

Is Your NPP Your Best Defense?

Save to myBoK

by Michael R. Lee

In the event of a privacy-related legal challenge, the content of your organization's notice of privacy practices (NPP) will be a focal point for both plaintiff and defense arguments with respect to the protected health information (PHI) disclosure activities of your organization. Is your organization's NPP ready to come to your defense?

When the final privacy rule revisions were introduced in August 2002, two changes dramatically affected information exchanges: individual consent is no longer required and covered entities are granted wide latitude in sharing PHI without authorization under the umbrella of treatment, payment, and operations (TPO). Both these changes elevate the legal significance of your notice of privacy practices (NPP), making the document the basis for defending all your organization's PHI disclosure activities.

This article will discuss specific design and content requirements for the uses and disclosures section of your NPP to defend your organization's actions in the event of a privacy-related civil action.

A "Model Notice"

In the final privacy rule, the Department of Health and Human Services (HHS) states, "Adequate notice of privacy practices is a fundamental right afforded individuals. . .the Department believes that the elements required by § 164.520(b) are important to fully inform the individual of the covered entity's (CE's) privacy practices, as well as his or her rights."

In response to public comments regarding a "model notice," HHS replied, "A covered entity's notice must reflect in sufficient detail the particular uses and disclosures that the entity may make. . .Such uses and disclosures will likely be very different for each type of covered entity."

Here, HHS is suggesting that the NPP is the principle vehicle for informing an individual of all of his or her privacy rights. Further, there is no single solution to defining the specific content for the uses and disclosures section of an NPP.

In practice, one can envision a scenario in which each "disclosure encounter" could require a unique explanation that "fully informs" an individual of his or her "fundamental privacy rights" in that particular situation or context.

Partial Preemption, Adequate Notice

The difficulty with HHS' requirement for the NPP is that the content must satisfy the "adequate notice" and "fully inform" requirements by creating an NPP that describes "in sufficient detail the particular uses and disclosures that the CE may make."

The privacy rule is considered "partially preemptive" because the legislative intent is to provide additional privacy protections without preempting more protective privacy protections existing under other federal, state, and local jurisdictions. As a result, the "adequate notice" and "fully inform" objectives require a CE to provide an individual with a context-specific NPP that includes all relevant privacy protections provided by empowered jurisdictions. In situations in which the CE's uses or disclosures under the privacy rule are "prohibited or materially limited," the NPP "must reflect the more stringent applicable law."

NPP as a Contract

When a breach of contract occurs, the law considers it a duty to remedy the situation. Under this definition, one must conclude that an NPP is actually a contract under which an individual can hold a CE accountable for any uses or disclosures of PHI that

are inconsistent with the entity's NPP.

The privacy rule grants CEs flexibility in sharing PHI under the umbrella of treatment, payment, and healthcare operations (TPO). However, it should be noted that by removing the requirement for "consent" in the final rule, HHS has fundamentally shifted the burden of proof to the CE in the event of privacy-related legal action. Without a signed consent or authorization, the NPP is the only means by which a CE can assert that in a given situation it was "permitted" to disclose the PHI in question.

Authorized, Permitted, Required Disclosures

The NPP must contain descriptions in sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required. Within the scope of the NPP, there are three categories.

Authorized Disclosures

In general, authorized disclosures should be less problematic because each authorization must explicitly state what PHI is involved, the purpose, duration, and to whom it is released. It must also be signed by the individual.

NPP content must fully inform the individual of the CE's obligations under law to release PHI without authorization. In situations in which "other applicable law" provides superior privacy protections, the NPP must include these "fundamental rights" to satisfy the adequate notice requirement.

Permitted Disclosures

The NPP must contain a description and at least one example of the types of use and disclosure permitted for each TPO function.

Required Disclosures

The NPP must contain a description of each of the other non-TPO purposes for which the CE is permitted or required to use or disclose PHI without the individual's written authorization. In addition to federal, state, and local regulations, established case law should also be considered.

Develop a Layered Notice

To compound the NPP content challenge, the privacy rule imposes a duty on CEs to develop the NPP in plain language and in a clear, concise, easy-to-understand manner that is written for the "average reader," while fulfilling the NPP "adequate notice" and "fully inform" requirements. This is a significant challenge because the NPP is a contract that will be interpreted by attorneys related to legal contract performance. A possible solution is to develop a layered notice. This is encouraged but not required by HHS.

The layered notice requires three parts: short notice, long notice, and acknowledgment. All three must be presented to the individual. The short notice provides individuals with a brief summary of their rights. The long notice contains all the elements required under section 164.520. Acknowledgment of receipt satisfies the requirement to document a CE's good faith effort to obtain the individual's written acknowledgment of receipt of the entire notice (all three parts).

With all of the above considered, the importance and purpose of the notice of privacy practices is clear. Make sure your NPP is thorough—it could be your best defense.

References

Hjort, Beth. "Practice Brief: HIPAA Privacy and Security Training." *Journal of AHIMA* 73, no. 4 (2002): 60A-G.

Hughes, Gwen. "Practice Brief: Laws and Regulations Governing the Disclosure of Health Information." Updated November 2002. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Hughes, Gwen. "Practice Brief: Notice of Information Practices." Updated November 2002. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Hughes, Gwen. "Practice Brief: Preemption of the HIPAA Privacy Rule." *Journal of AHIMA* 73, no. 2 (2002): 56A-C.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at <http://aspe.hhs.gov/admnsimp/>.

Michael R. Lee (Michael_Lee@AccessPerformanceNow.com) is president of AccessPerformanceNow, Inc., an application creation and analysis support company based in Thousand Oaks, CA.

Article citation:

Lee, Michael R. "Is Your NPP Your Best Defense." *Journal of AHIMA* 74, no.4 (April 2003): 56-57.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.