FACT SHEET

THE HIPAA MINIMUM NECESSARY RULE IN THE AGE OF DATA MODERNIZATION

INTRODUCTION

Twenty-five years after the finalization of the Privacy Rule, the public health landscape—particularly with respect to information technology and the way information is submitted to public health—has changed considerably. Electronic case reporting (ECR), electronic lab reporting (ELR), local disease surveillance systems, and other data technology like these promote timely and complete public health data reporting and interoperability. They also reduce burdens on data reporters and the public health departments receiving the data. For some public health professionals, the advent of automated reporting directly from electronic health records (EHRs) has brought to the surface questions about the Health Insurance Portability and Accountability Act's (HIPAA's) requirement to limit many uses and disclosures of, and requests for, protected health information (PHI) to the minimum necessary. This fact sheet takes a fresh look at an old rule and explores how a requirement that predates Y2K applies to public health reporting in the era of data modernization.

HOW DID WE GET HERE?

Most health care providers and many public health departments are HIPAA covered entities. This means that these entities must comply with HIPAA Administrative Simplification Rules, including the HIPAA Privacy Rule. Data submission to public health, such as through case reports or laboratory reports, involves HIPAA covered entities and, in many cases, business associates (collectively "regulated entities") using and disclosing PHI, and these regulated entities must comply with the HIPAA Privacy Rule requirements. This, however, is not new. The permissibility of these disclosures by regulated entities without an authorization is clear under the HIPAA Privacy Rule at 45 C.F.R. § 164.512, which permits these disclosures when it is required by law, and to public health authorities, for example.

The legal authority of state and local public health departments to collect this information, and for providers, labs and others to report it, is also long-established. Health care providers, labs, and other entities are required under state law to report cases of certain diseases and conditions, in addition to vaccine, lead, HIV, STI, and other data, to appropriate public health authorities.

What has changed, however, is the technology landscape. The use of intermediaries to facilitate the exchange of electronic data has become commonplace. The Trusted Exchange Framework and Common Agreement (TEFCA), for example, promotes interoperability and real time sharing of data across a seamless national network of health information networks (HINs). TEFCA may currently be used for exchange of data for treatment, payment, health care operations, public health, government benefits determination, and individual access services. Electronic case reporting transmits case data directly from EHRs to public health authorities, and ELR transmits data from labs to health care providers and public health authorities.

Regional and local health information exchanges (HIEs) around the country also facilitate the real time exchange of data. A regulated entity's ability to facilitate public health reporting through intermediaries, such as HIEs, or HINs, with the use of valid business associate agreements, is unambiguous.

The real time exchange of large volumes of health data across such platforms and informatics solutions can, however, create minimum necessary headaches for some public health practitioners and exchange partners who grapple with exactly how to fully comply with HIPAA's minimum necessary requirements in such an automated environment.

EXPLAINING THE MINIMUM NECESSARY

HIPAA's minimum necessary rule is laid out at 45 C.F.R. §§ 164.502 and 164.514. It requires that, when using, disclosing, or requesting PHI, regulated entities must make reasonable efforts to use, disclose, or request only the minimum amount of PHI necessary to accomplish the intended purpose. However, this requirement does not apply to:

(i) disclosures to or requests by a health care provider for treatment;
(ii) uses or disclosures made to the individual;
(iii) uses or disclosures to third parties made pursuant to an authorization;
(iv) disclosures made to the Department of Health and Human Services for oversight purposes;
(v) uses or disclosures that are required by law; and
(vi) uses or disclosures that are required for HIPAA compliance.

Regulated entities must identify those persons who are authorized to access PHI and identify appropriate conditions to limit access by these individuals. Regulated entities requesting PHI from another regulated entity must also limit such requests to the minimum data reasonably necessary to accomplish the stated purpose.

For routine requests and disclosures of PHI, the Privacy Rule requires regulated entities to implement policies and procedures or standard protocols that limit PHI to the minimum necessary. For non-routine requests and disclosures, regulated entities must identify criteria intended to limit requests and disclosures of PHI to the information reasonably necessary to accomplish the purpose for which the information is requested or disclosed and evaluate any non-routine request for disclosures of PHI using these criteria.

A regulated entity may reasonably rely on the representations of a public health official, or other public official, that certain requested PHI is the minimum necessary. This reliance is allowable if the request is permitted under one of HIPAA's permitted uses and disclosures for which a patient's authorization is not required in 45 C.F.R. § 164.512. Among other things, that section permits a regulated entity to disclose PHI to a public health authority, authorized by law to receive the information, for public health activities. Regulated entities may similarly rely on such representations as to minimum necessary from other HIPAA regulated entities if the reliance is reasonable under the circumstances.

A use, disclosure or request involving an entire medical record may meet the minimum necessary requirement when the entire record is "specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request."

EVOLUTION OF THE MINIMUM NECESSARY RULE

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. § 17935, expanded on minimum necessary, by expressing a preference for covered entities to use and disclose only limited data sets, where practical, "*or, if needed by such entity, to the minimum necessary* to accomplish the intended purpose for such use, disclosure, or request…." HIPAA's Privacy Rule limits use and disclosure of limited data sets to research, public health, and health care operations.

The HITECH Act also clarified that it is the responsibility of the covered entity or business associate disclosing the PHI to determine the minimum necessary. This would appear to be a break from the permitted reliance on the representations of a public official as to what is the minimum necessary when the official is requesting PHI. The Department of Health and Human Services (HHS), however, did not scrub that provision from the Privacy Rule in its 2013 Omnibus rulemaking following the HITECH Act. The Privacy Rule at 45 C.F.R. § 164.514(d)(3)(iii) still permits covered entities to rely on the representations of a public official as to what constitutes the minimum necessary to accomplish the stated purpose.

HITECH also required business associates to comply with the Privacy Rule's requirements, including the minimum necessary rule.

REASONAABLENESS, NOT ABSOLUTE MINIMUS

The minimum necessary rule applies a reasonableness standard; that is, it requires regulated entities to make *reasonable efforts* to limit uses, disclosures, and requests relating to PHI to that which is the minimum necessary to achieve the stated purpose of the use, disclosure, or request. As such, HHS has said that the minimum necessary rule is flexible.

According to HHS, the minimum necessary rule "is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information." In the same guidance, HHS further states covered entities are granted flexibility to make their own assessment of circumstances and which PHI is reasonably necessary "given the characteristics of their business and workforce." The emphasis on reasonableness, and not on absolute minimums, is well-taken. Determining minimum necessary in an automated environment can be difficult. A focus on reasonableness under the circumstances makes compliance more achievable.

Where some have seen flexibility with the minimum necessary rule, others have seen a need for additional guidance from HHS to assist covered entities and business associates in determining minimum necessary.

HEALTH INFORMATION ORGANIZATONS AND MINIMUM NECESSARY

HHS does not appear to have provided guidance on minimum necessary in the ELR, ECR, or similar data modernization contexts. However, it has provided guidance on minimum necessary on the topic of exchange of electronic PHI generally, including through the use of a health information organization (HIO)—a broad term that HHS intentionally does not define. It has advised, for example, that "the application of the minimum

necessary standard can be automated by the HIO for routine disclosures and requests through the use of standard protocols, business rules, and standardization of data. More complex or non-routine disclosures and requests may not lend themselves to automation, and may require individual review under the Privacy Rule, to the extent the Privacy Rule otherwise applied to the disclosure or request."

MINIMUM NECESSARY IN PRACTICE: ELECTRONIC CASE REPORTING

To assist providers to fulfill their public health reporting obligations, ECR transmits case data directly from a provider's EHR to public health authorities. However, specific reporting requirements vary from one jurisdiction to the next. Not only does the list of reportable diseases vary by jurisdiction, but whether or not a mere suspicion of a case of disease is sufficient to trigger a report, and other decision items, also vary. These variances can create minimum necessary concerns relating to the risk of over-reporting of data elements or reporting of identifiable case information to a jurisdiction that does not in fact require reporting of that disease or condition.

To overcome these minimum necessary challenges, ECR incorporates (1) the Council of State and Territorial Epidemiologists' (CSTE's) Reportable Conditions Knowledge Management System (RCKMS), (2) Reportable Condition Trigger Codes (RCTCs), and (3) a standardized Initial Case Report (eICR).The RCKMS system is a reportable condition knowledge repository and decision-management tool, through which public health authorities input and update their jurisdictional reporting requirements.

The trigger codes are implemented within the EHR system, causing an eICR to be generated when matching clinical data is present in the EHR. The eICR contains data elements identified by a CSTE task force for an all-jurisdiction, all-condition case report. The eICR is then processed through RCKMS to determine if one or more conditions in the case report are reportable and to which public health authority/authorities they should be transmitted. Only then is the eICR transmitted by the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform to one or more jurisdictions.

Electronic case reporting provides an illustration of how minimum necessary can work in an automated reporting environment. It suggests that minimum necessary may be determined in advance through the use of standard protocols and rules in addition to public health reporting requirements. It further suggests minimum necessary may be determined broadly for categories of reportable events, rather than a case-by-case determination.

COMPLIANCE WITH MINIMUM NECESSARY IN PRACTICAL TERMS

In the context of electronic transfer of data, it is important to remember that minimum necessary does not apply to electronic transfers of PHI that are required by law. Thus, for example, where a state law requires specific data elements that must be reported in the event of a positive COVID test lab test result, sending that data through ELR, HIE, or otherwise, does not invoke the minimum necessary rule.

Where minimum necessary does apply, such as in the event of a discretionary report to public health that is not required by law, or where data elements reported go beyond what is expressly required by law, the reasonable minimum necessary standard applies. As noted above, the rule does not require the absolute minimum number of data elements, but rather a limited amount of data that is reasonable under the circumstances.

Minimum necessary also does not apply to treatment. A health care provider, therefore, need not concern itself with minimum necessary when disclosing data for treatment with anyone, including another provider that is also a public health authority that will use the information for treatment.

What's more, as noted above, a regulated entity may rely on the representations of a public health official as to what is the minimum necessary. However, questions persist around what exactly amounts to reasonable reliance on representations of a public official. Could this reasonably be interpreted to mean that reportable data elements communicated through a policy statement could be relied upon as minimum necessary? For example, could data elements identified in a jurisdiction-specific immunization policy agreement, that go beyond what is required by state law, be considered a representation as to minimum necessary? It might be reasonable to interpret it so if such guidance or document could serve as sufficient documentation of the representation of the public official as to the minimum necessary.

Further, because both covered entities and business associates are required to comply with minimum necessary, a covered entity may also rely on the representations of another covered entity or business associate as to what is minimum necessary. Thus, a health care provider could reasonably rely on the request of a covered entity, including a health department that is a covered entity, as the minimum necessary. Similarly, a health care provider may rely on the request from a business associate, such as a HIE or other intermediary that requires regular access to PHI, where appropriate, to determine the minimum necessary.

MINIMUM NECESSARY AND THE INFORMATION BLOCKING RULE

The tension between minimum necessary and the 21st Century Cures Act Information Block Rule has escalated. The Information Blocking Rule prohibits actors, such as health care providers, HINs, and HIEs, from engaging in a practice likely to interfere with access, exchange, or use of electronic health information (EHI) unless an exception to the rule applies. On September 3, 2025, the Assistant Secretary for Technology Policy (ASTP)/Office of National Coordinator (ONC) announced it will ramp up enforcement of the Information Blocking Rule. Some health care providers, including health departments, HIEs and HINs may find themselves between two opposite and competing regulatory requirements—a minimum necessary rule prohibiting them from disclosing too much PHI, and an information blocking rule prohibiting them from not disclosing enough PHI. This tension is a topic for another fact sheet, but it is a concern for the Network and the communities of practice we support.

CONCLUSION

Many would argue minimum necessary was easier to apply in the context of paper records two decades ago than it is in our current age of data modernization. Minimum necessary has been, since its inception, a flexible standard—but one that is also ambiguous, poorly understood, and inconsistently implemented. HHS, however, has emphasized that minimum necessary is not an absolute rule requiring the very least amount of PHI in each use, disclosure, or request, but rather that the regulated entity must make a reasonable effort to limit PHI to the minimum necessary to accomplish the stated purpose. To some extent, it appears minimum necessary solutions in the era of the data modernization initiative may need to be technical solutions, that streamline the reporting of some elements but not, for example, the whole record, in instances in which the whole record exceeds minimum necessary. Electronic case reporting serves as a potential model for other initiatives to apply

protocols and coding to successfully incorporate minimum necessary into workflows to satisfy the HIPAA Privacy Rule minimum necessary requirement.

This document was developed by Stephen Murphy, J.D., Director- Mid-States Region. The Network promotes public health and health equity through non-partisan educational resources and technical assistance. These materials provided are provided solely for educational purposes and do not constitute legal advice. The Network's provision of these materials does not create an attorney-client relationship with you or any other person and is subject to the Network's Disclaimer.

SUPPORTER
Support for the Network provided by the Robert Wood Johnson Foundation. The views expressed in this document do not necessarily reflect the views of the Foundation.