ (last accessed February 5, 2020).
[2] Washington/Baltimore High Intensity Drug Trafficking Area Overdose Detection Mapping Application Program, *ODMAP Policies and Procedures* at 2 (revised November 2019), available at http://www.odmap.org/Content/docs/training/general-info/ODMAP-Policies-and-Procedures.pdf (last accessed February 4, 2020).
[3] Office of National Drug Control Policy, *National Drug Control Strategy* at 22 (February 2020), available at https://www.whitehouse.gov/wp-content/uploads/2020/02/2020-NDCS.pdf.
[4] Washington/Baltimore High Intensity Drug Trafficking Area, *About HIDTA*, http://www.hidta.org/about-hidta/ (last accessed February 5, 2020).
[5] ODMAP, *How it Works*, available at http://www.odmap.org/ (last accessed February 5, 2020).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

Information reported to ODMAP is plotted on a national electronic map. The data visualization area of ODMAP is called "Level 2." Only users at participating agencies granted Level 2 access to ODMAP can see the information available on the national electronic map.

What are the purposes of ODMAP?
According to W/B HIDTA, the primary purposes of ODMAP include: (1) to provide near real-time surveillance of known or suspected overdose incidents across the United States and its territories; and (2) to support public safety and public health efforts to collaborate and mobilize immediate responses to overdose incidents.[6]

What overdose information is collected in ODMAP?
For each known or suspected overdose incident, an authorized user must report four pieces of information to the Level 1 area of ODMAP: (1) date and time of the incident; (2) location of the incident or first encounter; (3) whether the overdose was fatal or non-fatal; and (4) whether a first responder administered naloxone to the victim, and if so, how much. Other types of information may be reported in Level 1 by authorized users but is not required. The optional permissible categories of information include age of victim, gender of victim, suspected drug involved, additional drugs involved, if the victim was one of multiple victims, if the victim was taken to the hospital, if the incident involved a motor vehicle, and case number. Location data can be reported to ODMAP using either an incident address or GPS coordinates (latitude and longitude). If an address is entered, it is converted to GPS coordinates prior to data storage in the database.[7]

In the Level 2 area of ODMAP, overdose incidents are plotted as data points on a nationwide electronic map. If a data point is selected by the user, the information associated with the point becomes visible. A Level 2 user can filter data points by many of the categories of reported information.

The information in ODMAP is controlled unclassified information (CUI), which may only be released to authorized personnel. Recipients of this information must have a need and right to know the information in the performance of their criminal justice, public safety, and/or public health functions.[8]

---

[6] *ODMAP Policies and Procedures*, supra note 2, at 1.
[7] *See* Overdose Detection and Mapping Application Program, *Training Manual* at 4 (January 30, 2020), available at http://www.odmap.org/Content/docs/training/general-info/ODMAP-Training-Manual.pdf (last accessed February 3, 2020).
[8] *ODMAP Policies and Procedures*, supra note 2, at 5. CUI is "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified." National Archives, *About Controlled Unclassified Information*, https://www.archives.gov/cui/about (last accessed February 26, 2020).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

Is the overdose incident information reported to ODMAP accessible by the general public?
No. Only authorized users at participating agencies with Level 1 access may report to ODMAP and only users at participating agencies with Level 2 access may view/filter the electronic map.

How many ODMAP users are there?
Between January 2017 and October 2019, approximately 2,600 participating agencies in 48 states reported over 175,000 overdoses or potential overdoses to ODMAP. As of October 2019, W/B HIDTA reports that there are over 16,000 Level 1 users and over 5,000 Level 2 users.[9]

Who are the Level 1 users of ODMAP?
The majority of ODMAP Level 1 users are first responders, such as police, emergency medical services (EMS) providers, and fire department personnel who are often among the first people to arrive at an overdose scene. Level 1 users also include emergency departments and hospitals, although not the research units contained within some hospitals.[10]

Who are the Level 2 users of ODMAP?
Level 2 users are public health and public safety officials and policy analysts ~~granted~~ authorized by both the participating agency and W/B HIDTA.[11]

HIPAA AND THE PRIVACY RULE

What is HIPAA?
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) became law in August 1996.[12] The law contains five titles. Title II of HIPAA ("Preventing health care fraud and abuse; administrative simplification; medical liability reform")—specifically Sections 261 through 264— require the Department of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy, and security of health information. Collectively, these are known as the "Administrative Simplification" provisions.[13]

Pursuant to the Administrative Simplification directive, HHS promulgated five rules via regulation: (1) Privacy Rule; (2) Transactions and Code Sets Rule; (3) Security Rule; (4) Unique Identifiers Rule; and (5) Enforcement Rule.[14] This guidance document relates to the Privacy Rule. For purposes of this document, the term HIPAA means the Act itself along with HHS regulations promulgated thereunder, including the Privacy Rule.

---

[9] ODMAP Overview, supra note 1.
[10] *ODMAP Policies and Procedures*, supra note 2, at 2.
[11] *Ibid.* at 3.
[12] Public Law 104-191
[13] U.S. Department of Health and Human Services, *Summary of the HIPAA Privacy Rule*, at 1-2 (May 2003), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last accessed February 5, 2020)..
[14] Peter F. Edemekon and Micelle J. Haydel, *Health Insurance Portability and Accountability Act (HIPAA)* (June 2019), available at https://www.ncbi.nlm.nih.gov/books/NBK500019/ (last accessed February 5, 2020).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

What is the Privacy Rule?
HHS finalized the Privacy Rule in December 2000 and subsequently modified it in August 2002. The federal regulations constituting the Privacy Rule are located at 45 CFR Part 160 and 45 CFR Part 164, Subparts A and E.[15]

In short, the HIPAA Privacy Rule states that "[a] covered entity or business associate may not use or disclose protected health information [PHI], except as permitted or required by [the Privacy Rule]."[16] According to HHS, the purpose of the Privacy Rule is to protect all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[17]

What is a covered entity and a business associate?
A covered entity is a "health plan," a "health care clearinghouse," or a "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."[18] Each of these terms is defined in the Privacy Rule. A covered entity "may also be a business associate of another covered entity."[19]

A business associate is a person or entity (other than a member of the covered entity's workforce) that performs certain activities for the covered entity that involve the use or disclosure of PHI.[20] The functions covered by business associates include claims processing, accreditation, accounting, actuarial, quality assurance, and legal advice.[21]

Is law enforcement a covered entity under the Privacy Rule?
No.[22] If a law enforcement officer learns PHI about an individual from a family member or a person or evidence on the scene, then HIPAA does not apply, and the law enforcement officer may disclose that information to others (subject to state law).[23] However, if a covered entity discloses such information to a law enforcement officer pursuant to a permitted disclosure under the Privacy Rule, then the law enforcement officer's ability to "re-disclose" may be limited.[24] Nevertheless, even in the second scenario, it is critical to understand that the law enforcement officer is not a covered entity.

---

[15] *Summary of the HIPAA Privacy Rule*, supra note 13, at 2.
[16] 45 CFR § 164.502(a).
[17] *Summary of the HIPAA Privacy Rule*, supra note 13, at 3.
[18] 45 CFR § 160.103.
[19] *Ibid.*
[20] *See* 45 CFR § 160.103.
[21] Council of State Governments Justice Center, *Information Sharing in Criminal Justice – Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, at 17 (2010).
[22] U.S. Department of Health and Human Services, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement*.
[23] *See* Council of State Governments Justice Center, supra note 21, at 5.
[24] *Ibid*.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

What is protected health information?
Other than certain specified exceptions, PHI is "individually identifiable health information . . . that is . . .[t]ransmitted by electronic media; . . . [m]aintained in electronic media; or . . . [t]ransmitted or maintained in any other form or medium."[25]

What is individually identifiable health information?
Individually identifiable health information is a subset of health information, including demographic data, that identifies an individual or for which there is a reasonable basis to believe can be used to identify an individual and relates to: (1) an individual's past, present or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual.[26]

Does the Privacy Rule list the identifiers that make health information personally identifiable?
Yes. There is no provision in the Privacy Rule that affirmatively delineates the identifiers that make health information personally identifiable. However, the Privacy Rule lists 18 identifiers that must be removed in order to turn personally identifiable health information into de-identified health information, so long as the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[27] (The Privacy Rule's restrictions on disclosing PHI do not extend to de-identified health information.)

These 18 identifiers "of the individual or of relatives, employers, or household members of the individual" that must be removed to achieve de-identification are: (1) names; (2) all geographic subdivisions smaller than a state (subject to some exception); (3) all elements of dates (except year); (4) telephone numbers; (5) fax numbers; (6) email addresses; (7) social security numbers; (8) medical record numbers; (9) health plan beneficiary numbers; (10) account numbers; (11) certificate/license numbers; (12) vehicle identifiers and serial numbers, including license plate numbers; (13) device identifiers and serial numbers; (14) URLs; (15) IP address numbers; (16) biometric identifiers; (17) full face photographic images and any comparable images; and (18) any other unique identifying number, characteristic, or code.[28]

What are the permitted uses and disclosures of protected health information?
Covered entities and business associates may use or disclose an individual's PHI without prior authorization in the following six situations: (1) disclosure to the individual who is the subject of the PHI; (2) for treatment, payment, and health care operations; (3) in circumstances where the

[25] 45 CFR § 160.103.
[26] *Summary of the HIPAA Privacy Rule*, supra note 13, at 4; *see also* 45 CFR § 160.103.
[27] 45 CFR § 164.514(b)(2). There is an alternative method to de-identifying PHI—having a person "with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" 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." 45 CFR § 164.512(b)(1).
[28] 45 CFR § 164.514(b)(2)(i)(A)-(R).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

individual is clearly given an opportunity to agree or object; (4) incident to an otherwise permitted use or disclosure as long as the covered entity has adopted reasonable safeguards; (5) for 12 "national priority" public interest and benefit activities specified in the Privacy Rule; and (6) where the PHI is disclosed as part of a "limited data set" (some individual identifiers removed) and the recipient enters into a data use agreement with specific safeguards.[29,30]

What are the 12 "national priority" public interest and benefit activities for which use or disclosure of protected health information without the individual's prior authorization may be acceptable?

The Privacy Rule specifies 12 public interest and benefit activities for which use or disclosure of PHI without prior authorization by the individual may be acceptable. These 12 activities are uses and/or disclosures: (1) "required by law;" (2) "for public health activities;" (3) "about victims of abuse, neglect, or domestic violence;" (4) "for health oversight activities;" (5) "for judicial and administrative proceedings;" (6) "for law enforcement purposes;" (7) "about decedents;" (8) "for cadaveric organ, eye or tissue donation purposes;" (9) "for research purposes;" (10) "to avert a serious threat to health or safety;" (11) "for specialized government functions;" and (12) "for workers compensation."[31]

When using or making a permitted disclosure of PHI without prior authorization, what safeguards must a covered entity take?

In most but not all cases, a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the purpose of the use, disclosure, or request.[32] This is termed the "minimum necessary" requirement. With respect to the 12 "national priority" uses or disclosures made for public interest and benefit activities discussed above, the minimum necessary requirement does not apply to uses or disclosures "required by law;" otherwise it is applicable.[33]

What are the general compliance and enforcement mechanisms for the Privacy Rule?

HIPAA does not provide a private cause of action for individuals to file suit for alleged violations, including the Privacy Rule. As a result, "[w]hile [HIPAA] provides both civil and criminal penalties for improperly handled or disclosed information, the language of the statute specifically limits enforcement action to HHS and individual states' attorneys general."[34]

A person who believes a covered entity or business associate is not complying with HIPAA may file a paper or electronic complaint with HHS. HHS is required to investigate the complaint

[29] There are two situations in which covered entities must disclose PHI. Those instances are outside the scope of this guidance document. 45 C.F.R. § 164.502(a)(2).
[30] *Summary of the HIPAA Privacy Rule*, supra note 13, at 4-9. 45 CFR § 164.502(a)(1) contains the list of the six situations. HHS's *Summary* document paraphrases § 164.502(a)(1), as neither the phrase "national priority" nor disclosures for which an authorization or opportunity to agree or object is not required." 45 CFR § 164.512.
[31] 45 CFR § 164.512(a) though 164.512(l).
[32] *Summary of the HIPAA Privacy Rule*, supra note 13, at 10; 45 CFR § 164.502(b) and § 164.514(d).
[33] 45 CFR § 164.502(b)(2)(v) (referencing 45 CFR § 164.512(a)).
[34] *Lee-Thomas v. LabCorp.*, 316 F.Supp.3d 471, 474 (D.D.C. 2018).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

"when a preliminary review of the facts indicates a possible violation due to willful neglect."[35] HHS is permitted, but not required, to investigate, "any other complaint filed under this section."[36] The HHS Office of Civil Rights is charged with receiving, investigating, and resolving complaints. Violations can result in civil fines, or in cases of egregious conduct, criminal penalties. Monetary penalty amounts have changed over the years and are now adjusted annually for inflation. As of 2019, civil fines can range from $117 to $58,490 per violation, with a maximum penalty of $1.755 million per year for violations of an identical provision.[37]

Does the Privacy Rule preempt state law?

State laws that are contrary to the Privacy Rule are preempted by it, unless a specific exception applies.[38] "Contrary" means that it is impossible for a covered entity or business associate to comply with both the state and federal requirements simultaneously.[39] State law continues to control, however, if it relates to the privacy of individually identifiable health information and is more stringent than the Privacy Rule.[40] Thus, the Privacy Rule provides a "floor" of privacy protection for individuals.

What is 42 CFR Part 2, and is it involved in this ODMAP discussion?

42 CFR Part 2 contains a set of federal regulations that address the confidentiality of patient records concerning alcohol and substance use disorder diagnosis, treatment, or referral for treatment. These regulations apply to all "federally-assisted programs" (as those terms are defined in the regulations) holding themselves out as providing such diagnosis, treatment, or referral to treatment.[41] The information available to Level 2 users of ODMAP does not relate to patient records concerning substance use disorder diagnosis, treatment, or referral to treatment. Accordingly, 42 CFR Part 2 is not implicated in the use of ODMAP as it currently operates.

---

[35] 45 CFR § 160.306(a).
[36] *Ibid.* at § 160.306(c).
[37] Memorandum from Adam Snyder to Carolyn Quattrocki, *Emergency Medical Services Providers' Potential Use of HIDTA Overdose Detection Map; Compliance with HIPAA and the Maryland Confidentiality of Medical Records Act*, at 12 (October 19, 2017) (referencing § 13410(d) of the Health Information Technology for Clinical and Economic Health ("HITECH") Act); *HHS Increases Civil Monetary Penalties for HIPAA Violations in Line with Inflation* (November 11, 2019), available at https://www.hipaajournal.com/hhs-increases-civil-monetary-penalties-for-hipaa-violations-2019-inflation/ (last accessed March 2, 2020).
[38] 45 CFR § 160.203.
[39] 45 CFR § 160.202(a).
[40] 45 CFR § 160.203(b).
[41] Council of State Governments Justice Center, supra note 21, at ix. *See also* 42 CFR § 2.11 (defining the terms "program" and "federally-assisted").

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

INTERACTION BETWEEN ODMAP AND THE PRIVACY RULE

How does ODMAP implicate HIPAA and the Privacy Rule?
Three questions must be addressed in order to determine the implications. First, are any ODMAP Level 1 users covered entities? Second, does any of the information reported by ODMAP Level 1 users, and accessible to ODMAP Level 2 users, constitute PHI? Third, if the answers to the first two questions are both yes, then is the disclosure of PHI by covered entity Level 1 users to Level 2 users allowable under the Privacy Rule, and does the answer depend on the particular Level 2 user using the reported information?

Are any Level 1 users covered entities?
Yes. As noted above,[42] Level 1 users generally are employed (on a paid or volunteer basis) by first responder agencies. The participating agencies using ODMAP vary by locality but include law enforcement, fire department, EMS, poison control, medical examiners, and hospital emergency departments.

Under the Privacy Rule, a covered entity includes a "health care provider." Health care providers include "a provider of services [as defined by Medicare] . . . a provider of medical or health services [as defined by Medicare] . . . and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[43] Several types of ODMAP Level 1 users would appear to fall under this definition of health care provider, specifically EMS providers (with the fire department, rescue squad, or otherwise) and hospital emergency department medical personnel who bill, or are paid, for health care. Accordingly, some Level 1 users are covered entities.

Importantly, however, law enforcement officers are not covered entities.[44] Thus, a law enforcement officer's report in ODMAP Level 1 of information learned first-hand at the scene of an actual or suspected overdose does not implicate the Privacy Rule. It follows then, that the use of that law enforcement officer's reported information by any Level 2 user does not implicate the Privacy Rule. The same analysis would hold true for any other type of Level 1 user that is not a HIPAA covered entity who reports overdose incident information learned first-hand to ODMAP.

Is the overdose incident information reported via ODMAP protected health information?
Taking a conservative approach, yes, although identification of a person would require additional information not available in ODMAP.

Of the 18 identifiers that make health information personally identifiable under the Privacy Rule,[45] the overdose incident information collected via ODMAP involves only one—

[42] Pages 1-2.
[43] 45 CFR § 160.103.
[44] *See* page 6 above.
[45] *See* page 7 above.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

"geographic subdivisions smaller than a state."[46] An actual or suspected overdose appears on the Level 2 map as a colored data point. Each point is placed on the map based upon the GPS coordinates associated with the approximate location reported via Level 1. Level 2 users are limited in how far they can zoom into the map. According to ODMAP, the zoom level does not extend past Zoom Level 1D 15, which is a scale ratio of 1:18,055.[47] This means that when the map is fully zoomed in, each centimeter on the map corresponds to 180.55 meters, or approximately 600 feet. No additional information about the location of the actual or suspected overdose incident is provided to the Level 2 user.

The PHI question here boils down to determining if the approximate location of the event can be used, in combination with date, time, and some investigative effort, to determine the identity of the victim (or limited group of persons that includes the victim) who suffered the actual or suspected overdose. In dense, urban areas, ODMAP's zoom limitation provides a level of de-identification potentially sufficient to reduce substantially the possibility of identification. However, in rural areas, structure and population density often is so low that the mere existence of a data point on a street narrows the list of possible victims to a few homes or less. This would assume that the incident location indicates a direct correlation to the owner or resident at a specific location, which is not always the case. Actual identification, however, would require substantial effort beyond what is available on ODMAP.[48]

What provisions of the Privacy Rule permitting the use or disclosure of PHI by a covered entity are most relevant to ODMAP?

As detailed above, the Privacy Rule specifies 12 public interest and benefit activities for which use or disclosure of PHI by a covered entity without prior authorization by the individual may be acceptable.[49] Four of these 12 are implicated (at least potentially) by ODMAP usage, the provisions related to "required by law,"[50] "public health activities and purposes,"[51] averting "a

[46] 45 CFR § 164.512(b)(2)(i)(B).
[47] Aileen Buckley, ArcGIS blog, Web map zoom levels updated, https://www.esri.com/arcgis-blog/products/product/mapping/web-map-zoom-levels-updated/ (last accessed February 5, 2020).
[48] A hypothetical illustration may be useful. Assume that a law enforcement officer (LEO) goes to the scene of an overdose in a rural area. The LEO will know the identity of the overdose victim, and include the name in a police report, regardless of whether he or she reports information to ODMAP. It follows that some of the LEO's co-workers with authorized access to the police report may also learn the identity. The pertinent question is could an ODMAP Level 2 user who does not have authorized access to the police report learn the identity of the overdose victim simply by looking at ODMAP? The answer is no, since ODMAP does not collect names. Even if the overdose incident happened near a rural road with few residences, the Level 2 user would have to consult another database (such as real estate records or 911 phone-to-address lists) to attempt to identify the victim. In doing all this, the Level 2 user very well might exceed their scope of practice. Moreover, if the overdose incident occurred at that location to a victim in a car or on foot, the victim may have no ties to the location whatsoever.
[49] *See* p. 6-7 above, discussing 45 CFR § 164.512(a) though 164.512(l).
[50] 45 CFR § 164.512(a).
[51] 45 CFR § 164.512(b).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

serious threat to health or safety,"[52] and "law enforcement purposes."[53] Each of these three provisions is discussed in more detail below.

Does reporting overdose incident information via ODMAP fall within the Privacy Rule provision permitting use or disclosure of PHI by covered entities as "required by law"? Yes, to the extent there is a state law in place requiring the use of ODMAP.

Where relevant, this provision applies in straightforward fashion. Under the "required by law" provision, a covered entity may use or disclose PHI "to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law."[54] The term "required by law" means "a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law . . .[and] includes . . . statutes or regulations that require the production of information."[55] This provision does not replace any substantive or procedural requirements applicable in cases where the disclosure required by law also: (1) relates to victims of abuse, neglect, or domestic violence; (2) is for judicial and administrative proceedings; or (3) is for certain law enforcement purposes.[56]

Thus, when a state law directs an individual to report a fairly limited amount of PHI—in the form of a geolocation of a known or suspected overdose—via ODMAP, that falls squarely within this permitted use/disclosure. As of February 2020, a handful of states have such legislation.[57]

Initially, this interpretation might appear to contravene the purpose of the Privacy Rule. It is not, however, and HHS expressly discussed this at some length when it first promulgated the final version of the Privacy Rule. In response to comments HHS received about the proposed "required by law" provision in the Privacy Rule, HHS stated:

> We likewise disagree with the characterization of the proposed provision as inconsistent with or contrary to the preemption standards in the statute or Part 160 of the rule. As described in the NPRM [notice of proposed rulemaking], we intend this provision to preserve access to information considered important enough by state or federal authorities to require its disclosure by law.

[52] 45 CFR § 164.512(j).
[53] 45 CFR § 164.512(f).
[54] 45 CFR § 164.512(a)(1).
[55] 45 CFR § 164.103.
[56] 45 CFR § 164.512(a)(2) (providing that a covered entity must still meet the requirements of § 164.512(c), (d), or (f) for the "required by law" provision to apply).
[57] *See* F.S.A. § 401.253 (Florida) (effective October 1, 2017); 210 ILCS 50/3.233 (Illinois) (effective August 9, 2019); MD Code, Health - General, § 13-3602 (Maryland) (effective July 1, 2018); W. Va. Code, § 16-5T-4 (West Virginia) (effective June 3, 2019). In each case, the enacted legislation requires the report of overdose incident information, including the location of known or suspected overdoses, via ODMAP or a similar database application.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

> The importance of these required uses or disclosures is evidenced by the legislative or other public process necessary for the government to create a legally binding obligation on a covered entity. Furthermore, such required uses and disclosures arise in a myriad of other areas of law, ranging from topics addressing national security (uses and disclosures to obtain security clearances), to public health (reporting of communicable diseases), to law enforcement (disclosures of gunshot wounds). Required uses and disclosures also may address broad national concerns or particular regional or state concerns. It is not possible, or appropriate, for HHS to reassess the legitimacy of or the need for each of these mandates in each of their specialized contexts.[58]

Two additional items are worth noting. First, HHS clearly intends for the statute or regulation at issue to require reporting the PHI and not merely permit reporting it. In cases of permitted disclosure only, the "required by law" provision would not apply.[59] Second, the Legislative Analysis and Public Policy Association (LAPPA), the author of this document, recently developed a statewide Model Overdose Mapping and Response Act[60] under which first responders (law enforcement, fire department, EMS), emergency department personnel, coroners, and medical examiners are required to report overdose incident information to ODMAP.

Does reporting overdose incident information via ODMAP fall within the Privacy Rule provision permitting use or disclosure of PHI by covered entities for "public health activities and purposes"?
Yes, as to many types of Level 2 users.

Under the "public health activities and purposes" provision, a covered entity may use or disclose PHI to "[a] public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability . . . and the conduct of public health surveillance, public health investigations, and public health interventions."[61] Thus, the analysis requires determining: (1) who or what is a "public health authority;" and (2) is the information collected in ODMAP for the purposes of preventing or controlling injury and/or the conduct of public health surveillance.

---

[58] U.S. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, at 82667 (December 28, 2000).
[59] *Ibid.*, at 82667-68 ("In making this judgment, we have distinguished between laws that mandate uses or disclosures and laws that merely permit them. In the former case, jurisdictions have determined that public policy purposes cannot be achieved absent the use of certain protected health information, and we have chosen in general not to disturb their judgments. On the other hand, where jurisdictions have determined that certain protected health information is not necessary to achieve a public policy purpose, and only have permitted its use or disclosure, we do not believe that those judgments reflect an interest in use or disclosure strong enough to override the Congressional goal of protecting privacy rights.")
[60] The Act is available at https://legislativeanalysis.org/model-laws/.
[61] 45 CFR § 164.512(b)(i).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

The primary purposes of ODMAP include: (1) to provide near real-time surveillance of known or suspected overdose incidents across the United States and its territories; and (2) to support public safety and public health efforts to collaborate and mobilize an immediate response to overdose incidents.[62] These purposes clearly fall within item (2) in the paragraph directly above.

As for the first determination, a "public health authority" is defined within HIPAA as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an 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."[63] Written guidance from HHS indicates that an agency's official mandate "does not have to be exclusively or primarily for public health" for it to be considered a public health authority under the privacy rule.[64] So long as the agency "has public health matters as a part of its official mandate, it qualifies as a public health authority."[65]

Many types of Level 2 users fall squarely within this definition of "public health authority," including those with traditional public health roles such as federal, state, and local public health departments and agencies.

Does reporting overdose incident information via ODMAP fall within the Privacy Rule provision permitting use or disclosure of PHI by covered entities "to avert a serious threat to health or safety"?
Yes, as to many types of Level 2 users.

Under the "uses and disclosures to avert a serious threat to health or safety" provision, a covered entity may, "consistent with applicable law and standards of ethical conduct," use or disclose PHI if the covered entity believes in good faith that the use or disclosure "[i]s necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and . . . is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat."[66] Based on HHS commentary, it appears that this provision was drafted to apply to a range of scenarios, from the need to warn a particular person about an imminent threat to the need to deal with a public health emergency.[67]

---

[62] *See* page 4 above.
[63] 45 CFR § 164.501.
[64] U.S. Department of Health and Human Services, HIPPA For Professionals, *FAQ* (created December 12, 2002; last reviewed July 26, 2013), available at https://www.hhs.gov/hipaa/for-professionals/faq/297/does-the-hipaa-public-health-provision-permit-covered-entities-to-disclose-information-to-authorities/index.html (last accessed February 4, 2020).
[65] *Ibid.*
[66] 45 CFR § 164.512(j)(1).
[67] *See Standards for Privacy of Individually Identifiable Health Information, supra* note 58, at 82703 ("We do not believe it would be appropriate to narrow further the scope of permissible disclosures under this section to respond to specifically identified 'imminent threats,' a 'public health emergency,' or a 'national emergency.' We believe it

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

The nationwide public health emergency pertaining to the opioid crisis declared by HHS in October 2017 at the direction of the President, in addition to numerous, similar state-level declarations and task force formations pertaining to opioid and other drug overdoses, underscores how drug overdoses constitute a serious threat to the health and safety of individuals and the general public.[68] The actions taken by local public health and public safety authorities in responding to overdose incidents, based in significant part on information provided to them through ODMAP Level 2, serves to prevent or lessen this threat.

Moreover, one drug overdose might occur in a particular location for several reasons. A series of drug overdoses near a particular location, however, may indicate emerging concerns about drug potency or contamination. Some of the community members most in position to prevent or lessen the threat to a person's or the public's health due to drug potency include law enforcement officers and harm reduction agencies. These are the types of Level 2 users who fall under this exception but might not fall under the public health authority exception discussed above.

Does reporting overdose incident information via ODMAP fall within the Privacy Rule provision permitting use or disclosure of PHI for "law enforcement purposes"
It can. Some ODMAP Level 2 users work in law enforcement agencies. The Privacy Rule allows a covered entity to disclose PHI for a law enforcement purpose to a law enforcement official (as that term is defined in the regulations) for a number of reasons."[69] Two of the reasons are potentially implicated by ODMAP usage. These two are disclosures to law enforcement: (1) to report PHI when required by law;[70] and (2) when responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity.[71]

The situation in item (1) is discussed in more detail above in relation to disclosures "required by law."[72] As noted there, if state law directs an individual to report a fairly limited amount of PHI—in the form of a geolocation of a known or suspected overdose—via ODMAP, that falls squarely within this permitted use/disclosure to the extent that the ODMAP Level 2 user is a law enforcement official.

With respect to item (2), the disclosure of PHI to law enforcement is permitted if the disclosure "appears necessary to alert law enforcement to . . . [t]he commission and nature of a crime; . . . [t]he location of such crime or of the victim(s) of such crime; and . . . [t]he identity, description, and location of the perpetrator of such crime."[73] In some regions of the country, the site of a

would be impossible to enumerate all of the scenarios that may warrant disclosure of protected health information pursuant to this section.")
[68] Eric D. Hargan, Determination that a Public Health Emergency Exists (October 26, 2017), available at https://www.hhs.gov/sites/default/files/opioid%20PHE%20Declaration-no-sig.pdf (last accessed February 5, 2020); *HHS Acting Secretary Declares Public Health Emergency to Address National Opioid Crisis* (October 26, 2017).
[69] 45 CFR § 164.512(f).
[70] 45 CFR § 164.512(f)(1)(i).
[71] 45 CFR § 164.512(f)(6).
[72] *See* pages 11-13.
[73] 45 CFR § 164.512(f)(6)(i).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

known or suspected overdose is considered a crime scene.[74] In those areas, the reporting of overdose incident information via ODMAP amounts to notifying a local law enforcement agency with Level 2 access of the location of a crime (overdose incident) and the victim of the crime (the person who suffered the actual or suspected overdose).

How does the "minimum necessary" requirement factor into this analysis?
With respect to permitted uses or disclosures of PHI allowed under ~~both~~ the "public health activities and purposes," "serious threat to health or safety," and "for law enforcement purposes" provisions, the covered entity is required to make reasonable efforts to limit the PHI disclosed to the minimum necessary to accomplish the intended purpose of the disclosure.[75] As noted above,[76] in cases where the disclosure is "required by law," the minimum necessary requirement is not applicable.

In the case of ODMAP, the disclosure of PHI to Level 2 users is quite limited. The primary piece of identifying information is the approximate location of the known or suspected overdose. Absent geographical location information, the only way a Level 2 user could tie a reported overdose incident to any location at all (other than being in the U.S. or U.S. territory) is if the name/agency associated with the Level 1 user who reported provides a clue regarding the state or locality. Removing geolocation from ODMAP, therefore, would eliminate any benefit of using ODMAP for public health purposes.

Given the necessity of including geolocation information in the data set, ODMAP achieves disclosure of only the "minimum necessary" by introducing an element of vagueness into the location data. This imprecision in location is achieved by several factors, including not disclosing to users specific addresses (in fact, the database does not contain street addresses) and limiting the zoom level available to users such that any one data point on the map corresponds to several hundred feet on the ground. The imprecision in mapped location balances the need to protect PHI while not hampering Level 2 users using the information to develop public health responses.

Have any federal or state courts addressed ODMAP in any capacity?
There are no reported state or federal cases in Westlaw as of February 29, 2020.

[74] *E.g.*, Jeff Mordock, *N.Y. police now treat drug overdose sites as crime scenes in bid to take down dealers*, The Washington Times (February 19, 2019), available at https://www.washingtontimes.com/news/2019/feb/19/new-york-opioid-overdose-sites-now-crime-scenes/ (last accessed March 3, 2020).
[75] 45 CFR §§ 164.502(b) and 164.514(d).
[76] *See* page 8.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.

Are there any publicly available legal opinions addressing ODMAP and the Privacy Rule, and what are the conclusions?

As of February 2020, the Offices of the Attorney General in three states—Maryland, South Carolina, and Nevada—have issued legal memoranda analyzing the interplay between ODMAP and HIPAA. In each opinion, the respective attorney general's office concludes that the Privacy Rule allows the reporting of overdose information from covered entity Level 1 ODMAP users to Level 2 ODMAP users.

The first, and arguably most thorough, analysis comes from Maryland's Office of the Attorney General (Maryland AG).[77] Specifically, the Maryland AG concludes that both HIPAA and Maryland confidentiality law allow Maryland EMS providers who respond to known or suspected overdoses to report to ODMAP in connection with their response activities. The primary conclusion of the Maryland AG is that "there is a strong argument that EMS providers and law enforcement entities may both be given access to [ODMAP] so long as [it] is for the purpose of public health surveillance activities—*i.e.*, seeing where overdoses are occurring, so as to plan and provide additional resources for overdose response and treatment—-and is not used for the investigation or prosecution of criminal activity at a specific location."[78]

In reaching this conclusion, the Maryland AG, in a thorough and well-researched manner, determines that local law enforcement agencies (at least generally) may constitute "public health authorities" under the Privacy Rule, given that they often act pursuant to mandates with a public health component.[79] Likewise, the Maryland AG reviews the "serious threat to public health or safety" exception and also finds that it applies. In doing so, the Maryland AG concludes that this exception "seems fairly easily applicable to the risks addressed by [ODMAP]" in that giving first responders "the tools they need to properly respond to opioid overdoses serves 'to prevent or lessen a serious and imminent threat to the health and safety of a person.'"[80] Moreover, while ODMAP users do not know in advance the identity of the person(s) they will help because of the information, they do know in advance that a properly targeted and equipped response will lessen that threat. Also, as noted within this document, the Maryland AG observes that information reported to ODMAP by non-covered entity Level 1 users does not implicate the Privacy Rule.

In South Carolina, a state agency asked the state's Attorney General (South Carolina AG) if "the ODMAP application ('app') violates any state or federal law including HIPAA."[81] As in Maryland, the South Carolina AG finds no violation of law. In fact, the South Carolina AG specially references the Maryland AG's opinion, stating "[w]e have studied the Maryland

[77] Memorandum from Adam Snyder, supra note 37.
[78] *Ibid.* at 2.
[79] For purposes of local law enforcement, the Maryland AG notes that police officers and local law enforcement officials are issued doses of naloxone specifically for treating overdose victims, a public health activity much more than a criminal justice activity.
[80] *Ibid.* at 10.
[81] Letter from Robert D. Cook to Joseph Y. Shenkar (March 5, 2019).

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

Memorandum and advise that it provides an excellent analysis of the law and is correct."[82] Ultimately, the South Carolina AG concludes "[i]t is our opinion also that the interest of public safety and public health in providing treatment to opioid overdose victims overrides the privacy interest involved and is paramount."[83]

Most recently, the Nevada Department of Health and Human Services (DHHS) asked the Nevada Office of the Attorney General (Nevada AG) if reporting information through ODMAP implicates the Privacy Rule as to covered entities, and if so, if any exception permits disclosure to ODMAP.[84] The Nevada AG answered in the affirmative. With respect to the "serious threat to health or safety" exception, the Nevada AG concludes that "participation by first responders in ODMAP is reasonably characterized as necessary to prevent or lessen a serious threat to the health and safety of the public. Furthermore, the process for disclosing information through ODMAP to law enforcement and DHHS is narrowly tailored to protect sensitive information."[85] With respect to the "public health activities and purposes" exception, the Nevada AG noted that DHHS is authorized by law to collect overdose information.

Have any federal agencies weighed in on ODMAP and protected health information issues?
Not directly. However, the use of ODMAP is supported by many federal partners of the W/B HIDTA. In 2019, the U.S. Department of Justice, Bureau of Justice Assistance (BJA) and the Centers for Disease Control and Prevention (CDC) announced the ODMAP Statewide Expansion and Response grant solicitation.[86] BJA/CDC awarded grants to eight states in Fall 2019 (Connecticut, Florida, Georgia, Minnesota, Nevada, New Jersey, Ohio, and Rhode Island) to achieve statewide implementation of ODMAP within two years. [87] Moreover, the Office of National Drug Control Policy, Executive Office of the President has financially and intellectually supported LAPPA's development of the Model Overdose Mapping and Response Act that would require use of ODMAP by state and local agencies.

Has HHS investigated ODMAP or a covered entity reporting to or using ODMAP for failing to adhere to the Privacy Rule?
Not as of February 2020.

[82] *Ibid.* at 2.
[83] *Ibid*. at 6.
[84] Letter from Aaron D. Ford to Richard Whitley (June 25, 2019).
[85] *Ibid.* at 4.
[86] Background information available at https://www.coapresources.org/Content/Documents/Funding/ODMAP_Statewide_Expansion_and_Response_Grant.pdf (last accessed February 5, 2020).
[87] Defined as capturing fatal and nonfatal overdoses identified by first responders for at least 80 percent of the counties in the state.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.

Are there recommendations to further reducing the possibility of violating the Privacy Rule with ODMAP?
Participating agencies should ensure that the agreements required for gaining access to ODMAP make clear that such access may be used only for response to, and treatment of, overdoses and may not be used for law enforcement investigative or prosecutorial purposes.

What aspects of state PHI laws should be reviewed to determine how ODMAP interacts with those laws?
The analysis of how ODMAP interacts with a state law governing disclosure of PHI works much the same way as the analysis in this document. If there is no governing state law, or the state law is equal to or less strict than the Privacy Rule, then this analysis applies. Only if a state law is stricter must a second state-specific analysis be completed.

This project was supported by Grant No. G1999ONDCP03A awarded by the Office of National Drug Control Policy, Executive Office of the President. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government. Research is current through February 2020.