Maryland
GOVERNOR'S OFFICE OF CRIME PREVENTION AND POLICY

Summary: Data Sharing Within Police-Behavioral Health Collaborations

The Centers of Excellence (COE) within the Governor's Office of Crime Prevention and Policy[1] is pleased to assist communities in Maryland with improving the criminal legal response to adults with behavioral health needs, intellectual and developmental disabilities, and neurocognitive conditions by redirecting these individuals when appropriate to the healthcare system, thereby reducing unnecessary incarceration while improving public health and safety.

[1] *Please note that the Governor's Office of Crime Prevention, Youth, and Victim Services (GOCPYVS)* ***was renamed to the Governor's Office of Crime Prevention and Policy*** *by the Moore-Miller Administration, effective immediately, on 1/18/2024. This change does not invalidate previous, current, or future agreements or documents referencing the agency as GOCPYVS.*

Purpose

This document is intended to provide a topic overview and catalog of resources to facilitate the development of data-sharing strategies that promote public safety while aligning with state and federal privacy laws. This document is not intended to offer legal advice.

Background

The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes a set of national standards for implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The U.S. Department of Health and Human Services issued the Privacy Rule to standardize the use and disclosure of protected health information (PHI) by organizations subject to the Privacy Rule ("covered entities"); the Privacy Rule also defines standards that protect individuals' rights to understand and control the use of personal health information. Federal regulations define the following terms:

- ***HIPAA***[2]: HIPAA stands for "Health Insurance Portability and Accountability Act of 1996." It is a set of federal rules designed in part to protect the privacy of a person's healthcare information.[3]
- ***Privacy Rule***[4]: The Privacy Rule sets standards to protect healthcare information by regulating healthcare information that can be linked with a person. Healthcare information is any data relating to a person's past, present, or future health, or the payment for healthcare.[5]
- ***Protected health information (PHI)***: Healthcare information linked with personal identifying information is called "protected health information (PHI)." The Privacy Rule protects all PHI held or transmitted by a covered entity or its business associate, in any form (e.g., electronic, paper, or oral).
- ***Covered entity*** [6]: A covered entity is a healthcare provider, health plan, or healthcare

[2] See 45 C.F.R. § 160.103: https://www.law.cornell.edu/cfr/text/45/160.103.
[3] https://www.hhs.gov/hipaa/for-professionals/index.html
[4] U.S. Department of Health and Human Services. (2024, July 22). *The HIPAA Privacy Rule.* https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule&text=The%20Rule%20requires%20appropriate%20safeguards,information%20without%20an%20individual's%20authorization.
[5] U.S. Department of Health and Human Services. (2022). *Summary of the HIPAA Privacy Rule*. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[6] https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

clearinghouse; if a covered entity engages a "business associate" to help it carry out its healthcare activities and functions, the covered entity must have a written contract or arrangement that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

- ***Part 2***[7]: The regulations at 42 CFR part 2 ("Part 2") protect the confidentiality of substance use disorder (SUD) treatment records. Part 2 protects "records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or … assisted by any department or agency of the United States."

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by covered entities. A covered entity **may not** use or disclose protected health information except as the Privacy Rule permits or requires OR as authorized in writing by an individual or personal representative. A covered entity is permitted but not required to use and disclose protected health information without an individual's authorization under the following circumstances[8]:

- to the individual;
- for treatment, payment, and healthcare operations;
- in situations that clearly give the individual the opportunity to agree or object;
- incidentally to an otherwise permitted use and disclosure;
- for public interest and benefit activities, limited to twelve national priority purposes;[9] or
- within a limited data set for the purposes of research, public health, or healthcare operations.[10]

---

[7] https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-part-2/index.html

[8] Aggregate health data is generally considered to be de-identified and not subject to HIPAA if it meets certain conditions; the bulleted circumstances pertain to information that is not de-identified and therefore subject to the requirements of the Privacy Rule.

[9] The twelve national priority purposes include certain circumstances of the following purposes: (1) required by law (i.e., statute, regulation, or court order); (2) public health activities (e.g., FDA, OSHA, etc); (3) victims of abuse, neglect, or domestic violence; (4) health oversight activities (e.g., audits and investigations); (5) judicial and administrative proceedings; (6) law enforcement purposes (limited to six specific circumstances); (7) decedents (e.g., coroners, medical examiners, and funeral directors); (8) cadaveric donation; (9) research; (10) serious threat to health or safety; (11) essential government functions; and (12) workers' compensation.

[10] A limited data set is a limited set of identifiable patient information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set is not de-identified information and is still subject to the requirements of the Privacy Rule.

A covered entity is **required** to disclose protected health information in only two situations:

- to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
- to the U.S. Department of Health and Human Services (HHS) when it is undertaking a compliance investigation, review, or enforcement action.

Additionally, covered entities may be **required by law** (including by statute, regulation, or court orders) to use and disclose protected health information without individual authorization. State and local[11] laws contain a number of statutory reporting obligations that may apply within the context of law enforcement and behavioral health, including the following circumstances:

- child abuse or neglect;[12]
- abuse, neglect, or financial exploitation of a vulnerable adult;[13]
- abuse of a developmentally delayed individual;[14] and
- threat to inflict imminent physical injury on a specified victim or victims.[15]

Resources

As noted by policy analysts, corroborated by healthcare providers and first responders, and confirmed by research, the sharing of information across systems is essential to reducing the number of people with behavioral health needs in carceral settings. The availability of timely information can enhance safety and improve recovery outcomes.

Legal framework

As stakeholders strive to accommodate HIPAA requirements and other federal and state confidentiality laws, misconceptions may complicate the development of information-sharing agreements, collaborative strategies, and appropriate technology. Many agencies, such as HHS and the Substance Abuse and Mental Health Services Administration (SAHMSA) as well as agency partners and grantees, have developed resources to describe the landscape of information sharing in the context of privacy laws.

[11] Health-Gen §20-701, Health Gen §20-702 (moving vessel injuries), Health Gen §20-703 (gunshot injuries), and COMAR 10.07.04.05 (burn injuries) apply in the following counties: Allegany, Anne Arundel, Charles, Harford, Kent, Montgomery, Prince George's, Somerset, Talbot, and Wicomico.
[12] Fam Law § 5-704 and § 5-705
[13] Fam Law § 14-302(a) and (d)
[14] Health Gen §7-1005
[15] Cts. & Jud. Proc. § 5-609(b)

- ➢ HHS manages a webpage to act as a one-stop resource for federal guidance and other materials on how HIPAA applies to mental health and substance use information.
    - Office for Civil Rights. (2024, August 6). *Information related to mental and behavioral health, including opioid overdose.* U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html
- ➢ This HHS resource (linked on the one-stop page) addresses some of the more frequently asked questions about when the Privacy Rule permits a health care provider to share the protected health information of a patient who is being treated for a mental health condition. It addresses three key topics, the last of which has specific relevance to law enforcement: 1) how information related to mental health is treated under HIPAA; 2) when information related to mental health may be shared with family and friends of an individual with mental illness, including parents of minors; and 3) the circumstances in which information related to mental health may be disclosed for health and safety purposes.
    - Office for Civil Rights. (n.d.). *HIPAA Privacy Rule and sharing information related to mental health.* U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf
- ➢ This HHS resource (linked on the one-stop page) expands on the resource *HIPAA Privacy Rule and Sharing Information Related to Mental Health*. It directly addresses the question, "What constitutes a 'serious and imminent' threat that would permit a health care provider to disclose PHI to prevent harm to the patient, another person, or the public without the patient's authorization or permission?" by explaining that HIPAA defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health or safety posed by a patient, allowing, "health care providers to disclose the necessary protected health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, caregivers, and law enforcement, without a patient's permission."
    - Office for Civil Rights. (n.d.). *HIPAA Privacy Rule and sharing information related to mental health.* U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf
- ➢ This page summarizes a presentation by John Petrila, a national expert on data sharing and privacy law, offering strategies to enable appropriate information sharing between healthcare and criminal legal agencies; video is embedded for viewing as well. Petrila

suggests developing clear goals for information sharing and a framework to guide that effort, offering step-by-step instructions for doing so.

- Policy Research Associates. (2018, October 29). *Point-of-service information sharing between criminal justice and behavioral health partners.* https://www.prainc.com/point-service-information-sharing-criminal-justice-behavioral-health-partners-addressing-common-misconceptions/#

➢ This guide describes how HIPAA and Part 2 may affect exchanges among behavioral health care, law enforcement, and criminal legal system professionals, offering answers to frequently-asked scenario-based questions.

- Council of State Governments Justice Center. (2010). *Information sharing in criminal justice–mental health collaborations: Working with HIPAA and other privacy laws.* https://csgjusticecenter.org/cp/publications/information-sharing-in-criminal-justice-mental-health-collaborations/

➢ The Center of Excellence on Protected Health Information is grant-funded by the Substance Abuse and Mental Health Services Administration and administered by Cicatelli Associates Inc. in partnership with the Legal Action Center and the Network for Public Health Law. CAI offers expertise in practical strategies for improving health equity in focus areas including mental health and substance use.

- Cicatelli Associates Inc. (2024). *The Center of Excellence on Protected Health Information.* https://caiglobal.org/index.php?option=com_content&view=article&id=1149&Itemid=1953]

Law enforcement

Several agencies and organizations have developed fliers of relevant provisions for law enforcement that can be shared and posted in common areas.

➢ This resource, created by HHS, provides a brief summary of the relevant provisions that determine when a HIPAA covered entity may disclose PHI to law enforcement.

- Office for Civil Rights. (n.d.). *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A guide for law enforcement.* U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf

Strategies

Communities across the country have developed practical strategies for legally sharing behavioral health information to improve outcomes for people in their communities. Some of these efforts to support their police-mental health collaborations (PMHCs) while complying with HIPAA and the Privacy Rule are simple while others are more complex.

- ➢ Many jurisdictions have developed strategies to appropriately share information among behavioral health and law enforcement agencies by acknowledging the need for trust, the value of lived experience, and the benefit of sharing the minimum information necessary. This tip sheet provides practical strategies at the PMHC and state policy level.
    - Council of State Governments Justice Center. (2019, October). *Sharing behavioral health information: Tips and strategies for police-mental health collaborations.* https://csgjusticecenter.org/wp-content/uploads/2019/11/JC-Information-Sharing-for-Police-Mental-Health-Collaborations.pdf
- ➢ CSG Justice Center partnered with IJIS Institute to host a webinar on Secure Data Environments (SDEs), which can securely manage inquiries to participating agency source data systems. Presenters provide the steps necessary to develop a local SDE and address privacy concerns related to HIPAA and other relevant laws and regulations.
    - IJIS Institute. (2021, October 26). *Information sharing between justice and mental health partners: Beyond data warehouses* [Webinar]. Council of State Governments Justice Center. https://csgjusticecenter.org/events/information-sharing-between-justice-and-mental-health-partners-beyond-data-warehouses/
- ➢ A comprehensive 2020 report written for the Office of the District of Columbia Auditor (ODCA) states that the District, "can ensure compliance with all federal and local laws and appropriately tailor the information shared, by creating a process to obtain written, informed consent from individuals with SUDs who receive care at a community-based SUD provider or from DBH [Department of Behavioral Health], or who receive care inside DOC [Department of Corrections]...It is allowable under Part 2 for patients to specifically designate entities that can make disclosures or to provide a 'general designation' like 'my treating providers' or 'all programs in which the patient has been enrolled as an alcohol or drug abuse patient' in their consent, offering the flexibility of one consent form facilitating communications between DOC, DBH, and individual care providers in the community." The report goes on to provide guidance for the creation of interagency data-sharing protocols that allow for just-in-time interventions and ensure continuity of care while protecting privacy, promoting access to treatment, and reducing stigma. A

copy of the data-sharing agreement is included in the report ("Appendix B").

- ➢ Council for Court Excellence. (2020, August 25). *Everything is scattered…The intersection of substance use disorders and incarcerations in the District.* Office of the District of Columbia Auditor. https://dcauditor.wpenginepowered.com/wp-content/uploads/2023/08/SUD.Report.8.25.20.pdf

Discussions regarding information sharing are occurring within a broader conversation exploring the roles of cities, counties, providers, and law enforcement in responding to people with behavioral health needs. The Department of Justice has investigated the intersection of law enforcement and behavioral health to prioritize a behavioral health response whenever possible given concerns about excessive use of force by law enforcement disproportionately impacting individuals with serious mental illness.[16] The International Association of Chiefs of Police agrees, stating that those who don't fall into the category of potentially dangerous behavior are more appropriately handled by a civilian provider response.[17] However, as stated by Balfour et al. (2021), "the question is not just whether law enforcement should respond to behavioral health emergencies but how to reduce unnecessary law enforcement contact and, if law enforcement is responding, when, how, and with what support."[18]

- ➢ The establishment of 988 offers an opportunity for states and local communities to improve the response to behavioral health crises and redefine the roles of law enforcement and 911. This brief provides an overview and tips to assist communities in integrating 988 into the continuum of care.
    - ○ Council of State Governments Justice Center. (2022.) *How to use 988 to respond to behavioral health crisis calls.* https://csgjusticecenter.org/publications/how-to-use-988-to-respond-to-behavioral-health-crisis-calls/#:~:text=The%20free%2C%20dedicated%20988%20line,call%20center%20in%20their%20community.
- ➢ This brief, the first joint product in a series from Policy Research, Inc. (PRI) and the National League of Cities (NLC), details the various co-responder models available to city

[16] Kesic D, Thomas SD, Ogloff JR. Estimated rates of mental disorders in, and situational characteristics of, incidents of nonfatal use of force by police. Soc Psychiatry Psychiatr Epidemiol. 2013 Feb;48(2):225-32. doi: 10.1007/s00127-012-0543-4. Epub 2012 Jun 29. PMID: 22744175.

[17] International Association of Chiefs of Police. (2018). *Responding to persons experiencing a mental health crisis.* https://www.theiacp.org/resources/policy-center-resource/mental-illness/

[18] Balfour, M. E., Stephenson, A. H., Delany-Brumsey, A., Winsky, J., and Goldman, M. L. (2021). Cops, clinicians, or both? Collaborative approaches to responding to behavioral health emergencies. *Psychiatric Services, 73*(6). https://doi.org/10.1176/appi.ps.202000721

and county leaders and provides site examples corresponding to model variations.

- Krider, A., Huerter, R., Gaherty, K., & Moore, A. (2020). Responding to individuals in behavioral health crisis via co-responder models. Policy Research, Inc. and National League of Cities. https://www.prainc.com/wp-content/uploads/2020/03/RespondingtoBHCrisisviaCRModels.pdf