ALAN WILSON
ATTORNEY GENERAL

March 5, 2019

Joseph Y. Shenkar, General Counsel
South Carolina Department of Alcohol
And Other Drug Abuse Services
Post Office box 8268
Columbia, SC 29202

Dear Mr. Shenkar:

You have sought our opinion concerning whether the ODMAP application ("app") violates any state or federal law including HIPAA (Health Insurance Portability and Accountability Act of 1996), Pub.L. 104-191, and which protects the confidentiality of medical records. By way of background, you state the following:

> South Carolina, much like the rest of the nation, is facing the hardships of the current opioid epidemic. In 2017, our state saw more than 1,000 drug-induced overdose deaths, and for the first time in our state's history, drug overdose fatalities surpassed those caused by motor vehicle collisions. In December 2017, Governor Henry McMaster declared the opioid epidemic a "public health emergency" and issued an executive order that established the Opioid Emergency Response Team (OERT). The OERT was tasked with devising a multi-layered response plan to address the complex nature of this public health crisis. In June 2018, the Governor's Office published the first Opioid Emergency Response Plan. In Annex 4 of the plan, concerning coordination of law enforcement and other first responders, the OERT placed statewide usage of the ODMAP application by first responders as a mid-term goal to be implemented within six to 12 months.
>
> ODMAP was collaboratively developed by the Substance Abuse and Mental Health Services Administration and the White House Office of National Drug Control Policy in an effort to increase collaboration among first responders in the identification and reporting of drug-related overdoses. ODMAP provides real-time overdose surveillance data across jurisdictions to support public safety and health efforts to mobilize an immediate response to an overdose "spike." It links first responders on scene to a mapping tool that tracks overdoses and stimulates real-time response and strategic analysis across jurisdictions. The application initiates when first responders enter data into the system identifying whether or not the incident is fatal or non-fatal and whether or not naloxone was administered in a simple one-check system that takes seconds. No personal identifying information is collected on the victim or location. Unlike other reporting databases, the ODMAP application restricts the kind of information that can be reported and does not collect any personally identifiable information (e.g., names, addresses, telephone numbers). The

> data is then compiled to help improve response and treatment of future overdose victims by allowing predictive analytics to forecast "spikes" in overdose deaths and increase first responders' preparedness. Furthermore, ODMAP is only made available to first responders, such as emergency medical technicians and law enforcement, and only after the execution of a contract with the High Intensity Drug Trafficking Area program.
>
> Some first responders in South Carolina are disinclined to utilize ODMAP out of concern that they might violate state or federal privacy laws regarding protected health information. On October 19, 2017, the Maryland Attorney General's Office issued a comprehensive memorandum concerning first responders' use of ODMAP (enclosed hereto). The memorandum decisively opines that the information placed into the ODMAP application does not violate the federal Health Insurance Portability and Accountability Act (HIPAA) or any of Maryland's own state privacy laws.
>
> To clarify this issue for first responders in South Carolina, the S.C. Department of Alcohol and Other Drug Abuse Services is asking for an opinion on the following question: Does the information entered into the ODMAP application violate any state (e.g., §44-22-100, §44-115-40, §44-4-560, § 44-117-350, § 38-93-40) or HIPAA laws concerning protected health information?

We have studied the Maryland Memorandum and advise that it provides an excellent analysis of the law and is correct.

Law/Analysis

In South Carolina, there is a constitutional right to privacy. Art. I, § 10 of the South Carolina Constitution provides:

> [t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.

(emphasis added). In State v. Forrester, 343 S.C. 637, 644-45, 541 S.E.2d 837, 840-841 (2001), the South Carolina Supreme Court held that Art. I, § 10 bestows an independent right of privacy separate and apart from the 4th Amendment. There, the Court explained:

> [e]specially important in this analysis is South Carolina's explicit constitutional right of privacy. . . . In addition to language which mirrors the Fourth Amendment, S.C. Const. art. I, § 10 contains an express protection of the right to privacy: [quoting Art. I, § 10]. Initially, even in the absence of a specific right to privacy provision, this Court could interpret our state constitution as providing more protection than the federal counterpart. However, by articulating a specific provision against "unreasonable invasions of privacy," the people of South Carolina have indicated that searches and seizures that do not offend the federal Constitution may still offend the South Carolina Constitution resulting in the exclusion of the discovered evidence.

Forrester made it clear, however, that Art. I, § 10 did not convey an absolute constitutional right to privacy. In that case, the issue was whether Art. I, § 10 mandated "informed consent to government searches." 343 S.C. at 645, 541 S.E.2d at 841. Our Supreme Court concluded that it did not:

> As noted by the Court of Appeals, the drafters of our state constitution's right to privacy provision were principally concerned with the emergence of new electronic technologies that increased the government's ability to conduct searches. See Committee to Make a Study of the Constitution of South Carolina, 1895, Minutes of Committee Meeting 6 (Sept. 15, 1967). According to their minutes, "The committee agreed that [the search and seizure provision] should remain, but that is [sic] should be revised to take care of the invasion of privacy through modern electronic devices." Id. However, the committee also recognized that the provision would have an impact beyond just the area of electronic surveillance. As Committee Member Sinkler stated, "I think this is an area that, really, should develop and should not be confined to the intent of those who sit around this table." Id. at 6 (Oct. 6, 1967).
>
> Furthermore, the committee was aware they were drafting a provision that operated separately from the Fourth Amendment. . . During their discussions, the committee characterized the then prevailing United States Supreme Court standard as a liberal approach to the protection against search and seizure. Id. at 5 (Oct. 6, 1967). One committee member noted that "It is possible, too, that there will be a swing back from this liberal interpretation." Id. at 7 (Oct. 6, 1967).
>
> Forrester's "prior admonition rule" would subsume the "totality of the circumstances" test followed by this Court in State v. Wallace, 269 S.C. 547, 238 S.E.2d 675 (1977). Forrester also fails to cite any authority from South Carolina or any other jurisdiction adopting the rule she advocates. Except for the narrow Washington state exception for warrantless searches of the home, no precedential support for Forrester's position can be found. . . In conclusion, while our state constitution may provide a higher level of protection in the search and seizure context, it does not go so far as to require informed consent prior to government searches.

343 S.C. at 647-48, 541 S.E.2d at 842-43.

As noted above, Art. I, § 10 prohibits "unreasonable" invasions of privacy. Typically, however, issues of an imminent threat posed to health and public safety is overriding and is not deemed to be an "unreasonable invasion of privacy" for purposes of a release of confidential records to law enforcement or those who would use such records to treat the individual. The various statutes which you reference in your letter generally make exceptions for public health and safety in protecting the confidentiality of records. See Op. S.C. Att'y Gen., 1984 WL 159892 (July 24, 1984) [§ 44-23-1090 (now § 44-22-100(5) and (6)) "make an exception when disclosure is necessary in cooperating with law enforcement or public safety is involved. . . ."].

Indeed, the United Sates Supreme Court has upheld as reasonable the drug testing of railroad employees, even though there was no probable cause or reasonable suspicion that the

employee was using drugs based upon overriding public safety. In the words of the Court, "the governmental interest in ensuring the safety of the travelling public and of the employees themselves plainly justifies prohibiting covered employees from using alcohol or drugs on duty, or while subject to being called for duty." Skinner v. Railway Labor Executives Assn., 489 U.S. 602, 621 (1989). This interest in public safety was deemed "compelling," and thus "the toxological testing contemplated by the regulations is not an undue infringement on the justifiable expectations of privacy of covered employees. . . ." Id. at 633.

Your letter also references a Memorandum, dated October 19, 2017, written by the Maryland Attorney General's Office, and which analyzes state privacy laws, as well as HIPAA in the context of the use of the ODMAP app. In that Memorandum, the Maryland Attorney General concluded:

> [a]s discussed in greater detail below, I believe there is a strong argument that EMS providers and law enforcement entities may both be given access to the OD Map so long as their use of the app 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. Limited in that fashion, allowing access likely does not run afoul of HIPAA or the Maryland Act. This is not to say that there is no risk that the federal Department of Health and Human Services ("HHS")—which oversees the enforcement of HIPAA—or a reviewing court might conclude otherwise; there clearly is. But the arguments supporting the use of OD Map are strong enough that our Office can and will defend an agency's decision to use the tool. Whether to use the tool, of course, is something for each agency to decide.

Moreover, the Memorandum further stated:

> Disclosures to address a threat to public health or safety
>
> HIPAA also allows for the disclosure of PHI when necessary "to prevent or lessen a serious and imminent threat to the health and safety of a person or the public" when the disclosure is "to an entity that is reasonably able to prevent or lessen the threat." 45 C.F.R. § 164.512(j)(l). This provision appears to have been designed to allow for disclosure of a patient's medical information to prevent harm to an identified individual or to control the spread of a contagion, for example.
>
> While this exception may not have been originally drafted with public health monitoring tools in mind, its language seems fairly easily applicable to the risks addressed by the OD Map. It seems to me indisputable 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." The OD Map enables first responders to focus resources on a given area—thus reducing response time—and respond with the appropriate naloxone dosage to treat the victim—thus saving the victim's life. Although the designers of the OD Map do not

> know in advance which "person" may be saved, the information sharing that it provides clearly does help to save a person's life.
>
> I also think that the OD Map serves "to prevent or lessen a serious and imminent threat to the health and safety of ... the public." The ravages of opioid addiction and overdose are too well-documented to be disputed; it clearly is a public health and safety crisis, nationwide and here in Maryland. See, e.g., Executive Order 01.01.2017.11. And while the officials who use the OD Map do not know in advance the identity of the person they will save, they do know in advance that their response—properly targeted and equipped—will "lessen" a serious threat to public health and safety. . . .

We also note that in Maier v. Green, 485 F.Supp.2d 711, 721, n. 4 (W.D. La. 2007), the District Court agreed with reasoning similar to that contained in the Maryland Memorandum. There, the Court addressed the "threat to public health or safety" exception to HIPAA. The Maier Court stated:

> [i]t is worth noting that although this exact issue is not addressed, under the "HHS Questions and Answers FAQ's in Privacy of Health Information/HIPAA Disclosures In Emergency Situations," the U.S. Department of Health and Human Services explains that in cases of imminent danger "Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person for the public – consistent with applicable law and the provider's standards of ethical conduct."
>
> . . . .

Similarly in Op. S.C. Att'y Gen., 1975 WL 174062 (May 26, 1975), we addressed the situation involving mental health records, made confidential pursuant to § 44-23-1090 [now §44-22-100], and whether such records could be shared with outside medical personnel. Our opinions answered the question in the affirmative, as follows:

> Section 32-1022 [now § 44-23-1090], CODE OF LAWS OF SOUTH CAROLINA, 1962, as amended, prohibits disclosure of confidential records except in certain specified instances. When disclosure to persons outside the Department of Mental Health is necessary to further the treatment of the patient, certain safeguards should be used to insure that adequate confidentiality is maintained. Any release of records should be accompanied by sufficient notification to all who have access to the records of the fact that the records are confidential and the contents should not be disclosed. This could be facilitated by delivering the records in a sealed envelope with a brief notation on the outside that the records are confidential and also have a designated space on the envelope on which any person having access to the records would sign before viewing the records. Also I would suggest that the hospital have the consulting member of the staff make the persons with whom he or she is to be working aware of the confidentiality of the records. Another recommended safeguard is that the hospital would release only the portion of the record necessary

to perform the medical functions at the hospital outside of the Department of Mental Health.

Your letter states that the ODMAP app is quite limited in any intrusion. You note that "[n]o personal identifying is collected on the victim or location." In addition, you state that [u]nlike other reporting databases, the ODMAP application restricts the kind of information that can be reported and does not collect any personally identifiable information (e.g. names, addresses, telephone numbers)." Importantly, you advise that "ODMAP is only made available to first responders, such as emergency medical technicians and law enforcement and only after the execution of a contract with the High Intensity Drug Trafficking Area Program." With these important restrictions in mind, while we understand and appreciate the concern that first responders may have regarding a potential violation "State or federal privacy laws regarding protected health information," we believe the interests of public safety and the treatment of opioid abuse victims is paramount.

Conclusion

We agree with the Memorandum prepared by the Maryland Attorney General's Office which concludes that the limited data-sharing provided for through the ODMAP likely does not violate HIPAA or state privacy laws. It is our opinion also that, the interest of public safety and public health in providing treatment to opioid overdoes victims overrides the privacy interests involved and is paramount. See Curtis v. State, 345 S.C. 557, 549 S.E.2d 591 (2002) [public safety in workplace transcends privacy interests and other interests]. We can think of no interest more important today than providing treatment to opioid abuse victims. As we stated in an opinion many years ago, "[t]here exists ample authority, under present cases that the right of privacy may be overridden by the State's interest in protecting the health and welfare of its citizens." (June 3, 1986) [citing Whalen v. Roe, 429 U.S. 589 (1977) and other authorities]. Thus, we believe that the use of ODMAP app would withstand scrutiny with respect to privacy and confidentiality concerns.

Of course, we also must advise caution just as did the Maryland Attorney General's Office. Patient privacy concerns are fundamental and must be protected. Use of the app to locate and treat a potential opioid abuse victim should not go beyond the bounds you have indicated. As the Maryland Attorney General's Office advised, "[t]he State emergency response agencies that elect to use the ODMAP map 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." This is sound advice.[1]

[1] We note also that in Op. S.C. Att'y Gen., 2016 WL 1167292 (February 24, 2016), we discussed at length the Supreme Court's decision of Perry v. Bullock, 409 S.C. 137, 761 S.E.2d 251 (2014) which deemed an autopsy report a "medical record" and thus confidential for purposes of FOIA. There is, of course, a considerable difference between public disclosure of records generally and disclosure to law enforcement and other first responders for purposes of providing treatment to opioid abuse victims. Compare § 44-22-100(5) [authorizing disclosure of confidential mental health records for purposes of public safety or "furthering the welfare of the patient or the patient's family."].

With those caveats in mind, we believe the ODMAP app may be used to locate and treat opioid abuse victims in the manner set forth in your letter.

Sincerely,

Robert D. Cook
Solicitor General