P•C•R•C
PHYSICIAN CLINICAL REGISTRY COALITION

September 28, 2023

VIA ELECTRONIC MAIL (healthprivacy@help.senate.gov)

The Honorable Bill Cassidy, M.D.
United States Senate
455 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Cassidy:

The undersigned members of the Physician Clinical Registry Coalition (the "Coalition") appreciate the opportunity to respond to your request for information on improving Americans' health data privacy published on September 7, 2023 ("RFI"). The Coalition is a group of medical society-sponsored clinical data registries ("Registries") that collect and analyze clinical outcomes data to (i) identify best practices and improve patient care, (ii) enhance general knowledge through research projects, and (iii) support public health. We are committed to advocating for policies that encourage and enable the development of Registries and enhance their ability to improve quality of care through the analysis and reporting of clinical outcomes. All of the members of the Coalition are tax-exempt nonprofit organizations.

This letter provides background information on the value of Registries and the application of the Health Insurance Portability and Accountability Act ("HIPAA") to their operations. It then responds to the specific RFI questions that are most relevant to Registries.

The Value of Registries

The federal government, health care products manufacturers, and state and local governments have increasingly come to rely on Registries—and recognize their value—for a wide variety of purposes. For instance, the Food and Drug Administration ("FDA") has been encouraging drug and device manufacturers to work with Registries to conduct investigational and post-approval surveillance studies to ensure that both unapproved and approved drugs and devices are safe and effective. The Centers for Medicare and Medicaid Services ("CMS") has required participation in Registries as a condition of reimbursement for certain medical procedures that involve investigational or off-label (i.e., unapproved) uses of drugs or devices. Registries also report medical and clinical data to CMS on behalf of their participating health care providers ("Participants") for purposes of the Merit-based Incentive Payment System ("MIPS") program and for more general patient and disease tracking. Similarly, the Centers for Disease Control and Prevention ("CDC") and state and local governments are relying on Registries to track public health crises and responses.

The appropriate collection and use of protected health information ("PHI") is the foundation of this Registry work. The Coalition acknowledges the importance of the HIPAA Privacy and Security Rules (collectively, "HIPAA Rules") in ensuring patient privacy and the security of PHI and has diligently and successfully complied with them for over twenty years. Requiring entities covered by the HIPAA Rules to comply with possibly duplicative and redundant additional privacy or security laws, however, could be unnecessarily burdensome and hinder the important work of Registries. The current HIPAA Rules effectively ensure that the PHI that Registries collect is properly safeguarded. Likewise, the HIPAA Rules correctly do not regulate the use of properly de-identified data. The Coalition believes that imposing onerous restrictions on the use of de-identified data would result in significant, negative impacts on quality improvement, research, and public health.

The Application of HIPAA to Registries

Under HIPAA, PHI is individually identifiable health information that requires patient authorization for use and disclosure unless such disclosure falls within one of many exceptions.[1] HIPAA applies to "covered entities," defined to include health care providers that transmit health information in electronic form, health plans, and health care clearinghouses, as well as "business associates," defined as entities that provide services for or perform functions on behalf of covered entities, like Registries, that support or relate to the treatment, payment, or health care operations of such entities.[2]

The enactment of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") in 2009 extended HIPAA requirements and penalties to business associates.[3] Among other things, these changes subject business associates to the same penalties for unauthorized disclosure as covered entities and require business associates to notify individuals (or covered entities) and, in certain instances, the U.S. Department of Health and Human Services ("HHS") Secretary (the "Secretary"), in the event of a breach.[4] Business associates must also adopt appropriate policies and procedures to comply with the requirements of the HIPAA Rules.

The extent to which HIPAA applies to the activities of a Registry will depend on the nature of the data being collected and the purpose of the collection. Most Coalition Registries serve as business associates of the hospitals, physicians, and other covered entity sites from which they receive PHI and other data. These Registries perform data aggregation, curation, benchmarking, and analytic services on behalf of these covered entities for quality improvement purposes. They also perform secondary research on de-identified data and "limited data sets" that provide real-world evidence to support their Participants' quality improvement efforts.

The HIPAA Rules establish rigorous standards for the de-identification of PHI to ensure that it contains no personal identifiers or unique identifying numbers, characteristics, or codes, and so

[1] 45 C.F.R. §§ 164.502, 164.508, 160.103.
[2] *Id*. § 160.103. Health care operations include, among other activities, quality assessment and improvement activities.
[3] 42 U.S.C. §§ 300jj *et seq.*, 17901 *et seq*.
[4] *Id.* §§ 17934, 17937.

that the risk of re-identification is extremely small.[5] Once data is properly de-identified, it is no longer covered by the HIPAA Rules.

Registries also typically create limited data sets from the PHI they receive from their covered entity Participants. Limited data sets are information that is partially de-identified by removing direct identifiers like name, address, phone number, and email addresses, but that retains certain less sensitive PHI, such as an individual's date of birth, death, age, or address containing only the city, state, or zip code.[6] The HIPAA Rules require Registries to enter into data use agreements with their participating sites with conditions necessary to preserve the confidentiality and security of the limited data sets and restrict their use and further disclosure. The HIPAA Rules permit Registries to use and share limited data sets with their sites, researchers, and other parties for research, public health, and health care operations purposes, but only pursuant to the HIPAA-compliant data use agreement.

Some Registries collect PHI from Participants primarily for the purpose of engaging in research projects to enhance general knowledge about the safety and effectiveness of various medical procedures, diagnostic tests, treatments, and health care products. If PHI is being disclosed primarily for research purposes, the Privacy Rule requires either a patient's HIPAA authorization or a waiver of such authorization from an institutional review board ("IRB") or privacy board.[7] The criteria for IRB waiver authorization require that the applicant demonstrate that it has an adequate plan to protect PHI from improper use or disclosure and has other procedures for preventing unauthorized use or disclosure of the data. Typically, such plans and procedures involve the same level of privacy and security protections as those required by the HIPAA Rules for covered entities and business associates.

Registries that conduct research on human subjects (other than limited data sets) may also need to comply with the Common Rule[8] and/or the FDA's human subject protection regulations.[9] These rules have similar provisions to the HIPAA research rules. Human subject protection regulations apply to most Federally funded and to some privately funded research.[10]

Other Registries, such as public health databases, collect data on various population health events that may or may not involve medical treatment. The HIPAA Rules permit a covered entity to disclose PHI to a public health authority for certain public health activities and purposes, including preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.[11] Thus, where a state or federal law authorizes a public health authority to collect certain public health-related PHI, for

---

[5] 45 C.F.R. § 164.514.
[6] *Id.*
[7] "Research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. *Id.* § 164.501. Coalition members focused on research always obtain patient authorization or the appropriate waiver for their projects.
[8] 45 C.F.R. Part 46, Subpart A.
[9] 21 C.F.R. Parts 50 and 56.
[10] HHS, *Guidance Materials: Research*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/research/index.html.
[11] 45 C.F.R. § 164.512.

example, immunization data, a covered entity may share this information with a Registry operated for public health purposes without an individual's consent. The HIPAA Rules do not specify what types of procedures a public health authority must adopt to protect the privacy and security of PHI it receives under the public health exception. Coalition members serving this function, however, follow the same rules that apply to covered entities and business associates for the protection of PHI.

In short, regardless of the type of Registry or the purposes for which it collects data, Registries and their database vendors have adopted rigorous, HIPAA-compliant policies and procedures for protecting the improper use or disclosure of PHI. Coalition member Registries are all sponsored by physician-led medical societies or medical boards and, therefore, take this obligation very seriously.

General Privacy Questions

1. **What is health data? Is health data only data governed by HIPAA, or are there other types of health data not governed by HIPAA? Should different types of health data be treated differently? If so, which? How? If not, why not?**

The HIPAA Rules define health information as follows:

> *Health information* means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[12]

The Coalition sees no reason to reinvent the wheel and create a new definition of health data. The HIPAA definition is well understood in the health care field and broadly and accurately defines the data that Registries collect from their participating sites.

As noted above, the HIPAA Rules only cover PHI and explicitly do not apply to de-identified data. So, clearly there are health data that are not covered by HIPAA. The Coalition does not believe there is a public policy reason to regulate the use of properly de-identified data by nonprofit Registries who only use or disclose such data for research, public health, and quality improvement purposes consistent with their tax-exempt missions. As previously mentioned, federal agencies, including CMS, FDA, and CDC, are relying on such data, as are companies seeking to obtain or maintain FDA approval of their health care products.

[12] *Id.* § 160.103.

2. **Which entities outside of HIPAA Covered Entities should be accountable for the handling of health data (not necessarily HIPAA-covered data)? Should different types of entities have different obligations and privileges? Please explain using examples.**

As discussed above, the HIPAA Rules apply to covered entities and their business associates. They also cover limited data set recipients and researchers collecting PHI pursuant to HIPAA-compliant patient authorizations or IRB waivers. These entities are required to take similar measures to protect patient privacy and data security as covered entities. We believe the HIPAA requirements for business associates, limited data set recipients, and researchers are appropriate and are adequately tailored to the type of PHI they receive or the circumstances under which they receive it. For instance, business associates are subject to virtually the same rigorous HIPAA Rules as covered entities. The rules for limited data set recipients are more general, but this is appropriate given the less sensitive nature of this more limited form of PHI. Researchers either receive PHI pursuant to patient authorizations or IRB waivers and often have to comply with the Common Rule or FDA human subjects rules. This regulatory framework adequately protects the privacy and security of PHI.

That said, there are several exceptions to the patient authorization requirement in which there are no standards for protecting the PHI, including, without limitation, PHI received by public health entities, law enforcement, and health oversight activities. Recipients of PHI under these exceptions could be required to comply with the HIPAA Privacy and Security Rules.

3. **Should any or all of these entities have a duty of loyalty to consumers/patients?**
    a. **How could a duty of loyalty be imposed in a way that maximizes the safeguarding of consumer/patient data without creating burdensome implementation challenges? Should requirements of such a duty be based on the sensitivity of collected data? Please explain.**

A duty of loyalty is not necessary or appropriate in this context. The duty of loyalty is appropriate for fiduciaries, such as corporate directors, trustees, and investment advisors. It does not make sense for these purposes. Instead, a duty of care—meaning a duty to perform functions in good faith with the care that an ordinarily prudent person would reasonably be expected to exercise[13]—is standard under common law and state privacy laws and is sufficient to protect patient interests, both through civil lawsuits and regulatory enforcement. The duty of care does vary with the sensitivity of data. For instance, state and international consumer privacy laws only apply to personally identifiable data and not to de-identified data. Similarly, common law privacy cases generally would not apply to the wrongful disclosure of de-identified data.

[13] Principles of Corp. Governance § 4.01 (1994).

Health Information Under HIPAA

1. How well is the HIPAA framework working? What could be improved?

The Coalition believes that the HIPAA framework is effectively protecting patient interests. Our members and their database vendors are extremely diligent in their HIPAA compliance efforts. That said, as noted above, there are some gaps in the HIPAA Rules. In particular, recipients of PHI pursuant to the law enforcement, public health, health oversight, and other exceptions are not required to comply with any standards. The Committee may want to explore whether the HIPAA requirements for covered entities and business associates should be extended to recipients of PHI pursuant to these HIPAA exceptions.

2. Should Congress update HIPAA?

We do not believe Congress should be involved in updating HIPAA through legislation. As noted above, we generally feel that the HIPAA Rules are adequately protecting patient privacy and data security. More importantly, the legislative process can be cumbersome and time consuming. The HHS Office of Civil Rights ("OCR") and Office of Human Research Protections ("OHRP") are better equipped to make necessary changes to the HIPAA Rules and Common Rule, respectively. In addition, changes in the HIPAA Rules made through the regulatory process would allow for more robust stakeholder comment and input. Congress, however, should provide guidance and direction to OCR and OHRP based on the input it receives during this RFI process and otherwise.

3. Should Congress expand the scope of HIPAA? What specific information should be included in the HIPAA framework?

As noted above, the Coalition believes the HIPAA Rules adequately cover the use and disclosure of PHI, with the gaps we have identified. In particular, we do not believe the HIPAA Rules should be expanded to cover de-identified data. The use of de-identified, aggregated data by Registries is critical to accomplishing their quality improvement, research, and public health purposes. From a legal perspective, patients do not have rights in de-identified, aggregate data as such data are not tied to their identity. Indeed, all but one state assigns ownership of medical records to the health care providers that collect the data and not to patients.[14]

4. What challenges would legislative reforms to HIPAA create?

Per our comment above, OCR is better positioned to make changes to the HIPAA Rules and the rulemaking process under the Administrative Procedures Act, which provides stakeholders with the opportunity for meaningful input. The legislation process can take years to play out. However, Congress can play an important role in providing guidance and direction to OCR. We should also note that covered entities, business associates, and researchers have invested substantial resources in adopting HIPAA-compliant policies and procedures. Substantial

[14] George Washington Univ.'s Hirsh Health Law and Policy Program and the Robert Wood Johnson Found., *Who Owns Medical Records: 50 State Comparison*, http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison.

revisions to HIPAA could create unnecessary and costly redundancies, duplication, and other burdens on Registries that would not meaningfully enhance patient protections.

5. Are existing safeguards on the disclosure of health care data to law enforcement officials sufficient?

The HHS Office of Inspector General ("OIG") has independent authority to issue administrative subpoenas pursuant to 5 U.S.C. § 406(a)(4), and HIPAA authorizes the Department of Justice ("DOJ") to issue subpoenas for documents and testimony in investigations relating to any act or activity involving a federal healthcare offense.[15] In addition, the HIPAA Rules include an exception to the patient authorization requirement for disclosures to law enforcement agencies.[16] Registry data are potentially subject to third-party subpoenas seeking extensive data and documents, including PHI. Indeed, some Coalition members have received such subpoenas. These are cases in which Registries are not defendants, but are simply a source of data for prosecutors seeking to prove billing fraud by hospitals or physicians. These third-party subpoenas not only drain limited Registry resources, but also can discourage health care providers' willingness to submit data to Registries. Most importantly, the HIPAA Rules provide no clear protections for PHI obtained by law enforcement. We would like to see limits on this subpoena power. For instance, law enforcement could be required to (a) show a compelling need in order to subpoena Registry data or records, (b) obtain judicial approval, (c) comply with the HIPAA Rules for covered entities and business associates for protecting PHI, and (d) reimburse Registries for the reasonable cost of complying with such third-party subpoenas.

6. How should the sharing of health data across state lines be structured to account for different legal frameworks?

HIPAA provides a comprehensive framework for data that Registries receive and analyze. The HIPAA Rules only preempt state laws that provide *less* protection for patient privacy.[17] Many states have privacy and breach notification laws that impose more stringent privacy and security protections related to the use or disclosure of patient medical information. Currently, most state privacy laws exempt HIPAA covered entities and business associates, as well as nonprofit organizations. So long as state laws contain these exemptions, we think the HIPAA preemption rule provides adequate protection against varying state statutes. However, Registries are potentially subject to common law-based litigation in virtually any state from which they collect data. The HIPAA preemption rules should be clarified to provide a defense to such lawsuits if the Registry can show that it has met its HIPAA obligations.

[15] 18 U.S.C. § 3486.
[16] 45 C.F.R. § 164.512.
[17] *Id.* § 160.203.

Collection of Health Data

1. **How should consumer/patient consent to an entity to collect information be structured to minimize unnecessary data gathering? When should consent be required and where should it be implied?**

The HIPAA Rules and the Federal human subjects research regulations for researchers adequately define when it is necessary to obtain patient authorization/consent or a waiver of such authorization/consent from an IRB or privacy board. This framework is critical to the success of Registries. For instance, requiring covered entities or business associates to obtain patient authorizations for quality improvement activities would make it impossible for Registries to operate, as it would increase the administrative burdens and costs of clinical data collection.[18] Furthermore, such a requirement could significantly decrease the number of patients available for quality outcomes analysis and research and introduce selection bias in data collection.[19]

2. **How should information about data collection practices be conveyed to patients (i.e. plain language notice prior to consent, etc.)?**

The current HIPAA Rules requiring covered entities to develop and distribute a notice of their privacy practices are generally sufficient. Under these rules, covered entities should be disclosing whether they are sharing PHI with third parties for quality improvement, research, and public health purposes, whether pursuant to business associate agreements, data use agreements (for limited data sets), or IRB waivers.

3. **The European Union (EU) General Data Protection Regulation (GDPR) requires entities that collect personal data to delete it under certain circumstances if a consumer makes such a request. Should non-HIPAA covered entities be required to delete certain data at a consumer/patient's request?**

Not applicable to Coalition Registries.

4. **How should consumer online searches about health conditions (i.e., diabetes, in-vitro fertilization) be considered when part of health data?**

Not applicable to Coalition Registries

Biometric Data

Not applicable to Coalition Registries.

Genetic Information

Not applicable to Coalition Registries.

---

[18] Anthony L. Asher et al., *Regulatory Considerations for Prospective Patient Care Registries: Lessons Learned from the Nat'l Neurosurgery Quality and Outcomes Database*. Neurosurgical Focus. Jan;34(1):E5 (2013).
[19] *Id.*

Location Data

1. **How should location data that is being collected at a health care facility or website or other digital presence maintained by a health care entity be treated? For example, location data could potentially disclose a patient's health condition or treatment plan. Should this data be treated differently from the same data collected by non-health care entities?**

The HIPAA Rules adequately cover this issue by treating specific addresses as PHI but allowing less specific location information to be shared as limited data sets for research, health care operations, and certain public health purposes. As noted above, limited data sets are still protected by the HIPAA Rules because a covered entity sharing limited data sets must enter into a data use agreement with the limited data set recipient to preserve the confidentiality of the data and restrict its use, and the limited data set recipient must comply with the HIPAA protections for such information.

2. **What types of location data should or should not be considered health data?**

The HIPAA Rules adequately cover this issue.

Financial Information

Not applicable to Coalition Registries.

Sharing of Health Data

1. **Should there be an opt-in method of data collection for health data outside of the HIPAA framework versus an opt-out method? Please explain.**

As previously mentioned, requiring covered entities or business associates to obtain opt-in patient consent for quality improvement activities would make it impossible for Registries to operate, as it would increase the administrative burdens and costs of clinical data collection.[20] Furthermore, such a requirement could significantly decrease the number of patients available for quality outcomes analysis and research and introduce selection bias in data collection.[21]

2. **HIPAA permits the sharing of protected health information (PHI) under limited circumstances, provided the information is deidentified. Should this permissive framework be extended to the sharing of non-HIPAA covered data and what guardrails should be imposed?**

To meet the HIPAA Privacy Rule's de-identification standard, covered entities must use one of two validated methods: expert determination or safe harbor. Expert determination requires a formal determination by a qualified subject matter expert; the safe harbor method requires the

[20] *Id*.
[21] *Id.*

removal of 18 specified identifiers of PHI. De-identified data is fundamental to the work of Registries. It is critical that Registries be able to share de-identified data with third parties for research, public health, and other similar purposes. Furthermore, this sharing of de-identified data is essential to the development and assessment of medical treatments and procedures.

3. **Which, if any, obligations imposed on HIPAA Covered Entities should also be imposed on non-HIPAA Covered Entities handling health data? Please explain.**

We do not believe any additional obligations are necessary with respect to de-identified health data. Properly de-identified data should not pose significant risks to patients. As noted above, we think there is some room for extending the HIPAA Rules to entities that receive PHI under the various exemptions without having to comply with any privacy or security standards.

4. **What, if any, framework should be imposed on third parties who use third-party data sources to supplement HIPAA data to uncover an individual's health condition(s).**

Both de-identification methods are effective ways to protect patient privacy and maintain HIPAA compliance. We take patient privacy very seriously, and we have not had any members experience re-identification of Registry data.

Artificial Intelligence

Not applicable to Coalition Registries.

State and International Privacy Frameworks

1. **Currently 137 countries have a data or privacy framework in place. What have been the greatest challenges in complying with these frameworks for the governance of health data? Are there any policies that have been effective in safeguarding health data? What should be improved? How should the United States proceed, considering the existing international patchwork?**

Most member Registries are only collecting domestic data, meaning international privacy laws have not posed any challenges. However, for the few Registries collecting data from European Union patients, the General Data Protection Regulation ("GDPR") has posed significant challenges. The GDPR imposes a complex privacy regime that differs in certain key respects from the HIPAA Rules and has no exemption for compliance with local privacy laws like HIPAA or state privacy statutes. It is very burdensome for Registries to comply with both HIPAA and GDPR. International laws like GDPR need to provide an adequate exception for HIPAA-compliant entities. Alternatively, the federal government needs to provide entities that comply with HIPAA with immunity from international laws that do not provide such an exception.

2. **Nine states have passed data or privacy laws since 2018. What have been the greatest challenges in complying with these frameworks for the governance of health data? Have there been any lessons learned as states have implemented these laws on best practices to safeguard health data? How should the federal government proceed, considering the existing state patchwork?**

In response to the increasingly complex landscape of state privacy laws, we have analyzed the scope, applicability, key requirements, and relevant exceptions of the data privacy laws in thirteen states—California, Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia, and Washington. Most of these states exempt non-profits, covered entities, and business associates from needing to comply with the respective state data privacy law. Further, all of these state data privacy laws exempt PHI and de-identified data. Accordingly, these state laws have not yet posed major problems for Registries. However, if more states pass laws without these exemptions, it will make state-by-state compliance very difficult for Registries.

Enforcement

1. **What regulatory authorities does the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) have to safeguard health information that have not been exercised?**

We believe OCR is exercising appropriate authority over covered entities and business associates that do not have sufficient HIPAA policies and procedures or experience a data breach.

2. **OCR has primary authority over enforcement of HIPAA. However, other federal agencies such as the Federal Trade Commission (FTC) have oversight of certain health data that can implicate HIPAA. To what extent should these agencies have a role in the safeguarding of health data? What duplication or conflict currently exists between how different agencies enforce violations of health laws?**

As noted, we believe OCR's enforcement of HIPAA is sufficient. Multiple agency enforcement would be duplicative and burdensome. The FTC is better positioned to regulate non-health care consumer data and should not be in the business of regulating the use or disclosure of PHI.

3. **Please share challenges with compliance and enforcement of existing health data privacy and general data privacy laws. How should these challenges be overcome?**

As explained above, Registry data are potentially subject to DOJ and OIG third-party subpoenas, which not only drain Registry resources but also discourage health care providers' participation in Registries. We believe there should be limits to this subpoena power as described above.

******

The Coalition appreciates the opportunity to respond to your RFI. If you have any questions, please contact Rob Portman (Rob.Portman@PowersLaw.com), Leela Baggett

(Leela.Baggett@PowersLaw.com) or Allyn Rosenberger (Allyn.Rosenberger@PowersLaw.com) at Powers Pyles Sutter & Verville, PC.

Respectfully submitted,

American Academy of Neurology
American Academy of Ophthalmology
American Academy of Otolaryngology–Head and Neck Surgery
American Academy of Physical Medicine and Rehabilitation
American Association of Neurological Surgeons
American College of Emergency Physicians
American Society for Gastrointestinal Endoscopy
American Society of Anesthesiologists/Anesthesia Quality Institute
American Urological Association
Association for Clinical Oncology
Congress of Neurological Surgeons
Outpatient Endovascular and Interventional Society
Society of Interventional Radiology
Society of NeuroInterventional Surgery
The Society of Thoracic Surgeons