# Preemption of the HIPAA Privacy Rule (2010 update)



This practice brief has been retired. It is made available for historical purposes only.

---

*Editor's note: This update supplants the February 2002 practice brief "Preemption of the HIPAA Privacy Rule." The update is based on the August 2002 amendments to the HIPAA privacy rule and includes revisions based on the Health Information Technology for Economic and Clinical Health (HITECH) portion of the American Recovery and Reinvestment Act (ARRA). The content remains accurate.*

The HIPAA privacy rule includes numerous requirements for the use and disclosure of individually identifiable health information (IIHI). In some cases, covered entities (CEs) will be able to comply with both the privacy rule and their state's laws and regulations. In other cases, CEs will have to make a choice between the privacy rule and state laws. How can CEs ensure they are making the lawful choice?

This practice brief will explore what the privacy rule says about preemption. In addition, it will provide readers with a framework for making lawful preemption decisions.

## Legal Requirements

CEs must comply with both federal and state privacy laws and regulations when they can. The privacy rule preempts state law when state law is contrary to the privacy rule. According to the rule, a state law is contrary when:

- A CE would find it impossible to comply with both state and federal requirements
- Adhering to state law would stand as an obstacle to achieving the full purpose of the administrative simplification portions of HIPAA

As is the case with many of the standards within the HIPAA privacy rule, there are exceptions. According to the privacy rule, state law prevails in the following four situations:

- The state law relates to the reporting of disease or injury, child abuse, birth, or death or concerns the conduct of public health surveillance, investigation, or intervention.
- State law requires a health plan to report or provide access to information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.
- A determination is made by the secretary of Health and Human Services (HHS) under §160.204. This section allows a state's chief elected official or designee to petition for an exception from preemption when the state's law is necessary to prevent healthcare fraud and abuse; regulate insurance and health plans; collect healthcare delivery or cost information; ensure public health, safety, or welfare; or regulate controlled substances.
- State law relates to the privacy of health information and is more stringent than privacy rule requirements.

"More stringent" means state law meets one or more of the following six criteria:

- State law further prohibits or restricts a use or disclosure permitted in the privacy rule. However, this exception does not apply when the disclosure is required by the secretary of HHS to determine compliance with the rule or to the individual who is the subject of the individually identifiable health information.
- State law permits greater rights of access to or amendment by the individual who is the subject of the individually identifiable health information. However, this exception is not intended to preempt state law that authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.

- State law permits greater rights of access to the individual who is the subject of the individually identifiable health information about its use, disclosure, or the individual's rights or remedies with regard to the individual's health information.
- State law contains authorization or consent requirements that narrow the scope or duration, reduce the coercive effect, or increase the privacy protections (such as by expanding the criteria) afforded the individual.
- State law provides for more detailed record keeping or retention of information for a longer period.
- State law provides greater privacy protection for the individual who is the subject of the individually identifiable health information; state and federal laws providing extra confidentiality protection for AIDS/HIV information, mental health, alcohol and drug abuse, other sexually transmitted and communicable diseases, and genetic information laws will almost certainly provide greater privacy protection and therefore not be preempted.

## Recommendations

CEs may find that the number of preemption decisions needed can be numerous and overwhelming. Although they can certainly address preemption questions as the need arises, CEs may find that decisions made by employees vary. As a result, application of the privacy rule may be inconsistent. Referring such preemption decisions to legal counsel, however, can create difficulties meeting turnaround requirements and may prove costly.

As an alternative, CEs may find it advantageous to work together as an alliance. For example, CEs may collaborate with state health information management associations, state hospital associations, and legal counsel to assess variations between federal and state privacy rules. This alliance might determine whether CEs can adhere to both federal and state requirements or whether CEs must apply the federal or state law.

This alliance might also determine whether an exception should be requested of the Secretary of HHS or if changes in state law should be introduced. Should they decide to pursue either course, they could work together to achieve such an end.

In the absence of a preemption database, CEs may want to create their own database by using a preemption decision form as a starting point (see "Sample Preemption Decision Form"). This form could be completed and retained in a preemption database for reference by others in the organization when faced with similar questions of preemption. If the matter needs to be referred to legal counsel, the preemption decision form could be forwarded to legal counsel and a copy retained in the preemption database. The attorney's reply could be matched to the copy of the preemption decision form in the preemption database and maintained for future use. CEs may wish to summarize preemption decisions by using an electronic table accessible throughout the organization (see "Sample Preemption Decision Summary Log").

Once you have made a preemption decision, incorporate that decision in your policies and procedures where appropriate. In addition, incorporate some type of ongoing monitoring process to make sure staff is aware of adherence to preemption determinations.

## The Effect of ARRA's HITECH ACT on Preemption

In February 2009 ARRA was signed into law, including revisions to HIPAA's privacy and security rules. Specifically, revisions to CEs and business associate (BA) relationships required changes to business associate agreements (BAAs). ARRA's HITECH provisions require all BAs to comply with the HIPAA security rule and the HIPAA privacy safeguards. HITECH provisions require BAs terminate a BAA or report CE noncompliance to HHS. ARRA also requires BAs to notify the CE in regard to breaches. Because this obligation to notify is statutory, the failure of a BA to comply is more than a breach of contract; the BA could be subject to both civil and criminal penalties found in §13401 and §13404 of ARRA.

In regard to preemption of state law, HITECH references preemption provisions within the Social Security Act (SSA). SSA Act set forth the general rule regarding preemption; however, there is an exception to the SSA general rule in regard to a state law that "relates to the privacy of individually identifiable health information." The HITECH data breach provisions are contained in subsection D, and legislative history references state these provisions affect protection of patient privacy. On the basis of that history, it would be difficult to say that state data security breach laws that apply to health information do not also relate to the privacy of health information. Therefore, to the extent that a state security breach law similarly pertains to health information and is more stringent in the protection of that information than is HITECH, it would appear not to be preempted by the security breach provisions in HITECH. BAs and CEs should be prepared to comply with both laws.

## References

AHIMA. "Analysis of Health Care Confidentiality, Privacy, and Security Provisions of the American Recovery and Reinvestment Act of 2009, Public Law 111-5." April 2009.

AHIMA. "Analysis of the Interim Final Rule, August 24, 2009, Breach Notification for Unsecured Protected Health Information." 2009.

AHIMA. Healthcare Breach Management: Business Associate Agreement Addendum, 2009.

AHIMA. "DRAFT: Template: Health Information Privacy and Security Breach Notification Letter." 2009.

AHIMA. "Health Care Reform and Health IT Stimulus: ARRA and HITECH." Available online at www.ahima.org/advocacy/arrahitech.aspx [web page no longer available].

AHIMA. "Model Breach Notification Letter: Content and Format." 2009.

AHIMA. "Public Law 111-5, 'American Recovery and Reinvestment Act.'". March 2009. Available online at

AHIMA. "Reports and Other Submission Requirements; Public Law 111-5, 'American Recovery and Reinvestment Act.'" April 2009.

American Recovery and Reinvestment Act of 2009. Public Law 111-1.

Health Insurance Portability and Accountability Act of 1996. Public Law 104-191.

Journal of AHIMA. Privacy and security posts. Available online at http://journal.ahima.org/category/privacy-and-security/.

Rhodes, Harry. "Developing Breach Notification Policies and Procedures: An Overview of Mitigation and Response Planning." 2009.

Rhodes, Harry. "The Path to Security Breach Notification Regulation." 2009.

Standards for Privacy of Individually Identifiable Health Information; Final Rule. 45 CFR Part 160. *Federal Register* 67, no. 157 (August 14, 2002).

Tomes, Jonathan P. *The Compliance Guide to HIPAA and the HHS Regulations*. Overland Park, KS: Veterans Press, 2001.

## Prepared by

Angela K. Dinh, MHA, RHIA, CHPS

## Prepared by (original)

Gwen Hughes, RHIA, CHP

## Acknowledgments (original)

Holly Ballam, RHIA
Jill Callahan Dennis, JD, RHIA
Michelle Dougherty, MA, RHIA, CHP
Beth Hjort, RHIA, CHP
Mary Thomason, RHIA
Jonathan P. Tomes, JD

**Sample Preemption Decision Form**

**1. What is the issue you need to resolve?**

**2. What does the privacy rule say about the issue (include citation)?**

**3. What does the state law or regulation say (include citation)?**

**4. Can you comply with both the privacy rule and state law or regulation?**

___ Yes (Implement procedures that enable you to comply with both federal and state law.)

___ No (Go to question 5.)

**5. In general, the privacy rule preempts state law. There are, however, four exceptions. Does your issue meet one or more of the following exceptions?**

1. It relates to the reporting of disease or injury, child abuse, birth, death, or the conduct of public health surveillance, investigation, or intervention.
2. It relates to the requirement that a health plan report or provide access to information for the purpose of management audits, financial audits, program monitoring, and evaluation or the licensure or certification of facilities or individuals.
3. The secretary of Health and Human Services granted an exception under §160.204 of the HIPAA privacy rule.
4. State law or regulation is **more stringent** than the privacy rule. In other words, it meets one or more of the criteria below:

    - State law further prohibits a use or disclosure of information other than to the individual or secretary of HHS.
    - State law permits greater rights of access to the individual who is the subject of the protected health information (Note: This is not intended to preempt other state law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.)
    - State law provides greater information about use, disclosure, rights, and remedies to the individual who is the subject of the individually identifiable health information.
    - State law requires a narrower scope or duration, increases the privacy protections afforded (such as by expanding the criteria for), or reduces the coercive effect of the consent or authorization.
    - State law provides for more detailed record keeping or retention of information for a longer period.
    - State law provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

**No, my issue does not meet one of the exceptions above. (Apply federal law.)**

**Yes, I have checked one or more of the four exceptions. (Apply state law or regulation.)**

**6. Is the decision about whether to adhere to either or both federal and state law clear?**

___ **Yes**? My organization must adhere to:

- both federal and state law or regulation
- federal law or regulation
- state law or regulation

___ **No**? Refer to legal counsel.

_____
Employee Name

_____
Employee Title/Department

_____
Extension

_____
Date

_____
Date Submitted to Legal Counsel

Subsequent Comments: (Please date and sign)

*This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.*

**Sample Preemption Decision Summary Log**

**Decision**
**(Check appropriate box below)**

| | |
|---|---|
| **Issue** | |
| **HIPAA standard and citation** | |
| **State standard and citation** | |
| **Adhere to both federal and state laws** | |
| **Adhere to federal law** | |
| **Adhere to state law** | |
| **Date** | |
| **Preemption decision made by** | |

*This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.*

**Article citation**:
AHIMA. "Preemption of the HIPAA Privacy Rule (2010 update)." *Journal of AHIMA* (Updated June 2010).