



Submitted to: healthprivacy@help.senate.gov

September 28, 2023

Senator Bill Cassidy, M.D.
Ranking Member
U.S. Senate Committee on Health, Education, Labor and Pensions
Washington DC 20510-6300

RE: Health Data Privacy Request for Information

Dear Senator Cassidy:

The Confidentiality Coalition appreciates the opportunity to provide feedback in response to your September 7, 2023, letter requesting information on various health data privacy issues (RFI).

The [Confidentiality Coalition](#) is composed of a broad group of hospitals, medical colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

I. General Comments

The Confidentiality Coalition strongly agrees that safeguarding patient privacy is a prerequisite for trust in our health care system. We also agree that, since its inception, the Health Insurance Portability and Accountability Act (HIPAA) has fostered that trust by providing a robust framework for the protection of protected health information (PHI), while allowing for its appropriate sharing as needed for treatment, payment, and health care operations.

As the RFI points out, there have been enormous technological advances since the passage of HIPAA that have not only transformed the ways in which health data is generated and collected, but also exponentially increased the amount and types of health data that fall outside the protections of HIPAA. The Confidentiality Coalition has long called for federal legislation that would provide strong national privacy and security protections, similar to those in HIPAA, for personal health information that falls outside HIPAA. We have enclosed for your consideration a copy of the Coalition's "Beyond HIPAA Privacy Principles" which set forth our position on this important issue.

As explained further in our Beyond HIPAA Privacy Principles, the Coalition believes that any federal privacy legislation should govern only personal health data that falls outside of HIPAA, thus preserving the existing HIPAA framework for PHI. The HIPAA framework was carefully calibrated to recognize the unique nature of health information used in the health care sector, and to ensure that its appropriate exchange for healthcare purposes continues without disruption while protecting patient privacy.

II. Specific Comments

A. General Privacy Questions

The RFI asks a critical foundational question, namely, what constitutes health data. We believe that the HIPAA framework can provide a useful guide in this regard. It first defines "health information" broadly, and then distinguishes between health information that identifies or can reasonably be used to identify an individual ("individually identifiable health information" or IIHI), and health information that does not.

Drawing from the HIPAA definitions¹, we recommend defining "health data" as any information, whether oral or recorded in any form or medium, that 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. IIHI is then health information that identifies an individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. IIHI created or received by on behalf of a HIPAA covered entity is PHI, and IIHI created and received by or on behalf of any other entity is referred to hereinafter as personal health information or personal health data. These definitions are also consistent with the definitions used in the Health Breach Notification Rule issued by the Federal Trade Commission (FTC) and the Information Blocking regulations issued by the Department of Health and Human Services (HHS) Office of the National Coordinator of Health Information Technology (ONC).

As with PHI under HIPAA, we do not recommend that federal health privacy legislation distinguish between different types of personal health data for regulatory purposes. All personal health information deserves robust privacy protection. In addition, experience has shown that applying different rules or levels of protection to different types of personal health data has the unintended consequence of causing data segmentation or "data siloing" to the detriment of patient care. Thus, in 2020, Congress passed section

¹ See 45 CFR 160.103 and Section 1171(4) of the Social Security Act.

3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act to better align the rules governing substance use disorder (SUD) patient records with HIPAA precisely in order to eliminate this type of data segregation.

We understand and support Congress' intent to protect personal health care information. All entities that collect or access personal health data should have a duty to protect that data and to use and disclose it only for appropriate purposes. Thus, entities outside the HIPAA framework should not have different obligations or privileges with respect to personal health information. Since the term "duty of loyalty" is open to different interpretations, we recommend that any privacy legislation specify the duties or obligations of entities that generate or collect personal health information. At a minimum, entities should be required to implement reasonable and appropriate physical, administrative, and technical safeguards to protect the information, to use and disclose it only for purposes that are consistent with the reasonable expectations of consumers/patients, and to adhere to the principle of minimum necessary in all aspects of their handling of personal health data. This will avoid creating burdensome implementation challenges while ensuring that data protections are maximized. The above protections should apply only to health data that identifies an individual or is reasonably capable of identifying an individual (i.e., personal health information) and not to de-identified data.

B. Health Information Under HIPAA

The HIPAA framework has been in place for many years and has served patients and the health care system well, establishing strong safeguards for the protection of PHI while facilitating its use and disclosure for health-related purposes. Its principles have been broad and flexible enough to accommodate significant changes in the health care environment and technological developments. In addition, through HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) Act, Congress has given the Department of Health and Human Services (HHS) broad authority to implement these requirements.

Since the HIPAA framework has worked and evolved well over time and is respected and understood by patients and the health care community, we do not believe there is any need for Congress to expand its scope, nor do we believe this would be beneficial. HIPAA is tailored to health care organizations, and its provisions were carefully designed to balance privacy protections with the appropriate flow of health information for health delivery and coverage purposes. While we strongly believe that other entities that have access to personal health information should be subject to privacy and security safeguards that are commensurate with those required under HIPAA, we do not believe that HIPAA should be expanded to encompass these entities. Instead, federal legislation to protect personal health information that falls outside of HIPAA should be enacted. That legislation should harmonize with HIPAA, such as using the same standards for de-identification, breach notification and risk-based security requirements. It should also include the same principles, such as minimum necessary, transparency in the form of a plain language privacy notice, and consumer rights. By using a separate legislative framework for health information that falls outside HIPAA, Congress will have

the flexibility to tailor the legislation to non-HIPAA entities that are not primarily engaged in health care.

National Privacy Standard

Should Congress choose to revisit HIPAA, it should create a true national standard by preempting all state privacy laws that apply to PHI. The Coalition has long advocated for strong national privacy standards and continues to believe that this is the best approach for both PHI and personal health data that falls outside HIPAA. Covered entities and their business associates have struggled for many years with the many different, sometimes conflicting state rules governing PHI, and this challenge has only increased over time as data is shared more easily and crosses state lines on a regular basis. In addition, the patchwork of different state laws has grown into a thicket in more recent years as more and more states have passed comprehensive privacy laws. While some of these laws carve out PHI, others do not or are unclear as to the application to PHI. This makes compliance a significant challenge, particularly for larger organizations that operate in all states, but even for smaller regional organizations, or local organizations that provide services to patients from other states. In all cases, requiring organizations to comply with multiple different, often inconsistent, privacy laws for the same health data not only creates complexities and compliance challenges, but does not serve the best interests of patients who are better served by a clearly understood, strong, implementable privacy standard. We therefore strongly urge that if Congress chooses to reopen HIPAA, it amends HIPAA to create a true national privacy standard by providing that HIPAA preempts state privacy laws that apply to PHI.

By the same token, any federal privacy law for non-HIPAA personal health data should similarly preempt state privacy laws that might otherwise apply to that data. As long as the federal privacy law provides a robust framework for the protection of personal health data, there is no need for, or benefit in, duplicative or overlapping state laws. On the contrary, it simply increases the costs and challenges of compliance without commensurate benefit to patients or consumers.

Accounting for Disclosures

If Congress chooses to reopen HIPAA, it should also consider repealing the expanded accounting for disclosure provision that was included in the HITECH Act.² HHS has not yet implemented this requirement since the statute requires that it do so in a manner that takes into account both the potential benefits and the administrative burden³, and HHS has received extensive feedback on multiple occasions that the costs and administrative burden in implementing this provision would be enormous. Having worked on this issue since 2009, the Confidentiality Coalition strongly believes that there is little demand for or benefit from this requirement, and that the resources it would require would be better invested in providing health care services.

² See Section 13405(c) of the HITECH Act.

³ Section 13405(c)(2) states that any regulations must “require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.

At the time the provision was included in the HITECH Act there was no HIPAA Breach Notification Rule in place, and patients had no legal right to know whether their PHI had been accessed or disclosed inappropriately. The expanded accounting provision was understood to have been enacted, at least in part, to address this concern. In addition, it was believed that EHR technology would soon automate the collection of this type of information such that responding to the expanded accounting request would involve little effort or expense on the part of health care providers. However, more than a decade later, the impetus for the requirement has fallen away and the expected advances in EHR technology have not occurred.

Today, EHR technology is still not capable of capturing and integrating all disclosures for treatment, payment, and health care operations into a single understandable format. Indeed, preparation of the existing, much narrower, accounting of disclosures reports today (for non-routine disclosures) requires significant manual effort, including chart review and searches of spreadsheets received from various departments and business associates. In addition, most hospitals and health systems have multiple information systems, the disclosures from which would need to be manually cataloged and collated. Lastly, patients who do ask for an accounting of disclosures under current law often reverse course when they are told what an accounting of disclosures report would contain. Instead, what these patients typically are seeking is an investigation into whether a specific user of the EHR inappropriately viewed their record. Patients already have a right to understand how their information is used for treatment, payment, and healthcare operations and, since 2013, the HIPAA Breach Notification Rule has required that patients be notified in detail if their PHI is used for unauthorized purposes that compromise their privacy. In light of these developments, we urge that if Congress considers making changes to HIPAA, it repeals the HITECH Act expanded accounting requirement, since it will serve only to increase costs to the health care system without commensurate benefits if ever implemented.

Law Enforcement and Public Health

To increase trust in the health care system, we recommend that HHS revise the HIPAA Privacy Rule to allow disclosure of PHI to law enforcement only pursuant to a court order or an individual authorization. Any authorization for this purpose should be required to include a prominent statement warning the individual that their authorization is voluntary and that their PHI could be used in legal or administrative proceedings or investigations against them or potentially others, such as their health care providers. Not only will this better protect patients' information from improper or unnecessary requests for PHI by law enforcement, but it will increase the level of trust between health care providers and their patients, resulting in more open exchanges and, ultimately, better patient care. It will also give HIPAA entities a clearer standard and greater certainty for compliance purposes.

Related to this, once PHI is disclosed to law enforcement or a public health authority, HIPAA no longer applies to the data and these entities may further use and disclose the data for purposes beyond those for which it is shared. This latitude erodes patient trust,

making patients reluctant to share information with their health care providers and health plans, even if they know that those entities will only use the information for appropriate purposes themselves. For example, when public health agencies encouraged individuals to share their health information with the agencies during the COVID-19 pandemic through tracking apps developed and operated by entities not bound by the HIPAA framework, many individuals declined to do so, concerned that the data could potentially be used for other purposes. Patients similarly did not want their health care providers or health plans to share this information with law enforcement or public health authorities. To avoid this distrust and to encourage the appropriate sharing of PHI for beneficial public purposes such as law enforcement and public health, HHS should consider amending the HIPAA Privacy Rule to provide that when PHI is provided to law enforcement, public health authorities and potentially other government agencies, those agencies must agree in writing that the PHI will only be used and disclosed by those agencies and their contractors for the purpose for which it was disclosed to the agency unless the data is deidentified.

Deidentification

Another area in which HHS should consider revising the HIPAA Privacy Rule is with respect to the de-identification of PHI. Given the amount of information publicly available, as well as the vast computing power and sophistication of artificial intelligence (AI) tools, data once thought to be deidentified may be at risk for reidentification using such AI tools. To address this concern, HHS should revise the HIPAA Privacy Rule by providing that, as a condition for treating data as de-identified when disclosed to another entity, the recipient must contractually agree not to attempt to re-identify the data.

HHS Breach Portal

A final area in which we would ask Congress to consider changes if it decides to reopen HIPAA is with respect to the HITECH Act requirement that HHS publicly post on its website a list that identifies each covered entity involved in a breach of unsecured PHI affecting 500 or more individuals.⁴ While we understand that Congress' goal in imposing this requirement may have been to act as a deterrent against poor privacy and security practices, the list has increasingly grown to include more healthcare organizations that are victims of cyberattacks or other crimes that have occurred despite the organizations having in place robust privacy and security protections.

We do not believe it is appropriate for organizations that are victims of cyberattacks or other crimes, such as robbery and looting, despite having in place appropriate safeguards, to be stigmatized by being publicly listed on the OCR website. Instead, these organizations should be encouraged to work with government agencies to help apprehend the criminals and prevent similar attacks on other entities. In addition, as consumer-serving organizations, health care organizations are already strongly incentivized to avoid the potential harm to consumers, as well as the loss of trust and associated reputational harm from required media postings. Finally, these public postings undermine patient confidence in the affected healthcare organizations and the healthcare system as a whole, which ultimately could adversely affect patient care.

⁴ See section 13402(e)(4) of the HITECH Act.

In light of the above, and the very changed information security landscape since the HITECH Act became law in 2009, we recommend that if Congress revisits HIPAA, it repeals this requirement. Alternately, if Congress believes there is still some utility to the public posting requirement, we recommend that it be revised in two respects, namely (1) to not require the public posting of names of organizations that have in place appropriate privacy and security protections but have been the victim of a cyberattack or other crime, and (2) to require that HHS remove the name of an organization from the list if the organization can demonstrate that it has taken appropriate corrective action and implemented privacy and security safeguards to avoid similar incidents in the future.

C. Collection of Health Data

The Confidentiality Coalition supports holding all entities accountable for the manner and purposes in which they collect, use and disclose personal health data without imposing responsibility on the consumer to police this through a formal consent mechanism.

While certain additional uses and disclosures may be conditioned on obtaining affirmative express consent, consumer consent should not be the primary mechanism to control how health data is used and disclosed. Not only does it inappropriately place the onus on the consumer to protect their own health data, but in most cases, it is an illusory control in that most consumers do not read consents and, even if they do, they have little option but to consent if they wish to proceed with the service in question. Consents also involve significant paperwork and administrative burden for entities required to collect them and keep them current. We recognize and support that when a third party, such as a law firm, requests patient information, this should be accompanied by a patient consent or authorization.

Instead, entities should be required to abide by common privacy principles⁵, including use consistent with consumers' reasonable expectations. Consumers' reasonable expectations should be set through the use of simple and plain language privacy notices that explain the purposes for which their personal health data is collected, as well as the consumers' rights and choices with respect to this information. Information collected by non-HIPAA entities should be required to be deleted when it is no longer needed for valid purposes consistent with consumers' reasonable expectations.

The RFI specifically asks how consumer online searches about health conditions, such as diabetes or in-vitro fertilization, should be considered when part of health data. Generally, we believe the same privacy rules stated above should govern the collection of data through online searches. Thus, if the data collected by an entity from a consumer online search can reasonably be linked to the health of that individual, it

⁵ See, for example, the Organization for Economic Co-operation and Development (OECD) ["Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."](#)

should be treated as IIHI. However, if there is not a reasonable basis to believe that the data relates to the health of the individual performing the search, the data should not be considered health data, let alone IIHI.

For example, merely because an identifiable individual conducts an online search about a particular health condition does not necessarily mean that the individual conducting the search has that health condition. On the contrary, it is very common for such a search to be performed by a caregiver, family member, friend, researcher, student or simply someone looking up a condition based on a news report or article they read. In most cases, it will likely require a very fact-specific inquiry to determine whether the data constitutes personal health information from a regulatory perspective.

In this regard, OCR issued a bulletin on December 1, 2022, entitled “Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates” (Bulletin)⁶ that discussed the use of tracking technologies on a HIPAA entity’s website. Among other things, the Bulletin concluded that a search for health conditions or for an available appointment with a health care provider by an IP address, even on an unauthenticated webpage of a covered entity, constituted PHI. This new and expansive interpretation of what constitutes PHI goes well beyond the regulatory definition and has far-reaching implications for HIPAA entities. In addition, the Bulletin addressed many complex and nuanced issues regarding online data collection that deserve careful consideration and input from the health care community. Given the significant regulatory ramifications of the new determinations and conclusions reached in the Bulletin, we do not believe that a guidance document such as the Bulletin is the appropriate vehicle to make such changes to the HIPAA Privacy Rule. As such, we urge Congress to direct OCR to rescind the Bulletin and instead follow the required notice and comment rulemaking process if it wishes to make these changes to the HIPAA Privacy Rule.

D. Specific Types of Data

As mentioned above, the Confidentiality Coalition does not believe it is necessary or advisable to distinguish between different types of personal health information from a regulatory perspective. Biometric information is a form of individually identifiable data and should only be regarded as health information to the extent it is collected in a health care context, consistent with the proposed definition of “health information.” Similarly, certain location data may be an indirect identifier and, if collected in a health care context, may meet the definition of personal health information. If so, it should be subject to the same privacy protections as other personal health information.

⁶ See <https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html> (“Tracking technologies on a regulated entity’s unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual’s email address and/or IP address when the individual visits a regulated entity’s webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.”)

Finally, while genetic information is inherently individually identifiable health information, we do not believe that different privacy rules or standards should be applied to it. To the extent the purpose for its collection meets existing definitions for human subject or other research, it should be subject to the rules governing such research.

E. Sharing of Health Data

As mentioned above, we do not support the use of an opt-in or consent as the primary mechanism to regulate the collection and use of personal health information outside HIPAA. Instead, we would recommend limitations on the purposes for which such data may be used and disclosed that are consistent with the individual's reasonable expectations based on the purposes for which the data was shared, and consistent with the entity's plain language privacy notice. Additional uses beyond these may require the individual's opt-in or affirmative express consent.

We support excluding deidentified data from a federal privacy law, provided that the deidentification standard is strong. This will encourage entities to deidentify data when practicable, which will improve the privacy of personal health data. It will also allow for greater use of the data for many beneficial types of data analytics and research, much of which would not be done if the data is subject to the same restrictions and limitations as apply to personal health information. With respect to the deidentification of personal health information, we recommend that the same deidentification requirements apply to personal health information that falls outside of HIPAA as applies to PHI. Thus, the recommendation above that, as a condition for treating data as de-identified when disclosed to another entity, the recipient must contractually agree not to attempt to re-identify the data, should also apply to the deidentification of personal health information that falls outside of HIPAA. By adopting the same deidentification requirements, a new federal privacy law would harmonize with HIPAA and avoid unintended consequences, such as potentially covering HIPAA deidentified data because it is no longer PHI but also not deidentified in accordance with the new federal law's deidentification requirements.

F. Artificial Intelligence

With respect to AI, we refer you to our comments submitted to your office on September 21, 2023 in response to the White Paper entitled "Exploring Congress' Framework for the Future of AI: The Oversight and Legislative Role of Congress Over the Integration of Artificial Intelligence in Health, Education, and Labor," to which we attached the Confidentiality Coalition's recently developed "Principles for the Responsible Development and Use of Artificial Intelligence in Health Care."

The RFI also asks to what extent patients should be able to opt-out of datasets used to inform algorithmic development. This should depend on the purpose for which the algorithms are developed, and not on the fact that AI or algorithmic processes are used. Thus, for example, if the algorithmic development is for a health care operation of a HIPAA covered entity, such as quality improvement or to help identify where clinical interventions are likely to be most effective, a patient should not be permitted to opt out

of the use of their data for this health care operation purpose just as they are not permitted to do so for other health care operation purposes. In contrast, if the algorithmic development is for marketing purposes, a HIPAA authorization would be required as it would for other uses of PHI for marketing purposes. Similarly, for non-HIPAA entities, it should depend on the purpose for which the algorithms are being developed, and whether this use falls within the reasonable expectations of consumers. The use of deidentified data should also be separately considered as a way to benefit from the power of AI while protecting privacy. Ultimately, AI is technological tool and, while a powerful one to which general privacy and security principles must be applied with great care, should not in and of itself warrant different privacy rules or principles when dealing with PHI and personal health data outside HIPAA.

G. State and International Privacy Frameworks

The RFI notes that nine states have passed data privacy laws since 2018 and asks what the greatest challenges are for compliance and how the federal government should proceed considering the existing state patchwork. As discussed above and in our Beyond HIPAA Privacy Principles, the Confidentiality Coalition believes strongly that privacy and security requirements for IIHI, whether PHI under HIPAA or personal health data outside of HIPAA, should be set at the federal level, creating a single, strong, uniform, national standard for each. Federal law should not operate merely as a floor, allowing states to pass more stringent privacy laws as is currently the case with HIPAA. This serves only to create confusion and uncertainty, increasing the costs and challenges of compliance without commensurate benefits to patients and consumers.

H. Enforcement

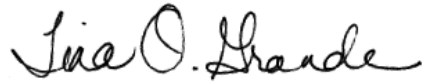
As the RFI points out, both OCR and the FTC have regulatory authority over health data. While the two agencies have worked well together and have gone to great lengths to explain to regulated entities and individuals how their authority overlaps and what this means as a practical matter, ultimately it would be simpler, clearer, and a better use of scarce regulatory resources to eliminate this overlap. Thus, OCR should have regulatory authority to implement and provide oversight with respect to HIPAA, and the FTC to implement and have oversight with respect to federal privacy legislation governing personal health data that falls outside of HIPAA.

Finally, as the number and types of laws governing health data proliferate, whether privacy, interoperability, information blocking, cybersecurity or otherwise, we ask that Congress and the relevant regulatory agencies consider the combined impact of the laws, as well as of other laws affecting health data. This evaluation would be to ensure that these laws are written and implemented to act harmoniously and in concert with one another as intended, and that Congress' priorities are reflected in their application. For example, there is a natural tension between privacy rules and the information blocking rules, and while the latter are written to create exceptions for privacy restrictions, the more the laws pull in opposite directions, the less effective each becomes. Thus, it is important for Congress and regulatory agencies to regularly evaluate from a holistic perspective, such as through annual or biannual reports by the Government Accountability Office, how the various laws governing health data are

operating together, and whether they are achieving their intended goals, and if not, to take action to correct course.

Thank you for your consideration of our comments. Please do not hesitate to contact me at tgrande@hlc.org or 202-449-3433 if you have any questions.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, prominent "T" and "G".

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council



Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.
 - a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.
 - b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.
2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:
 - a. Should not conflict with HIPAA,
 - b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
 - c. Should align with HIPAA's definitions of health information, and
 - d. Should adopt a risk-based approach for the development and implementation of security and privacy controls like HIPAA.
3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.
4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.
6. For data use and activities other than the purpose for which the data was provided, individuals must provide authorization for collection and use of individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.
7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.
8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.