November 9, 2016

Honorable Sylvia M. Burwell
Secretary, Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Recommendation on the HIPAA Minimum Necessary Standard

Dear Madam Secretary,

As Chair of the National Committee on Vital and Health Statistics (NCVHS or Committee), your advisory committee on health data, statistics, and the Health Insurance Portability and Accountability Act (HIPAA), I write to transmit findings and recommendations of the Committee regarding the HIPAA Privacy Rule's minimum necessary standard. This standard establishes the circumstances under which a custodian of protected health information must limit the sharing of information to the minimum necessary to accomplish the purpose of the disclosure.

The Committee held a hearing on the minimum necessary standard on June 16, 2016. Experts who testified agreed that this standard and its underlying principles are as important today as when the Privacy Rule was drafted. They underscored that although it is an integral part of the Rule, the minimum necessary standard remains poorly understood and inconsistently implemented by covered entities and their business associates. They also agreed that it is time to update the guidance and implementation specifications and work to improve compliance with the standard.

Executive Summary

The Committee reaffirms the importance of the minimum necessary standard as an essential provision of the HIPAA Privacy Rule for four key reasons. First, it limits disclosure of protected health information outside the HIPAA umbrella and serves as a guide for covered entities when responding to requests from third parties. Second, it serves as an added safeguard in combination with other policies and practices to ensure compliance by covered entities and business associates with the HIPAA Privacy and Security Rules. Third, it is an additional protection for patients in situations where authorization is not required. Finally, it serves as a critical check across the health information ecosystem, including public health, prompting dialogue about what information is needed and for what purposes.

The Committee's overarching recommendation is that HHS should update its guidance on the minimum necessary standard to incorporate changes to HIPAA introduced by legislation since the Privacy Rule became effective, and to address known barriers to effective implementation. To that end, the Committee offers ten recommendations. The first six address substantive issues with the minimum necessary standard or implementation specifications that should be addressed in updated guidance. These are:

Recommendation 1: HHS should clarify the independent obligations of business associates to comply with the minimum necessary standard and should develop specific guidance and instruction for business associates in this regard. HHS should also develop guidance for covered entities on oversight of business associate compliance with minimum necessary obligations.

Recommendation 2: HHS should clarify the breach notification requirements pertaining to violations of the minimum necessary standard. HHS' guidance should define the circumstances under which a breach of the minimum necessary standard occurs, at what level reporting is mandatory, and what types of enforcement may be expected for different violations.

Recommendation 3: HHS should clarify the elements of an adequate "specific justification" that is required to use, disclose, or request a patient's entire medical record. For example, HHS should illustrate with specific examples, use cases, or analytic methodologies circumstances that may legitimately warrant the use or disclosure of entire medical records and the justification that would be adequate to support each. The guidance also could recommend any special assurances about privacy and data security that covered entities should seek before supplying data for such uses.

Recommendation 4: HHS should require covered entities and business associates to adopt a list of criteria they will consider, a procedure for evaluating a request in accordance with the criteria, and a governance structure that provides oversight of the minimum necessary determination process.

Recommendation 5: The Committee recommends that HHS make no change to the current exception to the minimum necessary standard for treatment.

Recommendation 6: In developing new Minimum Necessary guidance(s), HHS should specifically address the application of the minimum necessary standard to HIPAA named transaction standards for administrative functions pertaining to payment and operations. In particular, HHS's guidance should address the applicability of the minimum necessary standard to new transactions, such as those involving attachments, and data exchanges involved in fulfilling alternative payment models.

The final four recommendations address ways to formulate, frame, and disseminate updated guidance and corresponding training materials. In particular, HHS should make a draft of the guidance available and solicit public comment prior to issuance in final form.

Recommendation 7: **HHS should offer education that clearly illustrates how the minimum necessary standard interacts with other provisions of the HIPAA Privacy Rule, to improve overall understanding of when the minimum necessary standard applies and when it does not apply. The Privacy Rule provides a four-tier framework of protections, which is subject to some misunderstanding among covered entities and the public. The Committee offers an analysis in Appendix A that explains these important interrelationships.**

Recommendation 8: HHS should issue updated guidance in draft form and solicit public comment before issuing final guidance.

Recommendation 9: HHS should prepare orientation materials and implementation guides tailored to the perspectives of various stakeholders.

Recommendation 10: In promulgating guidance, HHS should use a range of multimedia communication channels to disseminate published guidelines, "Frequently Asked Questions," web training, and case study illustrations tailored to the needs of various constituencies. Dissemination should include a public education component.

In addition to these recommendations, the Committee offers its preliminary perspective on issues relevant to the minimum necessary standard such as evolving technology, cybersecurity, and genetic information in Appendix B to this letter. These were beyond the scope of the June hearing and the Committee will consider how it might be of assistance to the Department in addressing these policy issues that, in the future, may place new pressures on the minimum necessary standard.

<u>The Minimum Necessary Standard and Implementation Specifications</u>

The minimum necessary standard embodies the general privacy principle that using, disclosing, or requesting a person's protected health information (PHI) impacts individual privacy. Covered entities, when they use or disclose PHI or request PHI from another covered entity or business associate, "must make reasonable efforts" to limit the PHI disclosed "to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[1] The minimum necessary standard acknowledges that PHI includes highly sensitive, personal information, and individuals care not only *whether* their data is shared, but they also care *how much* is shared.

After stating its broad minimum necessary standard, the Privacy Rule provides six exceptions. These exceptions allow data to be used by or disclosed to:

[1] *See* 45 C.F.R. § 164.502(b)(1).

1. Health care providers treating individuals;[2]
2. Individuals accessing their own information;[3]
3. Third parties that the record subject has authorized;[4]
4. The Secretary of HHS for performing oversight functions;[5]
5. Any party to whom the information is required to be disclosed by law;[6] and
6. Covered entities for their own HIPAA compliance activities.[7]

When the minimum necessary standard applies, covered entities must adhere to the implementation specifications.[8] These provide that the amount of information that is "necessary" should be judged relative to the data user's intended purpose.[9] Covered entities should use, disclose, and request only the least amount of PHI that is "reasonably necessary" to accomplish that purpose. They also must restrict the range of people who will have access to PHI. The minimum necessary standard requires covered entities to identify those persons or classes of persons "who need access to the information to carry out their duties," to limit their access to the types of PHI needed to do their jobs, and to place appropriate conditions on such access.[10]

For data disclosures and requests that are routine and recurring, covered entities should implement policies and procedures.[11] Covered entities may develop standard protocols for routine and recurring requests. For other, non-routine disclosures, case-by-case review is required, based on criteria that the covered entity must establish.[12] Importantly, the Privacy Rule provides for the possibility that, at times, a patient's entire medical record may be the minimum amount of data that is "necessary to accomplish the purpose of the use, disclosure, or request."[13] When this is true, the need for the entire medical record must be "specifically justified."[14]

The Department issued guidance on the minimum necessary standard in April 2003 when the original HIPAA Privacy Rule went into effect. The 2009 Health Information Technology for

[2] *See* 45 C.F.R. § 164.502(b)(2)(i).
[3] *See* 45 C.F.R. § 164.502(b)(2)(ii).
[4] *See* 45 C.F.R. § 164.502(b)(2)(iii).
[5] *See* 45 C.F.R. § 164.502(b)(2)(iv).
[6] *See* 45 C.F.R. § 164.502(b)(2)(iv).
[7] *See* 45 C.F.R. § 164.502(b)(2)(vi).
[8] *See* 45 C.F.R. § 164.514(d)(1)-(5).
[9] *See, e.g.*, § 164.514(d)(3)(i) (requiring minimum necessary disclosures of PHI to be limited "to the information reasonably necessary to accomplish the purpose for which the request was made."); § 164.514(d)(4)(i) (calling for covered entities, when requesting information, to limit their requests to what is "reasonably necessary to accomplish the purpose for which the request is made").
[10] *See* 45 C.F.R. § 164.514(d)(2)(i).
[11] *See* 45 C.F.R. § 164.514(d)(3)(i), (d)(4)(ii).
[12] *See* 45 C.F.R. § 164.514(d)(3)(ii), (d)(4)(iii).
[13] *See* 45 C.F.R. § 164.514(d)(5).
[14] *Id*.

Economic and Clinical Health (HITECH) Act[15] introduced some limits on covered entities' discretion for determining what constitutes "minimum necessary" and required covered entities to limit the use, disclosure of PHI, to the extent practicable, to a limited data set to accomplish the intended purpose of such use, disclosure, or request. HITECH also clarified that the custodian of the PHI (as opposed to the requester) is responsible for making the minimum necessary determination. HITECH called for the Secretary to issue guidance to clarify these changes no later than August 17, 2010. The Department has not yet issued this guidance.

In January 2013, the Department released a final rule, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*, that is known as the "Omnibus Rule."[16] The Omnibus Rule included amendments concerning the application of the minimum necessary standard to business associates when they are using, disclosing, or requesting PHI from a covered entity, and making business associates directly liable for violations of the minimum necessary standard. The Omnibus Rule also required that covered entities and business associates investigate any violation of the minimum necessary standard to determine the probability that PHI was compromised and whether a breach notification would be required. This Rule also clarified that genetic information is PHI and subject to the minimum necessary standard in the same way as any other PHI.

The Omnibus Rule sought to address concerns about how the minimum necessary standard applies to disclosures of data to public health officials. The implementation specifications originally allowed covered entities, when disclosing data to public health officials without individual authorization, to rely on public officials' representations that the amount of data requested was the minimum necessary.[17] However, privacy advocates, clinicians, and others raised concern that there was no oversight on potential overreach by public health officials since covered entities could simply defer to a requester's assessment that the amount of data requested was the minimum necessary. In response to this concern, the HITECH Act contained a provision requiring covered entities to determine the minimum amount of PHI for a disclosure.[18] The Department, after considering the issue, did not modify the provision of the Privacy Rule permitting a covered entity to rely on minimum necessary representations by public officials.[19] Access to data for public health activities continues to present weighty issues that will require a cautious and deliberate approach by HHS.

---

[15] The HITECH Act was passed as Div. A, Title XIII, and Div. B, Title IV, of Pub. L. 111-5, American Recovery and Reinvestment Act, 123 Stat. 115, at 226. The privacy provisions may be found at Sec. 13001, *codified at* 42 U.S.C. § 17921 *et seq*.
[16] 78 FED. REG. 5565 (Jan. 25, 2013).
[17] The specifications can be found at 45 C.F.R. § 164.514(d)(3)(iii).
[18] *See* HITECH Act, § 13405(b), *codified at* 42 U.S.C. § 17935.
[19] *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 78 FED. REG. 5566, 5700 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164) (revising various parts of 45 C.F.R. § 164.514, but not altering § 164.514(d)(3)(iii)).

Current State of Minimum Necessary Implementation

The 2003 HIPAA Privacy Rule was drafted and adopted at a time when health records were largely paper based and decentralized. Siloed paper records served as a *de facto* physical barrier that limited access and use. Today, electronic health records are rapidly becoming the norm, and the Department's policies promote interoperable health records so information is available when and where it is needed for coordinated patient care services. In addition, the Department's policy promotes the use of aggregated and de-identified health information to advance population and community health.

As the environment has changed and the Privacy Rule has been updated in ways that affect implementation of the minimum necessary standard, the guidance on how best to comply has not kept pace. Between 2003 and 2013, complaints related to the minimum necessary standard were among the top five issues investigated by the Office for Civil Rights (OCR). OCR has provided case study examples that highlight noncompliance caused by lack of organizational policy and training regarding application of the minimum necessary standard and by inappropriate handling of sensitive information.[20] The closely related issue of improper uses and disclosures of data has, every year through 2014, been the top issue investigated by OCR, and case examples OCR has published illustrate violations both in the actual disclosure and in the process. OCR has imposed remedial actions for infractions including the establishment of complete policies, institution of proper procedures, and improvements in training.

In preparation for testimony, the American Health Information Management Association (AHIMA) conducted an electronic survey of members working in privacy and security management, primarily in acute care environments. Three hundred six acute care hospitals or health systems responded. About half indicated that their organizations have policies and procedures related to the minimum necessary standard and a process for reviewing a request for information to determine whether it exceeds the adopted policy. Less than one-third of respondents have adopted an operating definition for what constitutes minimum necessary or have standard protocols to guide decisions about minimum necessary disclosures. In cases when a business associate carries out a disclosure on behalf of a respondent, fewer than half of the respondents reported having knowledge of the criteria used by the business associate in making minimum necessary determinations.

The Committee heard testimony that application of minimum necessary principles is an essential element of the overall design of the Privacy Rule precisely because the Rule permits many non-consensual uses and disclosures. We heard arguments in favor of applying the minimum necessary standard to disclosures for treatment and limiting disclosures for payment and health care operations to the least identifiable form. But we also heard that the current exception for treatment should be preserved at this time because of the potential impact on

[20] *See* case examples from the Office for Civil Rights, at U.S. Dep't of Health & Human Serv., "Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year," *available at* <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html>.

patient care, safety, legal liability and overall system efficiency. Even panelists who called for the minimum necessary standard to apply to treatment acknowledged that this would require information technology with advanced privacy functionality that does not now exist in practice.

The Committee heard testimony calling for a standard operating definition of "minimum necessary." We also heard testimony that the current implementation guidance calling for development of standard protocols for routine and recurring requests may be counterproductive because of the scale of disclosures and the burden of maintaining scores of such protocols. The current minimum necessary standard is based on "reasonableness" rather than an absolute standard, and the Committee heard testimony that this is a strength given the range of situations that arise in managing access, use, and disclosure.

Panelists at the July hearing were aligned that better guidance and improved education about best practices would be valuable. This includes guidance regarding the obligations of business associates. Current guidance ties the business associate's obligations to the covered entity's minimum necessary policies and procedures, a major challenge for business associates serving thousands or even tens of thousands of covered entities. Covered entities and business associates also need guidance as to whether disclosing more than the minimum necessary constitutes a reportable breach.

Short term Priorities and Recommendations

The Committee's overarching recommendation is that HHS update its guidance(s) on the minimum necessary standard to incorporate changes to the Privacy Rule introduced by the 2009 HITECH Act, the 2013 Omnibus Rule, and to address known barriers to effective implementation. As reported by our panelists, the lack of updated guidance creates a vacuum leading to a high degree of variability in how covered entities and business associates apply the minimum necessary standard. It should be noted that the Committee did not hear testimony from representatives of all types of covered entities such as physician practices, long term care facilities, or post-acute care facilities. However, the Committee believes it safe to assume that all will benefit from improved and updated guidance and corresponding education and training.

The first six recommendations address substantive issues with the minimum necessary standard or implementation specifications that should be addressed in updated guidance(s). The final four recommendations address ways to formulate, frame, and present updated guidance and corresponding training.

The Committee also discussed but is not offering recommendations on additional important issues relating to minimum necessary standard that were beyond the scope of the June 2016 hearing. These include minimum necessary implications of the evolving technology and data environment, cybersecurity, genetic information, and public health. A preliminary discussion of these issues is found in Appendix B.

Recommendation 1: Minimum Necessary and Business Associates

HHS should clarify the independent obligations of business associates to comply with the minimum necessary standard and should develop specific guidance and instruction for business associates in this regard. HHS should also develop guidance for covered entities on oversight of business associate compliance with minimum necessary obligations.

Under current guidance business associates contracts must limit uses of, disclosures of, and requests for PHI to be consistent with the covered entity's minimum necessary policies and procedures. The business associate is therefore expected to comply with the covered entity's policies. This can be problematic if the covered entity's practices are weak or inadequate. Further, business associates may contract with dozens, hundreds, or even thousands of covered entities each with their own policies and procedures.

Business associate guidance should make explicit the obligation of business associates to comply independently under the minimum necessary standard. Clarifying the obligations of the business associate to comply independently with the minimum necessary standard would be consistent with how other HIPAA provisions, such as the Security Rule, are handled for business associates. HHS should make explicit in its guidance for business associates the obligation to adopt compliant policies and procedures, and to provide evidence of compliance with minimum necessary standards. Covered entities can raise the bar at their discretion through business associate contracting, but specifying an independent obligation would create a baseline level of compliance that is not now in place.

Recommendation 2: Minimum Necessary and Breach Notification

HHS should clarify the breach notification requirements pertaining to violations of the minimum necessary standard. HHS' guidance should define the circumstances under which a breach of the minimum necessary standard occurs, at what level reporting is mandatory, and what types of enforcement may be expected for different violations.

The hearing revealed concerns regarding the relationship between the minimum necessary standard and breach notification requirements. In past guidance related to the HIPAA Breach Notification Rule, HHS has broadly stated that uses and disclosures of PHI that violate the minimum necessary provisions of HIPAA may qualify as breaches and that such incidents must be evaluated like any other security incident. Covered entities and business associates want to know under what circumstances the use or disclosure of PHI above and beyond what is minimally necessary to achieve a purpose constitutes a breach. For example, does it constitute a breach if a provider sends to a payer more data than what the payer needs to process a claim?

Under the Breach Notification Rule, a "breach" is defined as the unauthorized acquisition, use, or disclosure of PHI that compromises the security or privacy of such information. There are three exceptions to this definition: 1) when a member of the covered entity's workforce acquires or uses PHI in good faith, and does not further use or disclose the information in

violation of the HIPAA Privacy Rule; 2) when a person authorized to use PHI inadvertently discloses PHI to another person who is also covered by the Rule; and 3) when there is a good faith belief that the unauthorized person to whom the PHI has been disclosed would not be able to use or disclose the information. Given this definition and the exceptions, it is not clear under what circumstances a use or disclosure that included more than the information minimally necessary to achieve the purpose of the use or disclosure would constitute a breach.

Recommendation 3: Disclosing or Requesting a Patient's Entire Medical Record

HHS should clarify the elements of an adequate "specific justification" that is required to use, disclose, or request a patient's entire medical record. For example, HHS should illustrate with specific examples, use cases, or analytic methodologies circumstances that may legitimately warrant use or disclosure of entire medical records and the justification that would be adequate to support each. The guidance also could recommend any special assurances about privacy and data security that covered entities should seek before supplying data for such uses.

The minimum necessary standard has enduring relevance and in the years ahead, must be applied in a 21st-century data environment that challenges many of the assumptions underlying the original Privacy Rule. One important aspect of the future data environment is a growing capacity to extract useful insights (for treatment, research, and public health applications) by marshaling very large, detailed data resources that juxtapose individuals' longitudinal health histories with other sources of data characterizing their biology, behaviors, exposures, outcomes, and subjective patient experiences.

The minimum necessary standard is rooted in a 20th-century concept of hypothesis-testing studies, where investigators knew in advance precisely what they were looking for and could specify the data that would be "necessary" to test the hypothesis. In contrast, many 21st-century clinical, research, public health, and regulatory science questions lend themselves to hypothesis-free analysis: for example, sifting through large datasets to identify correlations between genotype and phenotypes to discover the clinical significance of a novel genetic variant, or searching through insurance records for signals of adverse events in patients who received certain treatments. For these analytical methods, the "minimum necessary" data to support discovery may be "as much data as can be obtained."

The Privacy Rule has always allowed for the possibility that, for some uses, a patient's entire medical record may be the minimum amount of data that is "necessary to accomplish the purpose of the use, disclosure, or request."[21] The Privacy Rule states that when this is true, the need for the entire medical record must be "specifically justified."[22] As advanced "big data" analytic techniques grow more common in coming years, covered entities may face a greater number of requests for patients' entire medical records. They could benefit from guidance on

[21] *See* 45 C.F.R. § 164.514(d)(5).
[22] *Id.*

appropriate criteria to apply, procedures to follow, and questions to ask when reviewing such requests.

Recommendation 4: Standard Protocols for Minimum Necessary

HHS should require covered entities and business associates to adopt a list of criteria for consideration, a procedure for evaluating a request in accordance with the criteria, and a governance structure that provides oversight of the minimum necessary determination process.

The current standard requires a covered entity to adopt *a priori*, a set of procedures and standard protocols for processing requests for PHI. However, the Committee heard testimony that developing standard protocols in advance for each type of disclosure (e.g. ER, admitting, radiology, etc.) is complex and burdensome, because each disclosure is necessarily contextual. Covered entities are continually processing substantial volumes of both requests and disclosures, but to try to create minimum necessary protocols for each routine disclosure or request creates an excessive burden that outweighs the benefits contemplated by the Rule. It is not practical or necessary to determine what can be used, disclosed, or requested, included or excluded, in every possible circumstance. Moreover, what we learned from the AHIMA survey was that the majority of organizations do not have protocols addressing every possible eventuality. While the minimum necessary standard should apply, covered entities should not end up "drowning in a sea of standard protocols."[23]

HHS could assist covered entities and business associates to better use their resources by adopting a clear operating definition of minimum necessary; promoting a criterion-based procedure for review of uses, disclosures, and requests where the standard applies; and requiring a robust process of oversight and accountability.

Recommendation 5: The Treatment Exception

The Committee recommends that HHS make no change to the current exception to the minimum necessary standard for treatment.

While the issue was raised in the hearing, we did not hear consensus, particularly because the technology is not available to support such a change.

Recommendation 6: Minimum Necessary and Administrative Functions

In developing new Minimum Necessary guidance, HHS should specifically address the application of the minimum necessary standard to HIPAA named transaction standards for

[23] *See*, Greene, Adam H., Testimony before the Subcommittee on Privacy, Confidentiality & Sec., Nat'l Comm. on Vital and Health Stat., "Minimum Necessary and the Health Insurance Portability and Accountability Act (HIPAA)" (June 26, 2016), at 4.

administrative functions pertaining to payment and operations. In particular, HHS's guidance should address the applicability of minimum necessary to new transactions such as those involving attachments, and data exchanges involved in fulfilling alternative payment models.

The minimum necessary standard applies to health care administrative transactions such as processing claims or determining eligibility. For each of these transactions (all associated with payment and operations functions), HHS has named an electronic standard that the industry must use. The electronic standard defines the data elements that a submitter of the transaction must send (or disclose) to the requester or recipient of that transaction in order to achieve the purpose of the disclosure. Where the transactions are repetitive, the submitter of the transaction can deem the set of data elements defined by the standard as the minimum necessary to be disclosed. (For example, in the case of a claim, the purpose is to process and receive payment for a service rendered, and there are a set of defined data elements.) For data elements that are considered "situational," the rules defined in the standard prescribe the situations and the data elements.

As noted by our panelists at the June hearing, the Attachment standard presents challenging minimum necessary situations. The Attachment transaction standard is used by health plans and providers to submit supplemental medical documentation in support of another transaction. For example, for certain health care claims, health plans require that providers submit additional supporting clinical documentation before they can be processed and paid. Health Level 7 (the national standards development body for the exchange, integration, sharing, and retrieval of electronic health information) finalized a national set of standards for attachments in 2016, but HHS has not yet adopted the standard in regulations.

In the meantime, current practices regarding the transmission of clinical data vary from limiting the amount of information submitted to that defined by the payer as minimally necessary, to, in some cases, sending more than the minimum necessary—perhaps the entire medical record—so that a health plan can select and use the part it needs in order to process the claim.

While the adoption of a national set of standards for Attachments will eliminate some of these practices, there will still be a need to ensure that the standard is implemented correctly, and that the parties involved—health plans and providers—understand the need to define and apply consistently minimum necessary requirements to requests for additional clinical documentation in an Attachment.

As the industry moves into the implementation of alternative payment models that rely less on claim-based transactions and more on clinical documentation, and that demonstrate achievement of defined service quality and outcome goals, the potential exchange of larger sets of more granular medical documentation will bring further challenges to ensuring that minimum necessary standards are met.

Recommendation 7: Framing the Minimum Necessary Standard

HHS should offer education that clearly illustrates how the minimum necessary standard interacts with other provisions of the HIPAA Privacy Rule to improve overall understanding. The Privacy Rule provides a four-tier framework of protections, which is subject to some misunderstanding among covered entities and the public. The Committee offers an analysis that explains these important interrelationships.

Appendix A describes the four distinct tiers of privacy protections that the Privacy Rule tailors to specific circumstances. Tier 1 reflects HIPAA's base-line protection: disclosing a person's PHI requires individual authorization, and the individual's expressed will, rather than the minimum necessary standard, governs the scope of disclosure**.**

In Tier 2, the Privacy Rule recognizes that certain discrete uses of data (listed in Appendix A, Table I) offer societal benefits so compelling as to justify the use or disclosure even without the individual's authorization. Here, the individual receives the protection of the minimum necessary standard, which allows disclosure *only* to the extent necessary to serve the beneficial use, and no more.

Tier 3 addresses certain disclosures required by law. Here, applying the minimum necessary standard could obstruct justice, so the Privacy Rule sets out alternative due-process standards to protect the individual.

Tier 4 outlines a very narrow set of circumstances (treatment and regulatory compliance) where covered entities may disclose data with neither authorization nor minimum necessary limitations.

The Committee is particularly concerned that some covered entities and, potentially, members of the public, remain confused about basic aspects of how the minimum necessary standard relates to the Privacy Rule's individual authorization requirement. Based on testimony, we understand that some covered entities may, at times, apply the minimum necessary standard to constrain disclosures of data even when the individual has previously authorized the disclosure.

The Privacy Rule offers, as its baseline protection, a requirement that individuals authorize disclosures of their data (Tier 1 in Appendix A). The minimum necessary standard comes into play only in certain situations where an individual authorization is *not* required (Tier 2 in Appendix A). Thus, it would not be appropriate for a covered entity to apply the minimum necessary standard when disclosing data pursuant to an individual authorization or when responding to individuals' data requests under the § 164.524 individual access right. In those instances, the Privacy Rule defers to the individual's expressed wishes about the scope of the allowed disclosure.

The Committee also heard some expressions of concern that individual authorizations, at times, may be subject to elements of coercion (for example, when an individual signs a pre-employment release form that is necessary to obtain a job). The committee understands that covered entities might look to the minimum necessary standard as a way to add an additional layer of protection when there are concerns about whether an individual's authorization was freely granted. However, the minimum necessary standard is not the proper pathway for addressing such concerns. Any ongoing concerns about coercion of individual authorizations should instead be addressed directly, by providing guidance on appropriate standards for obtaining authorizations to minimize the potential for coercion and to ensure that all authorizations are freely granted.

Recommendation 8: Public Comment on Draft Guidance

HHS should issue updated guidance in draft form and solicit public comment before issuing final guidance.

A public comment period will bring forth compliance issues that may not have been fully recognized or considered in preparing guidance. Covered entities and business associates who must comply with the minimum necessary standard are at very different starting points so public comment will also help to advance education, orientation and preparation for compliance.

Recommendation 9: Orientation and implementation guides

HHS should prepare orientation materials and implementation guides tailored to the perspectives of various stakeholders.

Multiple witnesses drove home the importance of education and training on use and disclosure generally and the minimum necessary standard specifically. It would be most helpful if orientation and guides could be tailored to the audience to raise awareness, understanding, and even skill, as needed. The staff responsible for day-to-day management of information use and disclosure need in depth training to apply the laws and regulations through sound policy, process, and technology. Clinicians and operations managers must understand the principles and policies that their organizations have adopted regarding access, use and disclosure of PHI, and senior leaders responsible for enterprise information governance and oversight must ensure that reasonable policies and practices are in place and are being followed. One size orientation and implementation guides are less useful than those tailored to a diversity of needs.

Recommendation 10: Broad Dissemination and Communication

In promulgating guidance, HHS should use a range of multimedia communication channels to disseminate published guidelines, "Frequently Asked Questions," web training, and case study illustrations tailored to the needs of various constituencies. Dissemination should include a public education component.

HHS has made great strides in stakeholder and public education regarding information rights and regulations. The Committee urges the Department to fully use these capabilities in communicating draft and final version of updated minimum necessary guidance and its application. In addition to covered entities and business associates, the communication plan should include law enforcement, national security, public health, research, and fundraising stakeholders to advance understanding and know-how in applying the minimum necessary standard. Upon release of guidance, HHS should use public service communications channels to incorporate information about the minimum necessary standard into consumer guidance related to information rights.

The Department has just recognized the 20-year anniversary of the HIPAA law and its privacy provisions have provided the essential foundation for the rapid advancements to an information-driven health system. The minimum necessary standard is in turn an essential element of the Privacy Rule. The NCVHS looks forward to discussing the recommendations and perspectives laid out in this letter with you and HHS staff members, and to working with the Department to shape future guidance and priorities for advancing this work.

Sincerely,
/s/
William W. Stead, M.D., Chair,
National Committee on Vital and Health Statistics

Cc: HHS Data Council Co-Chairs

Appendix A: The Privacy Rule's Four Tiers of Protection

The minimum necessary standard interacts with other provisions of the HIPAA Privacy Rule to provide four distinct tiers of protection tailored to specific circumstances. These tiers are summarized in Table 1 and discussed below.

Tier 1: HIPAA's base-line privacy protection respects individual autonomy by requiring a valid individual authorization[24] or request for individual access[25] prior to use or disclosure of data. When an individual has authorized a disclosure, the Privacy Rule allows the individual's expressed will, rather than the minimum necessary standard, to govern the scope of disclosures.

The Privacy Rule's default stance is to let the individual who is the primary subject of the protected health information, rather than a covered entity, define the scope of information that a covered entity can use or disclose. For this reason, the minimum necessary standard does not apply to disclosures made pursuant to an individual authorization for disclosure to a third party under § 164.508 or when individuals request disclosure of information to themselves under the §164.524 individual access right.[26]

Table 1: Tiers of Privacy Protection Provided Through Interplay of the Privacy Rule's Authorization Requirements and Minimum Necessary Standard

Tier of Privacy Protection	Circumstances falling within each Tier	Is individual authorization required?	Does the minimum necessary standard apply?
Tier 1 Disclosures directed by the individual require individual permission but are not subject to the minimum necessary standard	Valid authorization under § 164.508[27] Request for individual access under § 164.524	Yes Individuals request disclosure, rather than authorize it	No, the individual's expressed will, rather than the minimum necessary standard, determines the scope of the allowed disclosure. No, scope of disclosure is determined by HIPAA's definition and guidance on the content of the designated record set.

[24] *See* 45 C.F.R. § 164.508.
[25] *See* 45 C.F.R. § 164.524
[26] *See* 45 C.F.R. § 164.502(b)(2)(ii)-(iii).
[27] All section references in the table are to volume 45 of the Code of Federal Regulations.

Tier 2 Disclosures without individual authorization, but subject to the minimum necessary standard	Disclosures for payment and health care operations under § 164.506	No	Yes
	Disclosures for 9 of the 12 authorization exceptions in § 164.512:		
	▪ disclosures required by laws, when disclosures are limited to those required by the law under § 164.512(a)(1)	No	Yes, but § 164.512(a)(1) looks to the external laws to define the scope of disclosure needed in order to comply with them.
	▪ public health activities § 164.512(b)	No	Yes
	▪ health oversight activities § 164.512(d)	No	Yes
	▪ decedents § 164.512(g):	No	Yes
	▪ cadaveric organ, eye, tissue § 164.512(h) donation	No	Yes
	▪ § 164.512(i): research pursuant to waiver	No	Yes
	▪ § 164.512(j): to avert serious threat to health or safety	No	Yes, but the scope of minimally necessary disclosure presumably would be viewed in light of the emergent threat.
	▪ § 164.512(k): specialized governmental functions (military, national security, secret service, etc.)	No	Yes, but § 164.512(k) defers to military command authorities that publish notices in the *Federal Register* defining the scope of information necessary to their mission.
	▪ § 164.512(l): workers' compensation	No	Yes

Tier 3 Disclosures required by law that do not follow the minimum necessary standard, but alternative standards apply	▪ Section 164.512(a)(2) lists three types of disclosures required by law for which HIPAA sets out special requirements in lieu of the minimum necessary standard: ▪ disclosures about victims of abuse, neglect, or domestic violence § 164.512(c) ▪ disclosures for judicial and administrative proceedings § 164.512(e) ▪ disclosures for law enforcement purposes § 164.512(f)	 No No No	 No, § 164.512(c) sets out alternative requirements that substitute for the minimum necessary standard. No, § 164.512(e) sets out alternative requirements that substitute for the minimum necessary standard. No, § 164.512(f) sets out alternative standards that substitute for the minimum necessary standard.
Tier 4 No authorization or minimum necessary requirement.	▪ disclosures for treatment § 164.502(b)(2)(i) ▪ certain disclosures to Secretary of HHS § 164.502(b)(2)(iv) ▪ uses and disclosures by covered entities for their own HIPAA compliance § 164.502(b)(2)(vi)	No No No	No No No

The Privacy Rule states that covered entities should honor individuals' instructions about the use and disclosure of their data as reflected in a valid authorization: "When a covered entity obtains a valid authorization for its use or disclosure of protected health information, such use or disclosures must be *consistent with* such authorization."[28] The term "consistent with" implies that covered entities should not share *more* data than the individual has authorized, but neither

[28] *See* 45 C.F.R. § 164.508(a)(1) (emphasis added).

should they share *less* than the individual authorized. In HIPAA's base-line scheme of privacy protection, the individual manages his or her own information, and the minimum necessary standard is irrelevant if individuals have authorized disclosure or requested access to their own information.

When individuals request access to their own data, as permitted by § 164.524, the scope of the required response is determined by HIPAA's definition of the accessible designated record set and associated guidance interpreting that definition. The minimum necessary standard has no relevance.

Tier 2: Socially beneficial data uses that do not require individual authorization but must comply with the minimum necessary standard.

The Privacy Rule recognizes a number of discrete situations in which public interests in data sharing may outweigh the individual's interest in blocking data flows. The Privacy Rule allows data to be used and disclosed without individual authorization for treatment, payment, and health care operations[29] and to serve twelve categories of public interest listed in § 164.512. These public interest exceptions to authorization include, for example, disclosures of data to public health authorities, disclosures of data for research pursuant to a waiver approved by an Institutional Review Board or Privacy Board (see others listed in Table 1).

When data can be used and disclosed without individual authorization, the Privacy Rule generally protects individuals by applying the minimum necessary standard. Note, however, that this is not always true. Nine of the twelve public-interest-oriented authorization exceptions are subject to the minimum necessary standard,[30] but the other three (relating to disclosures required by law) are exempt from the minimum necessary standard.[31] They instead apply substitute standards discussed in point 3 below. Uses and disclosures for payment and health care operations listed in §164.506 are subject to the minimum necessary standard, but treatment is excepted from this requirement[32] as are disclosures related to HIPAA compliance and certain disclosures to the Secretary of HHS.[33] In these cases, no substitute standard applies as discussed in point 4 below.

Tier 3: The special case of disclosures required by law: not subject to individual authorization requirements or the minimum necessary standard, but subject to alternative protections.

The Privacy Rule recognizes that covered entities could be liable to charges of obstructing justice if they applied the minimum necessary standard to interpret data disclosures mandated by legislatures, courts, and law enforcement agencies. Therefore, uses and disclosures required by law are excepted from the usual minimum necessary standard.[34] Instead, the individual authorization exceptions in §164.512 contain specific limitations and procedural protections that

[29] 45 C.F.R. § 164.506(c).
[30] These nine are listed in 45 C.F.R. § 164.512.
[31] *See* 45 C.F.R. § 164.502(b)(2)(v).
[32] *See* 45 C.F.R. § 164.502(b)(2)(ii).
[33] *See* 45 C.F.R. § 164.502(b)(2)(iv), (vi)) (see discussion of Tier 4 below).
[34] *See* 45 C.F.R. § 164.502(b)(2)(v).

apply when covered entities must comply with laws requiring reporting of data about victims of abuse, neglect, or domestic violence;[35] or disclose data for judicial or administrative proceedings;[36] or respond to law enforcement requests.[37] Such disclosures do not require individual authorization and are not subject to the minimum necessary standard, but the Privacy Rule ensures that they observe due process and are specific and limited in scope.

Tier 4: Uses and disclosures that neither require individual authorization nor are subject to the minimum necessary standard.

In very narrow circumstances, the Privacy Rule allows covered entities to disclose data with no individual authorization and no minimum necessary or other standard to limit the scope of disclosures. These circumstances are: disclosures for treatment, uses and disclosures for HIPAA compliance, and certain disclosures to the Secretary of HHS.[38] In these situations, burdening individual privacy by allowing these data flows serves other interests that are deemed to benefit the individual.

The treatment exception[39] advances individuals' interest in receiving optimal health care that is well informed by unrestricted flows of data to treating providers.[40] The exceptions for HIPAA compliance activities[41] and for HHS oversight[42] both promote the individual's own privacy interests by helping to ensure a strong, well-enforced HIPAA regulation. These minimum necessary exceptions reflect trade-offs among competing *individual* interests (as opposed to trade-offs between individual and societal interests). Their ethical justification is that they place a burden on individual privacy in order to facilitate flows of data that ultimately may benefit the individuals.

[35] *See* 45 C.F.R. § 164.512(c).
[36] *See* 45 C.F.R. § 164.512(e).
[37] *See* 45 C.F.R. § 164.512(f)).
[38] *See* 45 C.F.R. §§ 164.502(b)(2)(i), (iv), (vi).
[39] *See* 45 C.F.R. § 164.502(b)(2)(i).
[40] Security best practices call for reasonable access controls and audit mechanisms to ensure that even in this context, information is accessible to those who need it to do their jobs. Role-based access controls should still be in place, so there is not really a "free flow" of information.
[41] *See* 45 C.F.R. § 164.502(b)(2)(vi).
[42] *See* 45 C.F.R. § 164.502(b)(2)(iv).

Appendix B: Other Issues Beyond the Scope of this Letter

The Committee also offers perspective on important issues that interact with and were discussed as part of this phase of work on the minimum necessary standard. However, they were beyond the scope of the June hearing. The Committee identifies these as potential future issues. As part of its planning the Committee will consider how it might be of assistance to the Department.

Technology Developments to Support Minimum Necessary

The capabilities of information technologies that will better support minimum necessary are evolving and maturing. For example technology to manage disclosure of information, improve role-based and attribute-based uses, segmenting sensitive health information with standardized computational tools, and even codifying and executing electronically patient privacy preference are improving.

According to testimony provided during the hearing, many health care organizations do not utilize a comprehensive technology solution to address their implementation of minimum necessary.[43] Most methods and approaches used for complying with the minimum necessary standard rely on manually executed policies and procedures. This is due in part to the fact that minimum necessary is significantly contextual, and in many ways depends on case-by-case analysis and interpretation of what data might be minimally needed to support the purpose for which the data are being requested, used, or disclosed.

In the case of routine disclosures, such as external periodic reporting of vital statistics or reportable conditions to public health agencies or submission of claims, the HIPAA covered entity disclosing this data, in these cases a provider, is permitted by the current Rule to rely on the requester of the data to determine what is minimally needed, establish its internal procedures to generate this data, and repeat the process without stopping each time the data is requested to define minimum necessary.

Evolving health information technology functionalities have the potential to improve implementation of the minimum necessary standard, particularly as more information is electronically exchanged. However, these technologies must be capable of at least computer assisted analysis of contextual elements (i.e., what data, for what purpose) of a data request, and electronically make a determination as to whether it fulfills the minimum necessary requirements, a capability that testimony confirmed is not currently well developed.

---

[43] *See Statement of the Electronic Health Record Association filed with the Subcommittee on Privacy, Confidentiality & Sec., NCVHS, Minimum Necessary and the Health Insurance Portability and Accountability Act (HIPAA)* (July 6, 2016), at 1-2; *see also* Rita K. Bowen, *Testimony and Statement on behalf of the Association of Health Information Outsourcing Services (AHIOS) (June 16, 2016)*, at 2-3, *both statements available at* http://www.ncvhs.hhs.gov/meeting-calendar/agenda-of-the-june-16-2016-ncvhs-subcommittee-on-privacy-confidentiality-security-hearing/.

.

The Minimum Necessary Standard in an Evolving Data Environment

The minimum necessary standard has enduring relevance but, in the future, it will be applied in a 21st-century data environment that differs in important respects from that of the past. The sharp line that once existed between "treatment" and "research" grows blurrier in view of initiatives like the Learning Healthcare System,[44] the President's Precision Medicine Initiative,[45] and the Vice President's Cancer Moonshot.[46] Common to these projects is a vision of harnessing data from routine treatment encounters to drive a process of continuous learning (i.e., research) to inform future health care and public health. The minimum necessary standard, which currently attaches to research uses of data but not to treatment uses of data, may grow difficult to administer in a Learning Heath Care System context where data flow seamlessly from "treatment" to "research" and back to "treatment."

At present, the data infrastructure to support a learning health care system is still under development, and this Committee does not believe the time is ripe to alter the minimum necessary provision's current distinction between "treatment" and "research." At this time, research uses continue to be recognizably distinct from treatment uses. NCVHS recommends that this issue be periodically revisited at two to three year intervals as interoperable data systems continue to develop in support of continuous learning.

Another feature of the 21st-century data environment is the growing capacity to extract useful insights (for treatment, research, and public health applications) by marshaling very large, detailed data resources that juxtapose individual's longitudinal health histories with other sources of data characterizing their biology, behaviors, exposures, outcomes, and subjective patient experiences. The minimum necessary standard is rooted in a 20th-century concept of hypothesis-testing studies, where investigators know in advance precisely what they are looking for and can specify the data that would be "necessary" to test the hypothesis.

---

[44] *See* INST. OF MED., NAT'L ACAD. OF SCI., BEST CARE AT LOWER COST: THE PATH TO CONTINUOUSLY LEARNING HEALTH CARE IN AMERICA (2012), *available at* http://www.nationalacademies.org/hmd/Reports/2012/Best-Care-at-Lower-Cost-The-Path-to-Continuously-Learning-Health-Care-in-America.aspx.

[45] In his 2015 State of the Union address, President Barack Obama announced a Precision Medicine Initiative (PMI), which launched with a $215 million investment in his 2016 budget. Precision medicine is an innovative approach to disease prevention and treatment that takes into account individual differences in people's genes, environments, and lifestyles. It gives clinicians tools to better understand the complex mechanisms underlying a patient's health, disease, or condition, and to better predict which treatments will be most effective. The PMI is headed by the Office of Science and Technology Policy in the White House with participation by the Departments of Health and Human Services, Defense, and Veterans Affairs. *See* OFFICE OF MANAGEMENT AND BUDGET, FISCAL YEAR 2016 BUDGET OF THE UNITED STATES 19 (2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/budget.pdf.

[46] During his State of the Union address on January 12, 2016, President Barack Obama called on Vice President Biden to lead a new national "Moonshot," to accelerate cancer research. The President established a Cancer Moonshot Task Force with its mission and functions. *See* Memorandum to Heads of Executive Departments and Agencies, "White House Cancer Moonshot Task Force," (Jan 28, 2016). The initiative aims to make more therapies available to more patients, while also improving our ability to prevent cancer and detect it at an early stage. On February 1, 2016, the White House announced a new $1 billion initiative to jumpstart this work. *See also* NATIONAL CANCER INSTITUTE, BLUE RIBBON PANEL REPORT: CANCER MOONSHOT (Sept. 7, 2016), *available at* https://www.cancer.gov/research/key-initiatives/moonshot-cancer-initiative/blue-ribbon-panel.

In contrast, many 21st-century research and public health questions lend themselves to hypothesis-free analysis: for example, sifting through large datasets to look for correlations between genotype and phenotypes to discover the clinical significance of a novel genetic variant, or searching through insurance records for signals of adverse events in patients who consumed particular drugs. For these analytical methods, the "minimum necessary" data to support discovery may be "as much data as can be obtained."

The Privacy Rule has always allowed for the possibility that, for some uses, a patient's entire medical record may be the minimum amount of data that is "necessary to accomplish the purpose of the use, disclosure, or request" (§ 164.514(d)(5)). The Privacy Rule states that when this is true, the need for the entire medical record must be "specifically justified." (id.) As advanced "big data" analytic techniques grow more common in coming years, covered entities may face a greater number of requests for patients' entire medical records.

Minimum Necessary and Cybersecurity

Strengthening the security, resiliency, and risk management of cyberspace in an ever-growing digital community is now a critical component of every industry, including health care. One of the main strategies has been to establish mechanisms and structures for trusted information sharing and analysis of cyber threats. The National Health Information Sharing and Analysis Center (NH-ISAC) is promoting information sharing among health care organizations. Such efforts seek to protect valuable PHI and comply with HIPAA regulations and standards.

While in most cases the type of cyber threat information shared by health care organizations is in aggregate, de-identified form, one of the concerns raised during the hearing was the possibility of having to release certain data about a cyber threat that might include information that could lead to the identification of an individual. In this context, exploring the applicability of Minimum Necessary to the sharing of cyber threat information would be an important area for HHS guidance.

Minimum Necessary and Genetic Information

The HITECH Act called for 2013 amendments to clarify that genetic information is health information for purposes of the HIPAA Privacy Rule. Thus, genetic information is subject to the minimum necessary standard on the same basis as other health information. However, genomic science is in an early and evolving stage that makes it difficult to assess which, and how much, genetic information will be necessary for specific tasks, such as conducting research into the clinical significance of specific genetic variants.

When the HIPAA Privacy Rule was drafted—in the late 1990s and early 2000s—"genetic information" was widely conceived in terms of simple, Mendelian inheritance: it was thought that specific gene variants would be associated with specific physical characteristics, so that particular data uses (for example, studying the cause of a patient's tremor) would only require use of a discrete, limited set of genetic variants known to be associated with that type of tremor.

As FDA noted in 2014, Next Generation Sequencing (NGS) technology is revolutionizing the current view of how inheritance works by making it possible to study large segments of an

individual's DNA or an individual's entire genome.[47] NGS is revealing that many traits of interest for treatment, public health, and research purposes—such as a person's susceptibility to chronic diseases—depend on very large constellations of genetic variants that may be scattered widely throughout the human genome. It is difficult to say which genetic variants are the "minimum necessary" to diagnose or study a disease, when new associations between genes and diseases are being discovered almost weekly.

Moreover, emerging evidence suggests that even when patients have genetic variants known to be associated with a disease, they may nevertheless remain healthy because of other variants that confer resistance.[48] Attempts to limit disclosure to known disease-associated variants could harm patients by failing to capture other, seemingly unrelated variants that affect disease manifestation.

A more practical concern is that genomic testing laboratories store information from an individual's NGS testing in large, standard file types and it could be burdensome to task laboratories with extracting specific genomic variants from these files, even if the current state of genomic science could identify which variants are the "minimum necessary" for a particular use.

[47] U.S. Department of Health & Human Services, Food & Drug Admin. *Optimizing FDA's Regulatory Oversight of Next Generation Sequencing Diagnostic Tests—Preliminary Discussion Paper* (Dec. 29, 2014), at: http://www.fda.gov/downloads/medicaldevices/newsevents/workshopsconferences/ucm427869.pdf).

[48] *See* Rong Chen et al, *Analysis of 589,306 Genomes Identifies Individuals Resilient to Severe Mendelian Childhood Diseases*, 34 NATURE BIOTECHNOLOGY 531 (2016).