REQUESTING PROTECTED HEALTH INFORMATION FROM MILITARY MEDICAL TREATMENT FACILITIES:
THE PRIVACY RULE MEETS THE PRIVACY ACT

BY MAJOR CHARLES G. KELS, USAF, ESQ.

Under the privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act (the HIPAA Privacy Rule),[1] organizations subject to the rule ("covered entities") must take special precautions in order to safeguard patients' protected health information (PHI). These heightened standards applicable to the healthcare industry did not supplant or modify existing federal law and thereby do not absolve covered entities from their duty to comply with other privacy standards.[2]

In particular, covered entities within federal agencies must comply with both the HIPAA Privacy Rule and the Privacy Act.[3] Satisfying the requirements of one does not guarantee compliance with the other.[4] In the majority of cases, the Privacy Rule proves more restrictive than the Privacy Act in regulating the use and disclosure of PHI by covered entities.[5] However, this is not always the case. One notable exception in the military context involves the release of PHI outside Department of Defense (DOD) channels in response to a subpoena or court order.

Satisfactory Assurances

The Privacy Rule provides that in the context of any judicial or administrative proceeding, covered entities may disclose PHI "…in response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal," if certain conditions are met.[6] Essentially, those conditions amount to "satisfactory assurances" – provided by the requesting party to the covered entity – that the requestor has either provided notice of the request to the individual who is the subject of the PHI sought or has made reasonable efforts to secure a qualified protective order preventing the PHI from being further disclosed outside the particular litigation or proceeding in question.[7]

In light of HIPAA's relative permissiveness regarding this aspect of disclosing PHI in the course of judicial and administrative proceedings, attorneys involved in various stages of litigation will oftentimes subpoena records containing PHI from military medical treatment facilities (MTFs). Understandably, the requesting litigators typically cite as their authority the Federal Rules of Civil Procedure, which empower attorneys to issue and sign subpoenas as officers of the court.[8]

continued on page 22

THE PRIVACY RULE MEETS THE PRIVACY ACT

continued from page 21

So far as HIPAA is concerned, such a subpoena duces tecum may be more than enough to permit the covered entity to disclose PHI to the issuer without the patient's authorization. However, as noted above, the Privacy Rule is not the only player in federal law when it comes to disclosing records containing personal information to outside entities. Specifically, medical, dental, mental health and other healthcare-related documents maintained by the DOD comprise government systems of records subject to the Privacy Act. As a result, PHI from such records "… may only be disclosed if disclosure is authorized under both" the HIPAA Privacy Rule and the Privacy Act.[9]

Court Orders

The Privacy Act enables agencies to disclose records without the consent of the individual to whom they pertain "…pursuant to the order of a court of competent jurisdiction."[10] The DOD's regulatory implementation of this provision interprets such an order to be, at a minimum, one specifically "signed by a judge."[11]

The Defense Privacy Board, which is charged with oversight responsibility for implementing the DOD Privacy Program,[12] has opined that "…to allow nonconsensual disclosure pursuant to a subpoena… would permit disclosure of protected records at the whim of any litigant, whether prosecutor, criminal defendant, or civil litigant." As such, disclosure of records under the court order exception "…requires that the court specifically order disclosure."[13]

In terms of what constitutes "the court," and an order thereof, the Defense Privacy Board has further determined that "…a subpoena signed by a clerk of a federal or state court, without specific approval of the court [i.e., judge] itself," is not sufficient for purposes of nonconsensual disclosures under the Privacy Act. "Even though a subpoena signed by a clerk of the court is issued in the name of the court and carries with it the threat of contempt to those who ignore it,"

the board noted that "…there is no guarantee that it is based upon a careful consideration of the competing interests of the litigant and the individual who is the subject of the record."[14]

Leaving aside the more complex question of what amounts to "competent jurisdiction" when state courts order nonparty federal agencies to disclose information,[15] it is at least clear that the term "order of a court" under the Privacy Act excludes routinely issued subpoenas by attorneys or court clerks that have not been "specifically approved" by a judge.[16] It is also settled law that federal agencies retain the discretion to prescribe regulations, consistent with existing statutes, dictating when official records under their control may or may not be released by agency representatives.[17]

PHI as Privacy Act Records

As federal medical facilities, military clinics and hospitals are both covered entities subject to HIPAA, as well as components of agencies subject to the Privacy Act. Medical documents maintained by MTFs are oftentimes similarly dual-designated as PHI and Privacy Act-protected official records.

The intricacies and relative newness of the Privacy Rule have conditioned many medical entities and those that interact with them to view HIPAA as the sole factor regulating the flow of medical information. More often than not, applying the Privacy Rule to potential health record disclosures may lead to the right answer. These favorable odds, however, do not obviate the need for covered entities to comply with other applicable law.

In the case of MTFs, local law offices may find themselves frustrated when subpoenas that apparently comply with HIPAA are met with requests for clarification or additional documentation. The reason for such responses is that DOD components have generally been instructed to "…release documents subject to the Privacy Act only with the consent of the individual or under a court order or subpoena specifically signed by a judge of a court of competent

continued on page 24

THE PRIVACY RULE MEETS THE PRIVACY ACT

continued from page 23

jurisdiction."[18] In this sense, the fact that such records may contain PHI is immaterial; what drives the heightened standard is their status as official DOD records containing information about individuals and maintained in a system of records.

Obtaining a HIPAA-compliant authorization from the patient for the disclosure of PHI to the requestor will typically satisfy both the "valid authorization" requirement under the Privacy Rule,[19] as well as the "written consent" requirement under the Privacy Act.[20] In this case, the subpoena duces tecum may not even be necessary to ensure compliance by the MTF, since the attorney's request accompanied by the patient's authorization will speak for itself. On the other hand, in the absence of such written consent by the subject of the records sought, an attorney-issued subpoena duces tecum will likely prove ineffective unless personally signed by the appropriate judge. ■

MAJOR CHARLES G. KELS, a judge advocate in the U.S. Air Force, serves as the Medical Law Consultant at the Mike O'Callaghan Federal Hospital on Nellis Air Force Base. Opinions expressed in this article are those of the author alone and do not necessarily reflect those of the Air Force or Defense Department.

1 Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160, 164 (2002).
2 With respect to state law, the Privacy Rule generally preempts "contrary" provisions. Exceptions to preemption exist for state laws that provide more robust privacy protections or that establish certain public health or health plan reporting requirements. See 45 C.F.R. § 160.203.
3 Privacy Act of 1974, 5 U.S.C. § 552a (2000).
4 U.S. Dep't of Defense, Reg. 6025.18, DoD Health Information Privacy Regulation at ¶ C2.6 (24 Jan. 2003) [hereinafter DoD Reg. 6025.18].
5 U.S. Dep't of Defense, Reg. 5400.11, DoD Privacy Program at ¶ C3.1.6.1 (14 May 2007) [hereinafter DoD Reg. 5400.11].
6 DoD Reg. 6025.18, ¶ C7.5.1.2.
7 Id., ¶¶ C7.5.1.2.1, C7.5.1.2.2.
8 Fed. R. Civ. P. 45(a)(3).
9 DoD Reg. 5400.11, ¶ C4.4.2.
10 5 U.S.C. § 552a(b)(11).
11 DoD Reg. 5400.11, ¶ C4.2.11.1.
12 U.S. Dep't of Defense, Dir. 5400.11, DoD Privacy Program at ¶ E4.1.2.1 (8 May 2007).
13 Defense Privacy Board, Advisory Op. 34, Definition of "Order of a Court of Competent Jurisdiction."
14 Id.
15 See *Bosaw v. NTEU,* 887 F. Supp. 1199 (S.D. Ind. 1995); *Boron Oil Co. v. Downie,* 873 F.2d 67 (4th Cir. 1989).
16 *Doe v. DiGenova,* 779 F.2d 74, 77-85 (D.C. Cir. 1985).
17 *Touhy v. Ragen,* 340 U.S. 462 (1951).
18 U.S. Dep't of Air Force, Instr. 51-301, Civil Litigation at ¶ 9.5.4 (1 Jul. 2002).
19 DoD Reg. 6025.18, ¶ C5.2.1.
20 DoD Reg. 5400.11, ¶ C4.1.3.2.