ACLU Pennsylvania

MEMORANDUM

TO: Pennsylvania House Health Committee

FROM: Elizabeth Randol, Legislative Director, ACLU of Pennsylvania

DATE: May 15, 2020

RE: OPPOSITION TO SENATE BILL 1110 P.N. 1661 (K. WARD)

Senate Bill 1110 (P.N. 1661) proposes a fundamental change in both content and scope to Pennsylvania's Disease Prevention and Control Law of 1955 (35 P. S. §§ 521.1–521.21), which prohibits state and local health authorities from disclosing reports of diseases or records pertaining to diseases to anyone outside those agencies, "except where necessary to carry out the purposes of this act."

SB 1110 largely keeps the current statute intact, but creates a new provision that regulates the disclosure of private health information related to a communicable disease that is the subject of a disaster declaration that:

- Requires (rather than limits) disclosure of "individually identifiable health information" within 24 hours of a confirmed case;
- Broadly defines the content of the health information to be collected/maintained;
- Expands the agencies with whom this personal health information is shared (beyond state and local health authorities) to include 911 centers, law enforcement officers, fire department personnel, emergency medical services personnel, ancoroners; and
- Discloses this data to *each* of those entities in *each* county in the commonwealth.

While SB 1110 aims to assist first responders by sharing identifying information of everyone who tests positive for a communicable disease declared as a disaster emergency, its provisions are needlessly invasive, capture more data than is reasonably warranted, and risk breaches by requiring health data to be shared so broadly.

The Pennsylvania Constitution places a high value on individual privacy, including medical privacy.[1] But the right to privacy, like all constitutional rights, is not absolute. When an individual's right to privacy is implicated, courts will use a balancing test to determine whether the invasion of privacy is outweighed by a compelling state interest.[2] There is no doubt that significant state interests are at stake here, given the grave public health risk posed by COVID-19. But even in the midst of extraordinary circumstances, fundamental rights can — and must — be protected against unnecessary government intrusion.

On behalf of over 100,000 members and supporters of the ACLU of Pennsylvania, I respectfully urge you to oppose Senate Bill 1110 for the following reasons:

---

[1] Article 1, Section 1 of the Pennsylvania Constitution provides even "more rigorous and explicit protection for a person's right to privacy" than the federal constitution. *In re B*, 394 A.2d 419, 425 (Pa. 1978). The right to privacy, for Pennsylvanians, is considered "as much property of the individual as the land to which he holds title and the clothing he wears on his back." *Pa. State Educ. Ass'n v. Commonwealth, Dep't of Comm. & Econ. Dev.*, 148 A.3d 142, 151 (Pa. 2016) (quoting *Commonwealth v. Murray*, 223 A.2d 102, 109 (Pa. 1966)). In *In re B*, 394 A.2d 419 (Pa. 1978), the Pennsylvania Supreme Court found that a mother's psychiatric records could not be subpoenaed in connection with a dependency placement for her son. The Court found that while the information might be "useful," the "right of privacy . . . must prevail." 394 A.2d at 426. In 2019, the Court reiterated that while protected medical information could be constitutionally disclosed in some instances, it "admonished that it should not be subject to wholesale release." *In re Fortieth Statewide Investigating Grand Jury*, 220 A.3d 558, 570 (Pa. 2019); *see also Stenger v. Lehigh Valley Hosp. Ctr.*, 609 A.2d 796, 800-801 (Pa. 1992) (finding privacy interest not to be offended by disclosure of HIV status *because* disclosure of information was anonymous).

[2] An individual's right to privacy is weighed against a countervailing state interest. *Denoncourt v. Commonwealth, State Ethics Comm'n*, 470 A.2d 945, 948 (Pa. 1983). An intrusion into a person's private affairs is only justifiable "when the government's interests are significant and there is no alternate reasonable method of lesser intrusiveness to accomplish the government's purpose." *Id.* at 949. "Whether there is a significant state interest will depend, in part, on whether the state's intrusion will affect its purpose; for if the intrusion does not affect the state's purpose, it is a gratuitous intrusion, not a purposeful one." *Id.*

SB 1110 will apply to all communicable diseases, not just COVID-19

SB 1110 would require disclosure of information for ***all*** infectious diseases, not just COVID-19, that become the subject of a disaster emergency. SB 1110's provisions are cabined such that the governor must first declare an emergency based on a communicable disease, but disclosure of health data would then be required, even if the nature of the disease does not lend itself to first responders benefitting from such information.

SB 1110 captures and maintains private health information far exceeding COVID-19 status

SB 1110 would collect "individually identifiable health information" defined as "*information, whether oral, written, electronic, visual, pictorial, physical or in any other form that relates to an individual's past, present or future physical health status, condition, treatment, service, products purchased or provision of care*." This data **must** reveal the identity of the person who is the subject of the record OR serve as a reasonable basis upon which to identify that person. In other words, these records *cannot be anonymous*.

In March, the U.S. Department of Health and Human Services's Office for Civil Rights issued guidance that states the HIPAA Privacy Rule does permit an entity like a health department to release protected health information to first responders "to prevent or lessen a serious and imminent threat to the health and safety of a person or the public."[3] But SB 1110 mandates disclosure of records far beyond what first responders may need when responding to a call. For instance, do first responders need to know what products someone has purchased when responding to a call? Their past COVID status if they are now testing negative? What treatment (including experimental) they may have received? It strains credulity to imagine that this much information is necessary before first responders can safely respond to a call.

SB 1110 requires disclosure to an alarmingly broad audience

SB 1110 requires that ***all*** personal information be disclosed to ***all*** 911 centers, law enforcement officers, fire department personnel, EMS personnel, and coroners in ***every*** county. There are approximately 4,800 entities across the commonwealth that could receive individually identifiable health information, including volunteer departments and private vendors that provide first responder services, like ambulance companies. Simply stated, SB 1110 puts personal health information in more hands than is necessary and hopes that employees do not violate someone's privacy. This is a dangerous gamble, especially considering how much personal information is collected and required to be disclosed.

SB 1110 is silent about data security precautions, raising critical questions

SB 1110 puts an enormous burden on first responders to maintain, manage, and protect private health data.

- What is the mechanism used to share this data every 24 hours? Is the information protected by end-to-end encryption during transmission?
- Once the information is received by each of the entities listed in this bill, how is that data protected within each agency/department? What measures are in place by each entity to protect against a data breach or hack?
- How many people can access the data, and who (at each entity) is providing oversight of that access?
- What kind of federal and state HIPAA / confidentiality compliance training is being provided to each receiving entity to ensure they comply with relevant privacy laws?
- Who is in charge, at each of the receiving entities, of making sure the information isn't being misused or abused?
- What is the liability exposure to each of these entities should there be unauthorized sharing of data or a data breach/hack?
- Why is there no provision to destroy this data after a period of time, or after a person is no longer contagious, or at least destroyed when the disaster declaration is lifted? Who would be responsible, at each agency/department, for destroying that information after they receive it? What mechanism does the state have to confirm that health data is destroyed?

---

[3] U.S. Department of Health and Human Services's Office for Civil Rights, COVID-19 and HIPAA Disclosures to First Responders, Public Health Authorities, March 24, 2020, *at* https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf

SB 1110 proposes overly-broad and ill-suited measures to protect first responders

When balancing public health and privacy interests, the ACLU relies on medical expertise to identify and assess the health interests at hand. Protecting the health of first responders is clearly an important priority for the state. However, public health experts[4] have noted that disclosing names and addresses of those testing positive for COVID-19 does not ensure a first responder would be safe from exposure. Many cases of COVID-19 are asymptomatic,[5] present mild symptoms, or are undiagnosed due to limited availability of tests.[6]

It is also important to recognize the critical role confidentiality plays in protecting the public health. Sharing individually identifying medical information of those who test positive could deter some people from getting tested. There is a long history of social stigma[7] attached to communicable diseases; vulnerable populations such as unhoused or undocumented individuals, or people living in marginalized and over-policed communities may not be willing to get tested if they know their information will end up in the hands of government authorities other than those responsible for public health. Confidentiality laws are neither insignificant nor mere administrative burdens; in fact, they are integral to successful public health management.

SB 1110's mandated disclosure of individually identifiable health information is far from the least intrusive way to achieve the state's goal of protecting first responders. At an absolute minimum, collecting less information and disclosing it to fewer entities might begin to better balance these two critical interests.

SB 1110 is an outlier among other states that share protected health information

12 states currently share PHI with first responders: AL, FL, MA, MN, NH, NC, OH, RI, SC, TN, VA, WI
Bordering states: Of the states that border Pennsylvania (DE, MD, NJ, NY, OH, WV), only Ohio currently shares protected health information with first responders.

Among the 12 states that share protected health information with first responders:*

- **Enabling mechanism:** 11 states share data per an executive order by the governor, by the state department of health, or through guidance, MOU, or similar agreement between the state department of health and dispatch centers. Pennsylvania would be the only state to enable data sharing solely by expanding the state's right to share statutorily protected confidential health information.
- **Applicability:** ALL states limit the data they share to positive cases of COVID-19. Because it amends PA's Disease Prevention and Control Law, SB 1110 would apply to all communicable diseases that are the subject of a disaster declaration.
- **Information shared:** 8 states limit data sharing ONLY to addresses of people who have tested positive for COVID-19. 4 states share names and addresses. None require the collection and sharing of the breadth of "individually identifiable health information" allowable under SB 1110.
- **Receiving entity:** 11 states disperse information from departments of health or local health boards only to 911 centers or other dispatch agencies. SB 1110 would require information to be dispersed to over 4,700 entities, including 911 centers, fire departments, EMS, law enforcement, and coroners.
- **Jurisdiction:** ALL limit the sharing of protected health information to the geographic region of the dispatch center / local health authority. SB 1110 would require distributing PHI to **each** of the receiving entities "in each county of this Commonwealth."
- **Data retention:** 9 include specific provisions to destroy the data collected either after a certain number of days or upon terminating the order or lifting the emergency declaration. SB 1110 includes no provision pertaining to retention or destruction of the individually identifiable health information.

Complete state comparison data can be found here.

---

[4] Greenwald, Robert. (2020 March 23). Applying Lessons Learned from the AIDS Epidemic to the Fight Against COVID-19. Harvard Center for Health Law and Policy Innovation. chlpi.org/applying-lessons-learned-from-the-aids-epidemic-to-the-fight-against-covid-19

[5] The Centers for Disease Control, How COVID-19 Spreads. https://www.cdc.gov/coronavirus/2019-ncov/prepare/transmission.html

[6] U.S. FDA (2020, February 29). COVID-19 Update: FDA Issues New Policy to Help Expedite Availability of Diagnostics. fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-issues-new-policy-help-expedite-availability-diagnostics

[7] Williams, J. L. (2011). Infectious diseases and social stigma. Applied Technologies and Innovations, 4(1), 58–70. academicpublishingplatforms.com/downloads/pdfs/ati/volume4/201105020547_07_ATI_V4_JoanWilliams_et_al_Social__Stigma.pdf