

**Testimony of the**

**American Health Information Management Association**

**to the**

**NCVHS Privacy, Confidentiality, and Security Subcommittee**

**on**

**HIPAA and Minimum Necessary**

**June 16, 2016**

**Melissa M. Martin, RHIA, CCS, CHTS-IM**  
**Board President, American Health Information Management**  
**Association**

[Presentation slides available [here](#)]

Chairwoman Kloss and members of the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality, and Security and staff, thank you for the invitation and opportunity to testify before you today on the minimum necessary requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the guidance needed to help ensure compliance is met.

AHIMA is a nonprofit association of over 103,000 health information management (HIM) professionals. These professionals work in a variety of sites that collect, store, analyze, use, and disclose protected health information (PHI). HIM professionals have been the stewards of health information confidentiality for decades, and with the advent of the HIPAA privacy and security requirements, many serve as privacy or security officers for HIPAA covered entities as well as release of information (ROI) officers and specialists. Many also work as, or for, business associates handling PHI on behalf of a covered entity. AHIMA has supported these efforts over the years and provides members, educators, the healthcare industry, and consumers with a variety of related best practices as well as other healthcare confidentiality, privacy, and security information and products. AHIMA also addresses privacy on its [myPHR.com](http://myPHR.com) website. AHIMA and its member professionals also participate in a variety of privacy-related projects, education, and advocacy at the federal and state levels. With this background and interest, we are pleased to see efforts by NCVHS to provide recommendations to the HHS Office for Civil Rights on the minimum necessary requirements under HIPAA.

To frame this testimony AHIMA solicited comments from privacy and security professionals about the issues and challenges they face in achieving compliance in today's healthcare environment regarding minimum necessary practices. These professionals include members of AHIMA's Privacy and Security Practice Council and its general membership.

### **Regulatory Requirements**

The minimum necessary standard in HIPAA's Privacy Rule requires covered entities to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.<sup>1</sup> The Privacy Rule requires that the covered entity identify persons or classes of persons in its workforce who need access to PHI and the category or categories of PHI to which access is needed and any conditions appropriate to such access.<sup>2</sup> This constitutes the requirements for ensuring minimum necessary use. For routine and recurring disclosures, the rule requires the covered entity to implement standard protocols that limit the disclosures to the amount reasonably necessary to achieve the purpose of the disclosures.<sup>3</sup> For all other disclosures, the covered entity must develop criteria designed to limit the PHI disclosed to the minimum necessary.<sup>4</sup> Covered entities must also limit any request they make for PHI to that which is reasonably necessary.<sup>5</sup>

---

<sup>1</sup> Amatayakul, Margret; Brandt, Mary D.; and Dennis, Jill Callahan. "Implementing the Minimum Necessary Standard (AHIMA Practice Brief)." *Journal of AHIMA* 73, no.9 (2002): 96A-F.

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

<sup>4</sup> Ibid.

<sup>5</sup> Ibid.

## Compliance Confusion and Challenges

It has been over a decade since enactment of the minimum necessary standard, and confusion around compliance still exists throughout the industry. AHIMA's findings and subsequent recommendations have been broken down into detail below.

### Defining Minimum Necessary

The consensus on the definition of minimum necessary is that it varies by organization. This makes implementing and meeting compliance with minimum necessary challenging and can result in the unnecessary release of PHI.

Since it is up to the covered entity rather than the patient to determine what "minimum necessary" means, this exposes an interpretation loophole which may lead to confusion and potential litigation should a patient and/or their legal representative disagree with what the covered entity defines as "minimum necessary." A business associate might also disagree with a covered entity's definition versus its own. Furthermore, there is confusion over whether business associates are required to follow each covered entity's definition of minimum necessary or have the ability to define it themselves. Generally, when PHI is requested by another covered entity, what is requested will depend on what the requestor has defined as minimum necessary. However, this information might differ from how the covered entity releasing the PHI defines it. In some cases, the covered entity seeking the PHI will request the entire record even though it is not needed. Release for treatment is listed as an exception to the rule. For example, a covered entity may request a specific report but receive the entire chart. Consequently, guidance is needed to standardize the definition of minimum necessary to minimize confusion and improve compliance.

### Technology Challenges

Since the minimum necessary standard was implemented, the use of technology has advanced tenfold. The adoption of innovative technologies has changed the way information is protected and managed in healthcare and will continue to do so well into the future. However, as technology continues to advance, so too will the technological challenges associated with complying with the minimum necessary standard.

Challenges that center on technology and that are faced routinely by HIM professionals include:

- Controls within electronic health record (EHR) systems that limit access to specific information. Most systems lack the sophistication to sequester patients by assigned employees (e.g., location, diagnosis, sensitive status). This often leads to approval for "any and all" access rather than imposing certain access restrictions on the PHI.

Sub-applications within EHR applications also do not necessarily allow for restrictions based on specific fields. For example, patient registration and billing information may not only allow access to demographics, but also reveal PHI including Social Security number(s), date(s) of birth, and other sensitive information.

- Stakeholders are increasingly focused on the data or health information itself. Consequently, this raises other issues including the ability to sequester data or parts of the record, the use of standardized metadata to allow for sequestering, the ability to allow for disclosure of de-identified information for purposes of research and improvement, as well as the ability of patients, consumers, caregivers, and patient representatives to access their information. Unfortunately, many EHR systems lack the functionality to perform such queries.

### Regulatory Challenges

Compounding the technology challenges associated with limiting access to specific data elements are the increasing numbers of regulations and legislative mandates that require the improvement of data access and sharing of PHI. This includes initiatives such as improving interoperability, advancing access and use of clinical research data under the Precision Medicine Initiative, as well as the Qualified Entity Program under Medicare. AHIMA has long advocated for the need to improve and enhance the flow of data throughout the healthcare system. However, as the paradigm has shifted to enhancing data sharing and improving data accessibility, the amount of PHI necessary to meet the minimum necessary standard has expanded exponentially, so that the concept is associated with fewer transactions.

### **Survey Findings**

In preparation for this testimony, AHIMA surveyed members who work in the areas of data analytics, clinical documentation improvement, education, and/or privacy and security. The survey included specific questions related to the policy and management of the minimum necessary standard as defined under HIPAA. Survey questions and findings can be found in Appendix A.

The findings from the survey revealed the majority of respondents (38 percent) did not know if they had adopted a definition for minimum necessary, while 27 percent of respondents affirmed that they had an adopted definition. Fourteen percent of respondents reported that they did not have a definition, while 21 percent of respondents reported that they are currently working on adopting a definition. Approximately half of the respondents reported having policies and procedures related to the minimum necessary standard, while one-third of respondents indicated they did not have any policies or procedures. In instances where the release of information (ROI) function is outsourced, almost half of all respondents did not know the criteria their ROI contractor used for determining minimum necessary.

Graphs of the survey findings can be found in Appendix A.

### **Complying with Minimum Necessary at West Virginia University Medicine**

At West Virginia University (WVU) Medicine, we have a policy regarding the disclosure of PHI in accordance with the minimum necessary standard. We take reasonable steps to limit both routine and non-routine uses, disclosures, and requests for PHI to accomplish the intended purpose of the use, disclosure, or request. In limited circumstances, we rely on the judgment of the party requesting the disclosure that the PHI requested is the minimum amount needed.

Daily operations are complicated due to the lack of clarity around the minimum necessary standard, as the volume of requests for PHI through release of information continues to grow. WVU Medicine processes over 85,000 requests for information annually. With each request, we must assure that only the minimum necessary is provided. The output could be anywhere from a few pages to thousands of pages. More importantly, each must be scrutinized to determine whether we have provided the minimum necessary based on the requestor's justification. This process is enhanced with the use of technology WVU Medicine has available within our EHR to help assure that we do not release sensitive information or more than the minimum necessary. There are also many challenges within our state regarding fees, as well as the time spent processing and fulfilling requests. Overall operations could be improved with clear guidance on the definition and standardization of meeting minimum necessary compliance.

## Recommendations

Given the challenges associated with the minimum necessary standard that have been identified by AHIMA and its members in this testimony, AHIMA makes the following recommendations:

- **A clear definition of minimum necessary must be developed in future guidance. This includes the development of clear, objective criteria that would enable stakeholders to meet the minimum necessary standard. An updated definition of minimum necessary could also include differing levels of minimum necessary that are dependent on specific identifiers. For example, the minimum necessary standard for research might include only gender and age versus location or name.**
- **Given the intensive industry focus on sharing and improving the access of data and health information, the role of metadata in the minimum necessary standard must be taken into account in any future guidance.**
- **Technology capabilities and limitations associated with achieving the minimum necessary standard must be acknowledged and addressed in any future guidance.**
- **Enhance focus on the patient's needs and the role of the steward in the development of future guidance. For example, the existing regulation that allows a patient to limit certain information from disclosure to their respective third-party payer.**
- **Improve standardization in the implementation of the minimum necessary standard so patients have a clear expectation from all data holders that PHI will not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a related function.**
- **Provide educational resources and materials with the accompanying guidance. This could include topical frequently asked questions and fact sheets to educate health professionals about changes to the minimum necessary guidance. Such materials should also include consumer-friendly resources to help consumers understand the minimum necessary standard.**

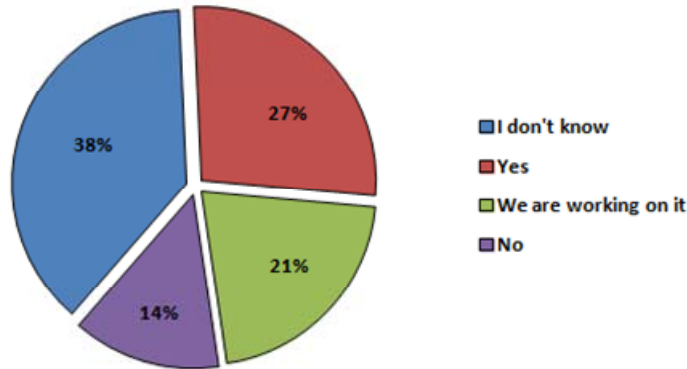
Chairwoman Kloss and members of the subcommittee, thank you for the opportunity to provide these comments. AHIMA looks forward to working with you on this important issue, and I am happy to answer any questions that the committee may have today or in the future.

## Appendix A

### AHIMA Minimum Necessary Survey Results

#### Service Line Survey

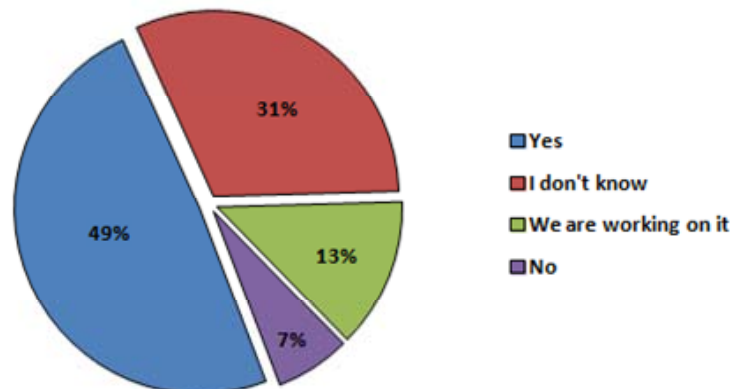
- For those participants with CDI, Data Analytics, Education, IG and/or Privacy/Security as part of their current role (N=306), most did not know if their organization has adopted a definition of 'minimum necessary.'



**Q: Has your organization adopted a definition of 'minimum necessary' relating to access and disclosure? [If current role includes CDI, Data Analytics, Education, IG, or P&S]**

#### Service Line Survey

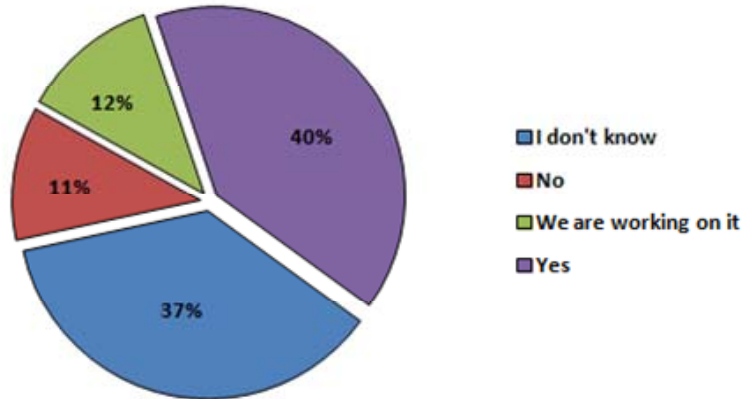
- For those participants with CDI, Data Analytics, Education, IG and/or Privacy/Security as part of their current role (N=306), almost half indicated their organization has written policies related to 'minimum necessary' principles.



**Q: Has your organization adopted written policies and procedures for access and disclosure that reflect principles of 'minimum necessary?' [If current role includes CDI, Data Analytics, Education, IG, or P&S]**

## Service Line Survey

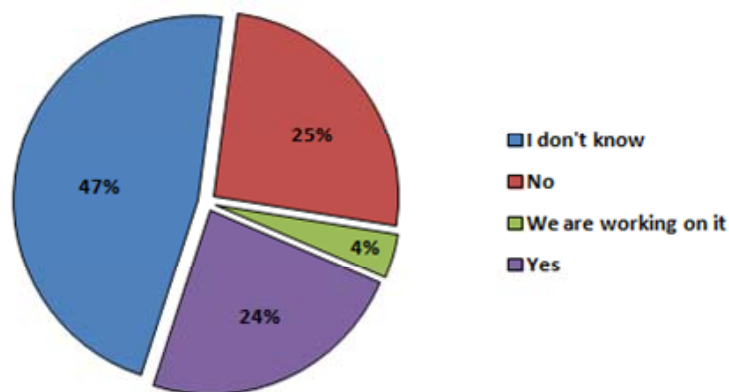
- For those participants with CDI, Data Analytics, Education, IG and/or Privacy/Security as part of their current role (N=306), 123 indicated their organization has a process for reviewing a request for information that exceeds the limit of what is minimally necessary.



**Q: Does your organization have a process for reviewing a request for information that appears to exceed the limits of what is 'minimally necessary?' [If current role includes CDI, Data Analytics, Education, IG, or P&S]**

## Service Line Survey

- For those participants with CDI, Data Analytics, Education, IG and/or Privacy/Security as part of their current role (N=306), most did not know the criteria their organization uses for determining minimum necessary when outsourcing release of information.



**Q: If your organization outsources release of information, do you know the criteria that your contractor uses for determining 'minimum necessary?' [If current role includes CDI, Data Analytics, Education, IG, or P&S]**