Enforcing HIPAA Administrative Simplification: Dispassionate Enforcement or Compassionate Prosecution?

By: Alan S. Goldberg, JD, LLM*
Goulston & Storrs, Boston, MA, Washington, DC, and London, UK
Past President, American Health Lawyers Association &
Moderator, AHLA HIT listserv
Adjunct Professor of Law, University of Maryland School of Law &
Suffolk University Law School
Webmaster, http://www.healthlawyer.com (sm)
[*Not admitted in DC]
May 7, 2002

The Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, will revolutionize how health information is, and patients are, treated privacy-wise, security-wise, and otherwise. The transactions and data codes sets rule requirements under HIPAA, as well as privacy and security, will be included in the enforcement part of HIPAA. Because of the many changes in health care delivery that HIPAA will require, lots of anxiety has been created about penalties. Certainly few areas of the HIPAA law are more important than the enforcement provisions.

Covered entities will need to address their de facto enforcement obligations with respect to business associates in order to avoid governmental enforcement against covered entities. But a careful reading of the law should provide comfort and encouragement that notwithstanding the hype, the enforcement procedure likely will not be so bad after all. Covered entities and business associates who study and learn can be prepared to meet the challenges of the HIPAA law. Note also that not discussed further below are possible state law enforcement activities based upon HIPAA and the new national standard set by HIPAA and likely to be embraced by state Attorneys General and judges in state courts in evaluating privacy and security compliance in health care.

In fact, the civil enforcement provisions of the HIPAA law evidence a Congressional mandate that civil sanctions – that is, monetary fines -- under HIPAA should be imposed leniently and in a way that will encourage compliance and not make covered entities feel as if they are being persecuted for inadvertent violations of the HIPAA law.

Although the Office for Civil Rights, to which the Department of Health and Human Services delegated the HIPAA enforcement responsibility, has not promulgated a proposed

enforcement rule, the HIPAA law provides a clear indication of Congressional intent regarding how enforcement should proceed. It can therefore be expected that the OCR enforcement rule will mirror the HIPAA law enforcement provisions and the enforcement language already set forth in the HIPAA final privacy rule.

These civil penalty enforcement provisions of the HIPAA law begin as follows:

"GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

SEC. 1176. (a) GENERAL PENALTY.--
(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
"(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A."

Thus the magnitude of a penalty assessment surely can add up, particularly for repeated transactional defaults. But Congress provided a generous and unusual opportunity in HIPAA to prevent, to deflect and possibly to avoid any penalty (***emphasis supplied***):

"(b) LIMITATIONS.--
"(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may ***not*** be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177 [namely, "HIPAA For Crooks": the criminal provisions].
(2) NONCOMPLIANCE NOT DISCOVERED.--A penalty may ***not*** be imposed under subsection (a) with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the penalty did ***not*** know, and by exercising reasonable diligence would ***not*** have known, that such person violated the provision."

So, if a covered entity is able to satisfy the Office for Civil Rights that the covered entity did not know, and by exercising reasonable diligence would not have known, of a violation of the HIPAA law, no penalty may be imposed under (a).

And even if the covered entity did know, or by exercising reasonable diligence would have known that the covered entity would be a violator (***emphasis supplied***), the possibility of deflecting a penalty would still exist:

"(3) FAILURES DUE TO REASONABLE CAUSE.--
(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may ***not*** be imposed under subsection (a) if--
"(i) the failure to comply was due to reasonable cause and ***not*** to willful neglect; and
"(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred."

Accordingly, no penalty would be imposed if a failure to comply with the HIPAA law – which failure a covered entity knew would be a failure – was due to reasonable cause and not to willful neglect, and the failure is corrected within thirty days after the first date on which the covered entity knew, or by exercising reasonable diligence could have known (whether or not, it appears, there was actual knowledge on the part of the covered entity) that the failure occurred. So, after receiving a complaint from the Office for Civil Rights, the possibility exists that a covered entity could promptly correct the problem and thereby avoid any penalties.

And more opportunities will exist to have penalties abated (***emphasis supplied***):

"(B) EXTENSION OF PERIOD.--
(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) ***may be extended*** as determined appropriate by the Secretary based on the nature and extent of the failure to comply.
(ii) ASSISTANCE.--If the Secretary determines that a person failed to comply because the person was ***unable*** to comply, the Secretary may provide ***technical assistance*** to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary."

So, the thirty-day correction and cure period could be extended by the Office for Civil Rights and during that additional period, the Office for Civil Rights could provide technical assistance. This could mean that the violation would be able to be corrected without any penalty being imposed by the OCR.

And finally, a penalty may be reduced (***emphasis supplied***):

"(4) REDUCTION.--In the case of a failure to comply which is due to ***reasonable cause*** and ***not*** to willful neglect, any penalty under subsection (a) that is ***not*** entirely waived under paragraph (3) ***may be waived*** to the extent that the payment of such penalty would be excessive relative to the compliance failure involved."

Thus even if is a penalty was going to be imposed, the Office for Civil Rights could reduce the penalty if deemed to be "excessive." As this review of the enforcement part of the HIPAA law indicates, Congress would seem to have intended the civil enforcement procedure to

be a conciliatory and encouraging process and not a process of persecution, because there are so many avenues for "mercy" to be shown by OCR.

Although we have not yet seen the preliminary rule that is being prepared by the Office for Civil Rights right now, we can hope that those working on the enforcement rule adhere to what Congress said in HIPAA.

We don't know what will be done regarding the criminal penalties under HIPAA. Perhaps the Department of Justice will offer some guidance regarding what "knowing" and what "intent" will be viewed by the DOJ as meaning, under the HIPAA statute, when HIPAA criminal prosecutions occur. In any event, the criminal part of HIPAA penalties is as follows:

"WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

SEC. 1177. (a) OFFENSE.--A person who knowingly and in violation of this part--
(1) uses or causes to be used a unique health identifier;
(2) obtains individually identifiable health information relating to an individual; or
(3) discloses individually identifiable health information to another person,
shall be punished as provided in subsection (b).
(b) PENALTIES.--A person described in subsection (a) shall--
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."

Questions raised by "HIPAA for crooks" include what "knowingly" will be found to mean under HIPAA; what "intent" will be found to mean under HIPAA; whether the confusion that arose under the anti-fraud and anti-kickback laws in health care relative to "the sole purpose" or "only one of several purposes" will find its way into HIPAA criminal enforcement; how the law of false claims, conspiracy and obstruction of justice and other such laws will relate to HIPAA enforcement; and how the Office for Civil Rights and the Department of Justice will determine which alleged violations are treated as civil violations and which alleged violations are treated as criminal violations. Surely all covered entities will want to have corporate compliance programs established and maintained in a manner consistent with the Federal Sentencing Guidelines, in order to endeavor either to avoid or to reduce the severity of criminal penalties.

With all the foregoing in mind, certainly the sooner covered entities begin the process of getting ready for HIPAA enforcement, the better. The key to avoiding penalties will be having

policies and procedures in place that evidence a good faith intention to endeavor to comply with the HIPAA law. A summary of what to do to endeavor to avoid civil HIPAA penalties follows:

- Use reasonable diligence to know as much as you can about HIPAA
- Establish policies that evidence a reasonable approach to prevention
- Don't be neglectful, willfully or otherwise, or reckless
- Try to cure breaches within 30 days
- Ask for an extension if necessary
- Seek technical advice if necessary
- Be sure to document everything done in furtherance of HIPAA corporate compliance, preparation, implementation, and education and training.

Ignorance will not be bliss, and avoidance will not be blissful. Instead, the only way to prepare for HIPAA is the old fashioned way: study it and learn it. Patients will expect no less, and covered entities surely will want to do even more to assure that their patients receive both quality care and the privacy and security protections, and the benefits of the transactions and data code sets standardization, that patients deserve and, under the law, are going to be required.

ASG/tt