

## Interpreting and Applying the HIPAA Preemption Provisions to State Privacy Law\*

Aimee N. Wall\*\*

The preemption provisions of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)<sup>1</sup> disappointed many players in the health care industry. Most industry representatives argued for total preemption so that covered entities would only need to comply with a single uniform law.<sup>2</sup> Patient advocates, on the other hand, wanted a federal floor so that states could continue to have the opportunity to enact more stringent state laws.<sup>3</sup> What the Congress produced in the HIPAA legislation has been termed a federal floor, but covered entities should be wary because this floor has several holes and loose boards. Now covered entities, attorneys and compliance officers around the country are faced with the daunting task of comparing their state laws with this complex and untested new federal law and determining whether and how each state law will be preempted.

Covered entities and their advisors cannot expect much assistance in this task from the federal government. In the proposed privacy regulation, the agency responsible for the HIPAA regulations – the U.S. Department of Health and Human Services (DHHS) – included an “advisory opinion” process by which states could request an opinion as to whether a state law would be preempted.<sup>4</sup> DHHS abandoned the advisory opinion process in the final regulation, offering a couple of reasons for its decision. The most convincing explanation pointed to the agency’s limited resources for providing technical assistance: “Our concern is that setting up an advisory opinion process for just one of the many types of issues that will have to be addressed

---

\* This paper was prepared for and presented at the American Bar Association’s Health Law Section Conference held in Phoenix, Arizona February 27-March 2, 2002.

\*\* The author is an Assistant Professor of Public Law and Government at the University of North Carolina’s School of Government in Chapel Hill.

<sup>1</sup> See 42 U.S.C.A. § 1320d *et seq.* (West Supp. 2001); Pub. L. No. 104-191, § 264 (1996); 45 C.F.R. § 160.201 *et seq.* (2001).

<sup>2</sup> See, e.g., *Hearing on Medical Privacy Legislation Before the Subcommittee on Government Management, Information and Technology of the House Committee on Government Reform and Oversight of the United States House of Representatives on Medical Privacy Legislation, 105<sup>th</sup> Cong.* (May 19, 1998) (testimony of the American Hospital Association) *available at* <http://www.aha.org/ar/Testimony/MedicalPrivacyLegislation.asp> (recommending that Congress enact privacy legislation that is “both a floor and a ceiling, preempting all state laws with which it may conflict, weaker or stronger. Only through such a uniform law can patients' health information be equally protected regardless of the state in which they live or travel.”).

<sup>3</sup> See, e.g., *Hearing on Medical Records Confidentiality in the Modern Delivery of Health Care Before the U.S. House of Representatives Committee on Commerce, Subcommittee on Health and the Environment, 106<sup>th</sup> Cong.* (May 27, 1999) (testimony of Abbey Meyers, President of the National Organization for Rare Disorders) *available at* [http://www.healthprivacy.org/usr\\_doc/33800.pdf](http://www.healthprivacy.org/usr_doc/33800.pdf) (urging Congress to enact legislation that provides a federal floor and permits “states [to] maintain their right to enact stricter privacy laws to address the specific needs of their residents”).

<sup>4</sup> See Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 60,051-52 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(b)).

will lead to a non-optimal allocation of the resources available.”<sup>5</sup> The agency further explained that it would not be conducting a global preemption analysis for all fifty states and that this burden fell on the regulated entities as part of their compliance process.<sup>6</sup>

As attorneys and others begin sorting through their state laws, it is important that they have a clear understanding of the preemption provisions as they are interpreted in the final regulation. In order to assist attorneys with this analysis, this paper will first describe and discuss the preemption provisions in detail, focusing exclusively on the application of those provisions to the privacy regulation. In reviewing the preemption provisions, this paper will highlight some of the regulation’s potential ambiguities and complexities. Finally, this paper will discuss the approach to conducting a preemption analysis adopted by the State Law Work Group of the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA).

## I. General Rule

The general rule of HIPAA preemption is that a standard, requirement or implementation specification (hereinafter “requirement”) of an Administrative Simplification regulation preempts any contrary provision of State law.<sup>7</sup> This general rule applies to all of the Administrative Simplification regulations, including the privacy regulation. There are, of course, several exemptions from this general rule, which will be discussed in more detail in Section II.<sup>8</sup> The general rule alone, however, raises several issues that merit further discussion and consideration.

### A. Covered entities only

One crucial aspect of the general rule that is not spelled out explicitly in the preemption sections of the regulation is perhaps intuitive but should always be kept in mind when reviewing

---

<sup>5</sup> Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,580 (Dec. 28, 2000). Had DHHS retained the advisory opinion process in the final rule, the agency would most certainly be flooded with requests for such determinations as thousands of covered entities are now struggling to comprehend their new legal landscapes.

<sup>6</sup> DHHS explained in the preamble to the final rule that “We . . . do not agree that the task of evaluating the requirements [of the rule] in light of existing state law is unduly burdensome or unreasonable. Rather, it is common for new federal requirements to necessitate an examination by the regulated entities of the interaction between existing state law and the federal requirements incident to coming into compliance.” *Id.* at 82,583.

<sup>7</sup> 42 U.S.C.A. § 1320d-7(a)(1) (West Supp. 2001); 45 C.F.R. § 160.203 (2001).

<sup>8</sup> In order to distinguish between the various types of “exceptions” to the privacy regulation – some of them created by statute as part preemption exceptions and some of them created by regulation as exceptions to the general rules of the privacy regulation – this paper uses the terms “exemption” and “exception” to distinguish different concepts. This paper uses the terms “exemption” and “carve-out” to refer to the provisions in 45 C.F.R. § 160.203 that effectively exempt a law from preemption that would otherwise be preempted under the general rule of preemption. This paper uses the term “exception” to refer to those categories of uses and disclosures in 45 C.F.R. § 164.512 that are permitted under the privacy regulation as an exception to the general privacy rules – such as uses and disclosures for public health, oversight, research and law enforcement purposes.

state laws: if a state law is preempted, in whole or in part, it will only be preempted as it applies to covered entities. The privacy regulation only applies to three types of covered entities – health plans, health care clearinghouses and health care providers who transmit health information in electronic form in connection with a HIPAA transaction.<sup>9</sup> DHHS explains in the preamble to the final regulation that “a state is free to continue to enforce a ‘preempted’ state law against non-covered entities to which the state law applies.”<sup>10</sup> One North Carolina statute, for example, applies to specific classes of information regardless of who maintains it. The statute reads in part:

All information and records, whether publicly or privately maintained, that identify a person who has AIDS virus infection or who has or may have a disease or condition required to be reported pursuant to the provisions of this Article shall be strictly confidential. This information shall not be released or made public except under the following circumstances ... [statute lists several different circumstances including treatment, public health, law enforcement, etc.]<sup>11</sup>

This statute, therefore, will continue to apply in its entirety to this class of communicable disease information maintained by all non-covered entities. For covered entities, however, each provision of the statute must be analyzed separately to determine how it interacts with the privacy regulation.

This result may not present any challenges for most entities. Each entity will first determine whether it is covered. If the entity is covered, it will comply with the privacy regulation and if it is not covered, it will comply with the state law. Consider, however, how the existence of these two separate legal schemes will affect hybrid entities.<sup>12</sup> The non-health care components of a hybrid entity will most likely be subject to an entirely different legal scheme than the health care components. As a result, the attorneys and compliance officers of hybrid entities must tackle both schemes and ensure that the workforce is appropriately trained. Employees who straddle both health care and non-health care components will not only need to erect internal firewalls, but they will also need to fully understand and comply with two separate, complex legal schemes. In those states with robust privacy laws, entities may elect to avoid designation as a hybrid entity because of the complexities related to compliance with two different legal schemes.

---

<sup>9</sup> 45 C.F.R. §164.104.

<sup>10</sup> See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,587 (Dec. 28, 2000).

<sup>11</sup> N.C. GEN. STAT. § 130A-143 (1999).

<sup>12</sup> A hybrid entity is “a single legal entity that is a covered entity and whose covered functions are not its primary functions.” 45 C.F.R. § 164.504(a). “Covered functions” are “those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.” *Id.* at § 164.501. A covered entity that satisfies the definition of a hybrid entity may elect to designate itself as a hybrid entity to avoid many of the additional administrative requirements imposed by the privacy rule.

## B. “Contrary” defined

The key to the general rule is that the provision of State law must be “contrary to” the federal requirement. DHHS explains that “where state law exists and no analogous federal requirement exists, the state requirement would not be ‘contrary to’ the federal requirement and would not trigger preemption.”<sup>13</sup> However, when both state law and federal law exist, the entity must evaluate both provisions carefully to determine if they satisfy the regulatory definition of “contrary.”

Intending to clarify the statutory language, DHHS defined “contrary” by drawing on decades of conflict preemption jurisprudence.<sup>14</sup> The definition states that when comparing a provision of State law to a requirement of the rule, contrary means either:

- A covered entity would find it impossible to comply with both the State and federal requirements; or
- The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act (Administrative Simplification) or section 264 of Pub. L. 104-191 (requiring privacy regulations), as applicable.<sup>15</sup>

Courts have struggled with the application of these two tests over the years. The “obstacle test” has been interpreted much more liberally than the “impossibility test;” in fact, one author recently decreed that “constitutional law has no place for the Court’s fuzziest notions of “obstacle” preemption....”<sup>16</sup> Despite the criticisms, these two tests are well-established and, in fact, were recently reaffirmed by the Supreme Court in *Crosby v. National Foreign Trade Council*.<sup>17</sup> In the proposed regulation, DHHS indicated that the obstacle test “is particularly relevant with respect to the...HIPAA regulations [other than the privacy regulation], where Congress clearly intended uniform standards to apply nationwide.”<sup>18</sup> Despite this DHHS commentary potentially limiting the scope of the obstacle test, covered entities are likely to rely on this more flexible test when determining the preemptive effect of the privacy regulation on their state’s laws. Considering that DHHS produced hundreds of pages of commentary supporting the regulation, attorneys will almost always have ready access to material explaining the “purpose and objectives” of any given requirement of the regulation.

Given the complexity of the privacy regulation and the level of detail in the requirements, this definition of contrary may present some interesting challenges in implementation. For

---

<sup>13</sup> See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,581 (Dec. 28, 2000).

<sup>14</sup> See Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,996-97 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. Parts 160 and 164).

<sup>15</sup> 45 C.F.R. § 160.202.

<sup>16</sup> See Caleb Nelson, *Preemption*, 86 VA. L. REV. 225, 231 (2000).

<sup>17</sup> *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 372-73 (2000) (applying the “impossibility” and “obstacle” preemption tests).

<sup>18</sup> See Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,997 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(b)).

example, the privacy regulation requires all authorization forms to include a “statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by [the privacy regulation].”<sup>19</sup> North Carolina law requires certain mental health providers releasing confidential information to inform the recipient that redisclosure is prohibited without the client’s written authorization.<sup>20</sup> Assuming that both legal requirements are followed, the authorization form might read:

Once information is disclosed pursuant to this signed authorization, the federal privacy regulation (45 C.F.R. Part 164) may not prohibit the recipient from redisclosing it. Other laws, however, may prohibit redisclosure. State law requires us to inform the recipient of the information that redisclosure is prohibited without your written consent.

As seen above, it is certainly not “impossible” to implement these two requirements nor does the state regulation necessarily “stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives” of the privacy regulation. However, this type of explanation is likely to be confusing and frustrating for individuals signing the authorization.

### ***C. “Provision of state law”***

In the context of preemption, DHHS defines “State law” to mean “a constitution, statute, regulation, rule, common law or other State action having the force and effect of law.”<sup>21</sup> The regulation, however, requires preemption analyses to break these state laws down even further into “provisions of state law” when comparing them to requirements of the regulations. Several commenters questioned whether state laws could be evaluated as a whole and determined to be more or less protective rather than breaking them down provision-by-provision.<sup>22</sup> DHHS rejected outright the possibility of doing more global comparisons of overall effect, arguing instead that the statute mandated this provision-by-provision approach.<sup>23</sup>

The statute does in fact utilize the term “provision of state law” and therefore it would appear that Congress might have envisioned such an approach.<sup>24</sup> In addition, with respect to statutes and regulations at least, this approach seems to be the most logical and appropriate way to conduct any type of comparison. The requirements of the privacy regulation are far too intricate to attempt a generalized comparison. Instead, it is more appropriate to isolate provisions of law and compare them to the specific requirements of the privacy regulation.

“Provision” is not defined in the regulation, therefore it is up to the attorneys, compliance officers and courts to determine its meaning. All will likely struggle with the concept of severability. A “provision” of a statute or regulation could be defined as a sentence, a clause, a

---

<sup>19</sup> 45 C.F.R. § 164.508(c)(1)(vi).

<sup>20</sup> N.C. ADMIN. CODE tit. 10, r. 18D.0214 (June, 2000).

<sup>21</sup> 45 C.F.R. § 160.202.

<sup>22</sup> See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,582 (Dec. 28, 2000).

<sup>23</sup> See *id.*; see also Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,995 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(b)).

<sup>24</sup> 42 U.S.C.A. § 1320d-7(a) (West Supp. 2001).

subclause and even a single word depending on the context. A “provision” of common law may be even more challenging to define.

In the preamble to the proposed regulation, DHHS signaled another potential challenge: “[t]here may ... be situations in which there is a federal requirement with no directly analogous State requirement, but where several State requirements in combination would seem to be contrary in effect to the federal requirement.”<sup>25</sup> Therefore, it appears that DHHS expects entities to first break down state laws into “provisions,” evaluate those provisions in isolation and also evaluate those provisions in the context of other applicable state laws before determining whether the provision will be preempted. Given this expectation, attorneys preparing a preemption analysis should be quite familiar with the entire landscape of state privacy laws rather than simply reviewing individual statutes and regulations provision-by-provision.

## II. Preemption Exemptions

If one concludes that a provision of state law is contrary to a HIPAA requirement, the preemption analysis has only just begun because the statute and regulation outline several different exemptions from the general rule. Each of these exemptions will be discussed in more detail below.

### A. “*More stringent*”

HIPAA will not preempt any provision of State law that “relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification of the privacy rule.” Therefore, in general, provisions of state law that provide greater privacy protections will not be preempted. This exemption is cobbled together from two different parts of the original legislation. The Administrative Simplification subtitle includes the following language:

A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall not supersede a contrary provision of State law, if the provision of State law ...[,] subject to section 264(c)(2) of [HIPAA], *relates to the privacy of individually identifiable health information.*<sup>26</sup>

Section 264(c)(2) provides that any health privacy regulation promulgated by DHHS “shall not supercede a contrary provision of State law, *if the provision of State law imposes requirements ... that are more stringent than the requirements ... imposed under the regulation.*”<sup>27</sup> DHHS clarified the legislative language by combining these two provisions into a single exemption in the regulation. In an effort to further clarify the exemption, the agency took steps to define

---

<sup>25</sup> Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,995 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(b)).

<sup>26</sup> 42 U.S.C.A. § 1320d-7(a)(2)(B) (emphasis added).

<sup>27</sup> Pub. L. No. 104-191, § 264(c)(2) (1996) (emphasis added)

several of the terms and even used the definitions to convey a significant policy decision regarding minors' health information.

1. "Relates to the privacy of individually identifiable health information"

In order for a provision of state law to satisfy the definition of the clause "relates to the privacy of individually identifiable health information," it must either:

- have the "specific purpose" of protecting privacy; or
- affect privacy in a direct, clear and substantial way.

The agency appears to have given careful consideration to the development of this definition. Drawing on years of interpretation of the term "relates to" in the context of ERISA litigation and in similar contexts, DHHS explained in the proposed regulation that the definition "grows out of the movement in recent years of the Supreme Court away from the literal, textual approach [to analyzing preemption statutes] to an analysis that looks more at the purposes and effects of the preemption statute in question."<sup>28</sup> DHHS identified a line of Supreme Court cases that it interpreted to mean that the regulation should take

an approach that looks to the legislative history of HIPAA and seeks to determine what kinds of State laws Congress meant, in this area, to leave intact and also seeks to apply more of a "rule of reason" in deciding which State laws "relate to" privacy and which do not.<sup>29</sup>

The agency then pointed to only a single source of legislative history, which simply stated: "[t]he intent of this section is to ensure that State privacy laws that are more stringent than the requirements and standards contained in the bill are not superseded."<sup>30</sup>

If one is fighting to save a provision from being preempted, it may be easier to demonstrate that a provision of state law "affects privacy in a direct, clear and substantial way" than it will be to identify the law's "specific purpose." In response to comments arguing that the "specific purpose" test is "difficult and speculative [ ] because many state laws have incomplete, inaccessible, or non-existent legislative histories," DHHS explained "[t]he purpose of a given state enactment should be ascertainable, if not from legislative history or a purpose statement, then from the statute viewed as a whole."<sup>31</sup> While both tests will most likely invite litigation, the first test – because it is less concrete than the "specific purpose" test – may result in some conflicting and confusing precedent.

---

<sup>28</sup> Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,996 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(b)) (citing *New York State Conference of Blue Cross v. Travelers Insurance Co.*, 514 U.S. 645 (1995)).

<sup>29</sup> *Id.*

<sup>30</sup> *Id.* (citing House Rep. No. 496, 104th Cong., 2d Sess., at 103) (emphasis added).

<sup>31</sup> *Id.* at 82,582-83.

## 2. “More stringent”

The regulatory definition of “more stringent” provides significant guidance to covered entities as they try to compare contrary state laws to the privacy regulation. The regulation provides that a provision of state law is “more stringent” if it meets one or more of the following criteria:

- With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which the privacy regulation would not, except if the disclosure is:
  - Required by DHHS in connection with determining whether a covered entity is in compliance with the Administrative Simplification requirements; or
  - To the individual who is the subject of the information;
- With respect to the rights of an individual who is the subject of the information of access to or amendment of health information, permits greater rights of access or amendment, as applicable (exception applicable to minors discussed below);
- With respect to information to be provided to an individual who is the subject of the information about a use, a disclosure, rights and remedies, provides the greater amount of information;
- With respect to the form or substance of an authorization or consent for use or disclosure of health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable;
- With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information for a longer duration; or
- With respect to any other matter, provides greater privacy protection for the individual who is the subject of the health information.

Each of the above components of the definition of “more stringent” is fairly intuitive and therefore may appear to be overly detailed or complex. Nonetheless, this level of specificity in the text of the regulation certainly provides clarity and is also likely to reduce the potential for litigation.

Rather than discuss each component of the definition in detail, it may be more helpful to illustrate the interpretation and application of one component of the definition of more stringent. One North Carolina statute provides:

[Notwithstanding any law] relating to the confidentiality of communications between physician and patient, in the course of an inspection [of an adult care home] Department representatives may review any writing or other record concerning the admission, discharge, medication, care, medical condition, or history of any person who is or has

been a resident of the facility being inspected ... unless the resident objects in writing to review of his records or disclosure of such information.<sup>32</sup>

Assuming that the adult care home is a covered entity, the first question to ask is whether this law is contrary to the privacy regulation. The privacy regulation would permit the adult care home to disclose protected health information (PHI)<sup>33</sup> to a health oversight agency for oversight activities authorized by law and specifically identifies inspections as possible oversight activities.<sup>34</sup> Such a disclosure would be allowed without any form of individual permission (e.g., authorization, opportunity to agree or object or opportunity to opt-out).

The North Carolina statute takes a somewhat different approach and could be considered “contrary to” the privacy regulation in at least two different respects.<sup>35</sup> First, the state statute restricts disclosure to limited classes of information (i.e., admission, discharge, medication, care, medical condition or history...) whereas the privacy regulation would permit the disclosure of any PHI requested by a public official of the oversight agency for oversight activities authorized by law.<sup>36</sup> This provision would be “contrary” to the privacy regulation with respect to any PHI that does not fall within one of the classes of information identified by the state statute because it would be impossible to comply with both the regulation and the state statute with respect to that information. The general rule of HIPAA preemption would dictate that the contrary provision of the state statute – i.e., the restricted classes of PHI – would be preempted. However, the provision would likely be exempted from preemption because it “relates to the privacy of individually identifiable health information” and is “more stringent” than the privacy regulation. Specifically, the provision “relates to privacy” because it affects privacy in a clear and substantial way and it is “more stringent” because it prohibits or restricts a use or disclosure in

---

<sup>32</sup> N.C. GEN. STAT. § [131D-2](#)(b)(4) (1999).

<sup>33</sup> Protected health information is any information, whether oral or recorded in any form or medium (including demographic information collected from the individual), that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and either identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- Is not health information in education records covered by the Family Educational Right and Privacy Act (FERPA) or certain medical record information about college students.

See 45 C.F.R. § 160.103 (2001) (definition of health information); 45 C.F.R. § 164.501 (definitions of individually identifiable health information and protected health information).

<sup>34</sup> 45 C.F.R. § 164.512(d)(1).

<sup>35</sup> This analysis assumes that a provision-by-provision approach requires the single sentence statute to be parsed into two separate sub-clauses that are to be examined independently. One could argue that in order for the provision-by-provision approach to be manageable, it must be limited to entire sentences or clauses.

<sup>36</sup> The minimum necessary principle applies to disclosures for oversight purposes but the “entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when ... [m]aking disclosures to public officials that are permitted under [45 C.F.R.] § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s).” 45 C.F.R. § 164.514(d)(2)(iii).

circumstances under which the privacy regulation would not. The end result of this analysis would be that, in the course of an inspection by an oversight agency, an adult care home should only disclose the classes of information identified in the state statute.

The second provision of the state statute that could be construed as “contrary to” the privacy regulation is that the resident may object in writing to the disclosure. As explained above, the privacy regulation would allow the home to disclose PHI to the oversight agency without any form of individual permission. It is arguably “impossible” to comply with both the state statutory provision and the privacy regulation and therefore one should conclude that the provision is “contrary.”<sup>37</sup> The state statutory provision could be interpreted in two different ways:

- the adult care home must inform the resident of the disclosure and provide her with an opportunity to object or
- the home is not required to affirmatively inform the resident of the disclosure but must honor any objections volunteered by the resident.

Both interpretations, however, run afoul of the privacy regulation. The first interpretation – the affirmative duty – could be compared to the privacy regulation’s requirement that in certain circumstances individuals must be provided with the opportunity to agree or object to certain disclosures.<sup>38</sup> Such a comparison is not valid because the privacy regulation’s “opportunity” is not available in the context of disclosures to oversight agencies.<sup>39</sup> The second interpretation – honoring volunteered objections – could be compared to the privacy regulation’s right to request restrictions on certain uses and disclosures of PHI.<sup>40</sup> This right does not, though, extend to uses and disclosures for oversight purposes.<sup>41</sup> Therefore, it would seem that the two laws are contrary to one another.

The state statutory provision would, however, ultimately be exempted from preemption. Specifically, the provision “relates to” privacy because it affects privacy in a direct, clear and substantial way and it is “more stringent” than the privacy regulation because it prohibits or restricts a use or disclosure in circumstances under which the privacy regulation would not – i.e., when the individual has objected to the disclosure.<sup>42</sup> Based on this analysis, this statutory provision relating to resident objections would also likely remain in force.

---

<sup>37</sup> It would, however, be possible to comply with both laws if the resident never objects to the disclosure.

<sup>38</sup> 45 C.F.R. § 164.510.

<sup>39</sup> The opportunity is only available in a few specific situations, including when a covered entity is using or disclosing PHI for a facility directory and when a covered entity is disclosing PHI to a person involved in the patient’s care. *Id.*

<sup>40</sup> 45 C.F.R. § 164.522(a).

<sup>41</sup> *Id.* at § 164.522(a)(1)(i).

<sup>42</sup> Alternatively, one could argue that the provision is more stringent in that it “provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding [an] authorization or consent, as applicable.” 45 C.F.R. § 160.202 (definition of “more stringent”). While the state statute’s recognition of an “objection” is different from a “consent” or “authorization” as those terms are used in the privacy regulation, this component of the definition of more stringent could be interpreted expansively to

### 3. Minors carve-out

In drafting the privacy regulation, DHHS faced a significant challenge balancing the policy interests regarding parental access to minors' health information. The statute did not speak directly to this controversial issue so the agency had much discretion when crafting this policy. The agency clearly tried to achieve a compromise that would satisfy advocates on both sides of this issue. First, in the body of the privacy regulation, the agency established a general rule regarding parents acting as personal representatives that would have created a landmark federal floor of protections for minors' records. Buried in the definitions section of the preemption provisions, however, the agency carved-out certain state laws relating to parental access, which effectively erased the federal floor in those states that have any law.

The general rule is that a parent, guardian or person acting *in loco parentis* (hereinafter parent/guardian) may act as an unemancipated minor's personal representative except, with respect to PHI pertaining to a particular health care service, in three situations:

- The minor consents to the health care; no other consent is required by law (regardless of whether another person's consent has been obtained); and the minor has not requested that the parent/guardian be treated as the personal representative;
- The minor may lawfully obtain the health care service without the consent of a parent/guardian and the minor, a court or another person authorized by law consents to the service; or
- A parent/guardian assents to an agreement of confidentiality between a provider and the minor with respect to the health care service.

Therefore, DHHS established a federal floor of new privacy rights for unemancipated minors who are legally able to consent to their own care, obtain court permission to obtain care or reach an agreement regarding confidentiality with their parents/guardians.

Anticipating strong opposition to this federal floor, DHHS created a large exception to this general rule. The agency carved-out certain existing state laws by defining "more stringent" to mean, in part:

[w]ith respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable, provided that, *nothing in this subchapter may be construed to preempt any 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.*<sup>43</sup>

The italicized clause may be interpreted quite broadly to mean that any State law addressing disclosure of a minor's information to a parent/guardian shall remain in force. It could also be

---

incorporate all types of individual permission given that a variety of different terms are currently used throughout the health care industry to represent similar concepts and legal documents.

<sup>43</sup> 45 C.F.R. § 160.202 (definition of "more stringent") (emphasis added).

interpreted strictly to be modifying the first part of the clause and therefore be limited to only those laws specifically addressing access to or amendment of PHI.

Interpretation of the clause could have far reaching implications in some states. For example, North Carolina law provides that a minor may consent to certain health services (e.g., prevention, diagnosis and treatment of venereal diseases and other reportable communicable diseases).<sup>44</sup> Another statute provides:

The physician shall not notify a parent, legal guardian, person standing in loco parentis...<sup>45</sup>, without the permission of the minor, concerning the [health services to which a minor may consent under § 90-21.5] unless the situation in the opinion of the attending physician indicates that notification is essential to the life or health of the minor.<sup>46</sup>

If the minors' carve-out to the privacy regulation is narrowly interpreted such that it only applies to laws addressing access to or amendment of PHI, it is possible that the statutory provision above permitting physicians to notify parents/guardians would *not* be carved-out of preemption because it would be considered related to notification rather than to access or amendment.<sup>47</sup>

Another sentence in the same North Carolina statute states that “[I]f a parent ... contacts the physician concerning the treatment or medical services being provided to the minor, the physician may give information.”<sup>48</sup> A strong argument exists that this provision is related to “access” and therefore would fall within the minors' carve-out even if it were narrowly construed. In other words, the state provision is contrary to the privacy regulation because the privacy regulation would not permit disclosure to the parent/guardian upon request (because the minor legally consented to the care) but the provision would *not* be preempted because it authorizes a parent's/guardian's access to PHI. Given the political volatility of the issue of minors' health information, it would be fair to assume that this ambiguity will serve as a lightning rod for litigation.

## ***B. Public health carve-out***

The privacy regulation carves-out provisions of state law that “provide[] for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance,

---

<sup>44</sup> N.C. GEN. STAT. § 90-21.5 (1999).

<sup>45</sup> The statute adds the following category as well: “a legal custodian other than a parent when granted specific authority in a custody order to consent to medical or psychiatric treatment.” N.C. GEN. STAT. § 90-21.4(b). It will be interesting to see whether courts interpret this fourth category as equivalent to “a person acting *in loco parentis* for the purposes of comparing the law to the privacy regulation.

<sup>46</sup> N.C. GEN. STAT. § 90-21.4(b).

<sup>47</sup> This result is troubling in part because a physician is likely bound by other laws or ethical guidelines that he or she believes compels notification of the parents in situations when “essential to the life or health of the minor.” If such notification is prohibited by the privacy regulation, physicians may be reluctant to care for minors without parental consent.

<sup>48</sup> *Id.*

investigation or intervention.”<sup>49</sup> This carve-out is likely to be interpreted and applied expansively for two basic reasons. First, the carve-out is not limited to public health laws that “require” certain disclosures. Rather, it applies to all state laws that “provide for” certain disclosures or activities. Because the term “provide for” is so expansive, it is likely to be interpreted to encompass not only laws that specifically authorize the use or disclosure of PHI, but also laws that implicitly authorize use or disclosure by establishing a public health program that utilizes PHI. Second, the carve-out applies not only to the state law but also to any procedures established under such law. For example, a state statute may authorize an agency to collect data for a cancer registry. In order to implement the statutory requirement, the agency may develop reporting forms for providers to use in reporting cancer diagnoses. This form – while not specifically required by state law – could be interpreted to be a “procedure” established under a state law and therefore would not be vulnerable to a preemption challenge.

DHHS recognized that by establishing such a broad public health carve-out, Congress clearly intended to leave untouched many of the state laws and procedures that govern our nation’s public health system.<sup>50</sup> In addition to the carve-out, therefore, the agency created a public health exception that identifies several circumstances in which covered entities may use and disclose PHI without individual permission for certain public health purposes.<sup>51</sup> It also created an exception for uses and disclosures “required by law,” which encompasses many state public health laws. Any analysis of a public health law should not begin with the carve-out but rather should begin with the exceptions to the general rules of the privacy regulation – particularly the “public health” and “required by law” exceptions. If the use or disclosure permitted by the state law does not fall within one of the exceptions and is contrary to the privacy regulation, the next step should be to review public health carve-out.

The public health exception is more expansive than the carve-out in some ways and narrower in others. The drafting of the public health exception is rather awkward but there are a few different general rules. In general, a covered entity may disclose certain PHI without individual permission to:

- A public health authority (or to an official of a foreign government agency that is acting in collaboration with a public health authority) that is authorized by law to collect or receive PHI for certain public health purposes;
- A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;
- A person subject to the jurisdiction of the Food and Drug Administration for certain purposes related to product tracking, recall, post marketing surveillance, etc.;

---

<sup>49</sup> 45 C.F.R. § 160.203(c).

<sup>50</sup> In the preamble to the final rule, DHHS explained: “We have deferred to Congressional intent by crafting the permissible releases for public health ... broadly....” Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,584 (Dec. 28, 2000).

<sup>51</sup> 45 C.F.R. § 164.512(b).

- A person who may have been exposed to a communicable disease (if otherwise authorized by law to make such a notification); and
- An employer in limited circumstances for purposes related to the employer’s legal obligations regarding work-related injury and illness.<sup>52</sup>

In order to illustrate the interplay between the public health exception and the public health carve-out, this paper will discuss in more detail the first category of uses and disclosures permitted under the public health exception.

The general rule is that a covered entity may disclose PHI without individual permission as long as three conditions are satisfied.<sup>53</sup> First, the disclosure must be for the broad purpose of “preventing or controlling disease, injury, or disability.”<sup>54</sup> The rule offers the following two non-exclusive examples:

- The reporting of disease, injury and vital events (such as birth or death); or
- The conduct of public health surveillance, investigation and intervention.

The second condition that must be satisfied is that the disclosure must be to a “public health authority” or “at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.”<sup>55</sup> Third, and finally, the public health authority must be authorized by law to collect or receive the information.

The first condition – that the disclosure must be for the purpose of preventing or controlling disease, injury or disability – appears to be much more expansive than the public health carve-out. The carve-out is limited in scope to allow disclosures only for a few specific purposes: the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention. While the examples listed in the exception incorporate all of the specific purposes listed in the carve-out, it is important to remember that they are listed only as examples. DHHS clearly intended to expand the scope of the public health exception beyond the categories covered in the carve-out.

The second and third conditions hinge on the definition of “public health authority.” The regulation defines the term broadly to mean:

an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.<sup>56</sup>

---

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> *Id.*

<sup>55</sup> *Id.* at § 164.512(b)(1)(i).

<sup>56</sup> *Id.* at § 164.501.

Because the definition is so broad, it is unlikely to present any significant challenges in implementation. The third condition requires the public health authority to be authorized by law to collect or receive the information. One question that arises is whether the public health authority must have specific authority to collect particular information, or whether general legal authority to protect the public health will be sufficient. For example, the Secretary of the North Carolina Department of Health and Human Services has the authority “[t]o develop and carry out reasonable health programs that may be necessary for the protection and promotion of the public health and the control of diseases.”<sup>57</sup> If the state Division of Public Health undertakes disease control measures that are not explicitly authorized by statute or regulation, it is debatable whether general authority such as this would be sufficient to meet the standard specified in the privacy regulation.

Consider the following hypotheticals:

- A provision of state law requires a covered entity to report a disease.
  - Not preempted: The provision would not be contrary to the privacy regulation because the disclosure is “required by law.”
  
- A provision of state law authorizes – but does not require – a covered entity to report a disease to a public health authority.
  - Not preempted: The provision would not be contrary to the privacy regulation because disclosure to a public health authority is permitted without individual permission pursuant to the public health exception.
  
- A provision of state law authorizes a covered entity to report a disease to an entity other than a public health authority.
  - Not preempted: The provision would be contrary to the privacy regulation and therefore preempted by the general rule. The provision of law would ultimately be saved from preemption by the public health carve-out because the carve-out does not limit disclosures to “public health authorities.”

Given the breadth of this one category of the public health exception, it is difficult to imagine a public health law that would not survive a preemption analysis. In order to be preempted, the law would, for example, need to authorize a use or disclosure that is *not* for the purpose of preventing or controlling disease, injury or disability and is *not* included in the public health carve-out. Such a law is unlikely to exist because almost any health-related use or disclosure, including those for private research or marketing purposes, can arguably be justified as being for the purpose of preventing or controlling disease, injury or disability. Although the preemption analysis is virtually always going to leave the public health law intact, it is important that covered entities undertake a thorough analysis for each state law rather than simply assume that all public health disclosures are permitted. Such diligence will ensure that the entity has made every effort to understand its legal responsibilities in the event that it is ever confronted with an enforcement action under HIPAA.

---

<sup>57</sup> N.C. GEN. STAT. § 130A-5(3).

### *C. Health plan carve-out*

The privacy regulation specifically carves-out any provision of state law that “requires a health plan to report, or to 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.”<sup>58</sup> Because this carve-out applies only to laws that “require” certain disclosures, it is not likely to come into play in any preemption analysis because the privacy regulation already permits any disclosure that is otherwise “required by law.” In comparing the flexible language of the public health carve-out (“provides for”) with the health plan carve-out (“requires”), it seems clear that the latter was intended to be narrower in scope.

If a state law simply “authorizes” rather than “requires” health plans to provide this type of access to PHI, such a law may not be contrary to the privacy regulation because it could be permitted under the oversight exception. The oversight exception permits covered entities to disclose PHI to a health oversight agency for oversight activities authorized by law.<sup>59</sup> “Oversight activities” include:

- Audits;
- Civil, administrative or criminal investigations;
- Licensure or disciplinary actions;
- Civil, administrative or criminal proceedings or actions; or
- Other activities necessary for the appropriate oversight of:
  - The health care system;
  - Government benefit programs for which health information is relevant to beneficiary eligibility;
  - Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
  - Entities subject to civil rights laws for which health information is necessary for determining compliance.<sup>60</sup>

---

<sup>58</sup> 45 C.F.R. § 160.203(d).

<sup>59</sup> *Id.* at § 164.512(d)(1). A “health oversight agency” is broadly defined as “an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe... that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.” *Id.* at § 164.501.

<sup>60</sup> *Id.* at § 164.512(d)(1). “Oversight activities” do not include investigations or other activities “in which the individual is the subject of the investigation or activity” unless the investigation or activity arises out of and is directly related to the receipt of health care, a claim for public benefits related to health, or qualification for, or receipt of, public benefits or services when the patient’s health is integral to the claim. *Id.* at § 164.512(d)(2). “Oversight activities” will situations where a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health. *Id.* at § 164.512(d)(2).

If the use or disclosure authorized by the law does not fall within the oversight exception, the last option available for leaving the law intact would be to submit a request to the Secretary of DHHS for a determination that the law is “excepted” from preemption (see discussion below).

#### ***D. Secretarial determinations***

The final category of exemptions to the preemption provision will only come into play if a person or entity requests an “exception” and the Secretary of DHHS affirmatively grants the request.<sup>61</sup> Specifically, a provision of state law will not be preempted if the Secretary makes a determination that the provision is necessary:

- To prevent fraud and abuse related to the provision of or payment for health care;<sup>62</sup>
- To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;<sup>63</sup>
- For State reporting on health care delivery or costs;<sup>64</sup> or
- For purposes of serving a compelling need related to public health, safety or welfare, and the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served.<sup>65</sup>

In addition, a law will not be preempted if the Secretary determines that the provision has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing or other control of any controlled substance (as defined in 21 U.S.C. § 802) or that is deemed a controlled substance by state law.

The first three categories overlap in large part with the oversight exception. Considering the breadth of the oversight exception, it would be surprising if any law relating to fraud and abuse, health insurance regulation or reporting on health delivery or costs did not fall within one of the categories identified in the oversight exception, particularly given the “catch-all” of “other activities necessary for the appropriate oversight of the health care system.” Therefore, it is

---

<sup>61</sup> As explained above, this paper uses the terms “exemption” to refer to the provisions in 45 C.F.R. § 160.203 that effectively exempt a law from preemption that would otherwise be preempted under the general rule of preemption and the term “exception” to refer to those categories of uses and disclosures in 45 C.F.R. § 164.512 that are permitted under the privacy rule as an exception to the general rules. *See discussion, supra* note 6. In the text of the privacy regulation, however, DHHS uses the term “exception” to refer to the categories of laws subject to Secretarial determinations. From this point forward, this paper avoids the use of the term “exception” in this context.

<sup>62</sup> 45 C.F.R. § 160.203(a)(1)(i). *See also* 42 U.S.C.A. § 1320d-7(a)(2)(A)(i)(I) (West Supp. 2001) (providing that the exception is for laws “necessary...to prevent fraud and abuse”).

<sup>63</sup> 45 C.F.R. § 160.203(a)(1)(ii). *See also* 42 U.S.C.A. § 1320d-7(a)(2)(A)(i)(II) (providing that the exception is for laws “necessary ...to ensure appropriated State regulation of insurance and health plans”).

<sup>64</sup> 45 C.F.R. § 160.203(a)(1)(iii). *See also* 42 U.S.C.A. § 1320d-7(a)(2)(A)(i)(III) (using the same language as the regulation).

<sup>65</sup> 45 C.F.R. § 160.203(a)(1)(iv). The second half of this analysis – “...the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served” – only applies with respect to requirements of the privacy regulation. *See id.*

unlikely that such laws will be “contrary” to the privacy regulation thereby triggering a request for a Secretarial determination.

The fourth category – laws serving a compelling need related to public health, safety or welfare – represents DHHS’s interpretation of the extremely general statutory language permitting Secretarial determinations for laws “necessary...for other purposes.”<sup>66</sup> The agency explained: “The scope of the statutory criteria is ambiguous, but they could be read so broadly as to largely swallow the federal protections. We do not think that this was Congress’s intent.”<sup>67</sup> This category may overlap with a few different exceptions embedded in the privacy regulation. For example, a law falling in this category could also fall within the exception for public health or the exception for uses and disclosures necessary to avert a serious threat to health and safety.<sup>68</sup> Each of these exceptions, however, is tailored to meet fairly specific goals while the preemption exemption is much more general in scope. One part of the serious threat exception, for example, is limited to serious and “imminent” threats to public health or safety.<sup>69</sup> A state could have a law in place that authorizes disclosures related to certain non-imminent threats to public safety. In such case, if the disclosure is not otherwise permitted by the privacy regulation (e.g., the public health exception), it would be necessary to request a Secretarial determination.

The controlled substances provision was significantly expanded from the statutory language and from the proposed regulation – both of which simply referred to laws that “address[] controlled substances.” DHHS indicated that the clarifying language builds on existing statutes and regulations and “delineates the area within which the government traditionally regulates controlled substances, both civilly and criminally....” This provision does not appear to directly overlap with any of the exceptions in the privacy regulation, although it is conceivable that some controlled substance laws could intersect with the law enforcement, judicial and administrative proceedings or serious and imminent threat exceptions.

Once states and covered entities have completed a comprehensive preemption analysis, it is possible – although unlikely – that they will have identified state laws that will not survive preemption without such a determination. If so, they must evaluate the need for or significance of the state law and determine whether to submit a request for a Secretarial determination. It is important to remember that the request does not “stop the clock” in any way. After submitting a request after the compliance date has already passed, a covered entity will still need to comply with the state law until the Secretary reaches a conclusion. DHHS did not provide an outside timeframe for coming to a decision but simply stated that it “will undertake to process ... requests as expeditiously as possible....”<sup>70</sup> Once a decision is reached, the agency intends “to publish notice of ... determinations on a periodic basis in the Federal register [and] consider

---

<sup>66</sup> 42 U.S.C.A. § 1320d-7(a)(2)(A)(i)(IV).

<sup>67</sup> Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,585 (Dec. 28, 2000).

<sup>68</sup> See, e.g., 45 C.F.R. §§ 164.512(b) (public health); 164.512(j) (necessary to avert a serious threat to health or safety)

<sup>69</sup> 45 C.F.R. § 164.512(j)(1)(i)(A).

<sup>70</sup> Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,584-85 (Dec. 28, 2000).

other avenues of making such decisions publicly available ....”<sup>71</sup> Covered entities and their advisors will then be faced with the tedious task of monitoring these determinations for every state in which they do business.

### III. NCHICA preemption analysis

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a privately funded, nonprofit organization that actively promotes the advancement and integration of information technology into the healthcare industry. The NCHICA Board of Directors established several Focus Groups that are populated with member-affiliated and other individuals with an interest in particular NCHICA-related information or activities. The Privacy and Confidentiality Focus Group is further subdivided into several “work groups.”

One of these work groups – the State Law Work Group – assumed responsibility for identifying and reviewing all state statutes that may be affected (or preempted) by the privacy regulation. The analysis is now publicly available on NCHICA’s website<sup>72</sup> and is intended to provide guidance to attorneys and compliance officers in interpreting covered entities’ legal obligations under North Carolina law. Several sample pages of the analysis are included as an attachment to this paper.

The goal of the Work Group’s analysis was to identify and analyze all North Carolina statutes relating to use and disclosure of PHI. Due to limitations in time and resources, the Work Group limited the scope of its work to state statutes only – it did not review any federal laws (other than HIPAA), state regulations or court decisions. In addition, the Work Group limited the analysis to only those statutes that relate to use and disclosure of health information, excluding, for example, state statutes addressing individual access to medical records.

Group members first identified and summarized relevant statutes and then cross-walked the statutes to the relevant provisions of the privacy regulation.<sup>73</sup> In order to make the analysis as straightforward as possible and to comply with the requirement that the analysis be conducted on a provision-by-provision basis, the Work Group divided the more complex state statutes into

---

<sup>71</sup> *Id.* at 82, 584. This is certainly an improvement over the proposed regulation, which only required DHHS to publish determinations on an annual basis. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 60,051 (proposed Nov. 3, 1999) (proposed to be codified at 45 C.F.R. § 160.204(a)(8)).

<sup>72</sup> NCHICA State Law Work Group, *Analysis of the HIPAA Privacy Rule and Selected North Carolina Statutes* available at <<http://www.nchica.org/HIPAA/Samples/Portal.asp>>

<sup>73</sup> Because some of the statutes are summarized, the background material accompanying the analysis advises readers not to rely on the summary but rather consult the original statutory language when conducting an independent legal review. See NCHICA State Law Work Group, *Analysis of the HIPAA Privacy Rule and Selected North Carolina Statutes: Background and Explanation 3*, available at <<http://www.nchica.org/HIPAA/Samples/statutesintro.pdf>>

provisions. For example, one statute provides (in general) that nursing home patient records are confidential and written consent is required to release them except:

- To family;
- For patient transfer purposes;
- When release is required by law; or
- When release is required by a third party payment contract.<sup>74</sup>

Each of these four permitted disclosures intersects with a different requirement of the privacy regulation. In this instance, the Work Group divided the statute into four different provisions and compared each provision to a requirement of the privacy regulation.

The primary problem with this approach is that the reader is not able to review the statute as a whole. Often, reviewing the entire statute is necessary to fully comprehend its purpose and to interpret it appropriately. Therefore, the Work Group recommended that readers should always consult the full text of the statute in conjunction with the preemption analysis. Another challenge using this approach is pairing the state statute with a single requirement of the privacy regulation. In many cases, each statute or statutory provision intersects with more than one requirement of the regulation. The Work Group debated whether it should:

- compare each state statutory provision to each relevant requirement of the privacy regulation independently; or
- select the single requirement of the privacy regulation that was most relevant to the state statutory provision and draw the comparison.

While the first approach would likely be the most thorough, the Work Group concluded that it would be both confusing and unwieldy to conduct each analysis independently. Therefore, in the final analysis, the statutes are generally paired with what the Work Group identified as the most relevant section of the regulation.

Once the state statutes were divided up and paired with a section of the privacy regulation, the Work Group then analyzed the two laws to determine whether and how the state statute might be affected by the privacy regulation. In deciding on the presentation of our analysis, we first considered the type and amount of information that would be most helpful to our audience and second we evaluated what kinds of conclusions we were willing to reach regarding preemption. On the first issue, we agreed that attorneys and covered entities would be relying upon this analysis as a starting point for their own preemption analysis; they would not be relying upon our conclusions in isolation. Therefore, we decided that the final product should provide some degree of narrative explanation of our analysis and conclusions. We recognized that some readers may not agree with our conclusions and therefore we wanted to provide them with the opportunity to review our assumptions and interpretations and reach their own conclusions.

---

<sup>74</sup> N.C. GEN. STAT. § 131E-117(5) (1999).

The second issue – our willingness to reach conclusions regarding preemption – was a significant concern throughout the analytical process. Several group members wanted to reach definitive conclusions in our analysis such as “preempted” or “contrary, but exempted from preemption.” They argued that in order to be helpful to readers, the analysis must reach final conclusions. Some group members were reluctant to take this approach. Some of these members opposed the approach because of the risk of potential impact on clients of the group members in the future. For example, if the final analysis concluded that a state statutory provision was “preempted,” a group member could find herself arguing the opposite conclusion on behalf of a client months or years later. Other members opposed the approach because the scope of our analysis was limited only to statutes, arguing that it was premature to reach such conclusions without fully researching applicable regulations and caselaw.

After discussing the issue in detail, the Work Group arrived at a compromise. We agreed that conclusions of some kind would be helpful but elected to use terminology that did not appear to reach legal conclusions. Therefore, we avoided terms used in the privacy regulation such as “contrary” and “preempted.” Rather we adopted the following five-tiered classification system:

- “Consistent” indicates that the state statutory provision does not appear to directly conflict with the privacy regulation. In other words, covered entities will likely be required to comply with both laws.
- “Inconsistent” indicates that the state statutory provision and the privacy regulation appear to be in direct conflict. This term does not necessarily mean “contrary to” because in some instances it may be possible to comply with both laws. Careful legal review is necessary to determine which provision – the state law or the privacy regulation (or perhaps both) – will remain in effect.
- “Consistent in part” indicates that the state statutory provision and the privacy regulation appear to be consistent in part and inconsistent in part.
- “Further analysis required” indicates that the Work Group could not reach a conclusion as to whether the two laws are consistent and that further information and/or analysis is required. Many of the state statutory provisions fall within this category but for several different reasons. In some cases, for example, the statute is not clear on its face while in others, the conclusion will be different depending on the specific circumstances. The narrative analysis accompanying the conclusion attempts to provide guidance as to why further analysis is necessary.
- “Beyond scope” indicates that the state statute does not appear to intersect with the privacy regulation. For example, the statute may relate only to a non-covered entity (e.g., Department of Insurance). The Work Group obviously did not include all statutes that are beyond the scope, only those that deserved particular consideration.

After finalizing our analysis and conclusions, we debated how best to present the vast amount of information. We concluded that readers are likely to have different needs and expectations regarding the material and therefore we should present the information in a variety

of different formats to ensure flexibility and usability. We collected all of the information in a Microsoft Word table with columns for:

- State statutory provision (cites);
- Summary of state statutory provision;
- Key privacy regulation requirement (cites);
- Narrative analysis;
- Conclusion; and
- Cross-references to other relevant privacy regulation requirements (cites).

By presenting the analysis in table format, we created a comprehensible and versatile tool.<sup>75</sup> On NCHICA's website, we have published three different versions of the table – one sorted by state statutory provision, one sorted by privacy regulation requirement and one sorted by conclusion. Depending on the circumstances, one version may be more helpful to the reader than another. In addition, the tool is also searchable so that a reader can enter a citation or key word and identify the relevant section(s) of the analysis.

There is still, of course, work to be done. For example, the Work Group is currently considering whether to expand the analysis to incorporate regulations and case law and also whether and how we will be able to update the analysis on a regular basis. In order to be of use to covered entities and their advisors, this type of global preemption analysis must be approached as a long-term, rigorous project and the analysts must be committed to sustaining the project into the future. Because the NCHICA product is publicly available, covered entities may take the initiative by maintaining and updating the analysis on a regular basis.

The Work Group's approach to a preemption analysis, as described above, is only one option to consider when undertaking a new analysis. Many consultants, law firms and attorneys have completed or are in the process of completing preemption analyses and most have developed their own unique approaches and formats to meet their particular needs. The only thing that they will all likely have in common is complexity. HIPAA preemption is intricate and complicated and covered entities, attorneys, compliance officers and courts will be struggling with its interpretation and application for years to come.

---

<sup>75</sup> We are also in the process of evaluating whether other formats – such as Microsoft Access – would help to make this tool even more user-friendly.