Enforcing HIPAA Administrative Simplification: Reactive Enforcement or Compassionate Persecution?

By: Alan S. Goldberg, JD, LLM
Goulston & Storrs,Washington, DC, Boston, MA 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)
Co-Chair, National HIPAA SUMMIT; Chair, ABA Health Law Section HIPAA Preemption Project
December, 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 with respect to breach of contract, negligence and class action litigation.

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 privacy 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. CMS will enforce the transactions and security rules.

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 and CMS (but not for the Department of Justice).

Although we have not yet seen the preliminary rules that are being prepared by the Office for Civil Rights and CMS now, we can hope that those working on the enforcement rules adhere to what Congress said in HIPAA. And regardless, the courts are bound to respect the HIPAA law.

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 "knowingly" and what "intent" will be viewed by the DOJ as meaning, under the HIPAA law, when HIPAA criminal prosecutions occur. In any event, the criminal part of HIPAA penalties 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, CMS and federal prosecutors 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

HIPAA ADMINISTRATIVE SIMPLIFICATION PRIVACY RULE CONTRARY & MORE STRINGENT STATE LAW PROJECT

The Health Law Section's eHealth and Privacy Interest Group is embarking on a new project and is looking for interested volunteers. The Interest Group is looking for volunteers to help compile a nationwide database of state privacy laws. The database will be available to anyone who needs the information to determine whether such laws are contrary to and/or more stringent than HIPAA's final privacy rule.

This project is necessary because under the Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act of 1996, and more particularly, Section 264(c)(2), stating: (2) PREEMPTION — A [privacy] regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation...," it will be necessary for "Covered Entities" and "Business Associates" and others to determine whether HIPAA privacy rule standards and requirements are contrary to and/or more stringent than applicable State law.

This need for state law determinations creates an enormous task and will require constant monitoring, analysis, and application of judgment. But perhaps the most difficult part of this task will be determining what the relevant State law (which includes constitutional, statutory and common law) will be for any analysis. It is here that our Project can be helpful. Unfortunately, we understand that the federal government does not have the resources available now to engage in such a project.

So, the Interest Group's approach will be to enlist the aid and support of lawyer-members of the American Bar Association's Health Law Section, as well as members of other Sections (such as the Science and Technology Section and the Business Law Section) interested in HIPAA. At least one volunteer, and more likely many volunteers, will be assigned for every state and in the four additional jurisdictions (the District of Columbia, the Commonwealth of Puerto Rico, Guam, and the U.S. Virgin Islands) for which such determinations must be made, in order to participate in preparing, maintaining and updating a database of relevant constitutional, statutory and common law.

The project intends to make maximum use of existing resources so that such database projects already underway by others for certain States and jurisdictions can be shared and enhanced. A leadership team of several lawyers would be appointed to serve as the liaison between each State and jurisdiction, and the leadership of our Interest Group project. The Interest Group intends to complete the project not later than the end of this year.

If you are looking for a way to make a professional contribution to how health care privacy will be maintained and enhanced by HIPAA and otherwise as part of your public service commitment as a member of the bar, this project is worthy of your consideration. There is a paucity of resources otherwise available for the information that the project will produce and maintain, and therefore this surely is an area in which the American Bar Association can assist our government, over two hundred eighty million patients, and those involved in the health care delivery system, in furtherance of the public interest.

For more information or to volunteer to be a part the project, contact Section Director Jill Peña at 312/988-5548 or e-mail her at jillpena@staff.abanet.org.

NOMINATION COMMITTEE

The Nominating Committee for the Section has been appointed. The Committee will consider nominees for Vice Chair, Secretary, Finance Officer, Delegate to the ABA House of Delegates, and two Council Members. The Nominating Committee will submit a report to Council. Elections will be held at the ABA Annual Meeting in August. The report of the Nominating Committee will be published on the Section web site (www.abanet.org/health) no later than June 21, 2002. The members of the Nominating Committee are:

- Robert L. Roth, Crowell & Moring, Washington, DC
- Patricia T. Meador, Kennedy Covington Lobdell & Hickman, Research Triangle Park, NC
- Christina M. Mireles, Crowell & Moring, Washington, DC

Contact Section Director Jill Peña at 312/988-5548 or jillpena@staff.abanet.org is you have any questions or comments.

goulston&storrs
counsellors at law

Resume of Alan S. Goldberg, JD, LLM

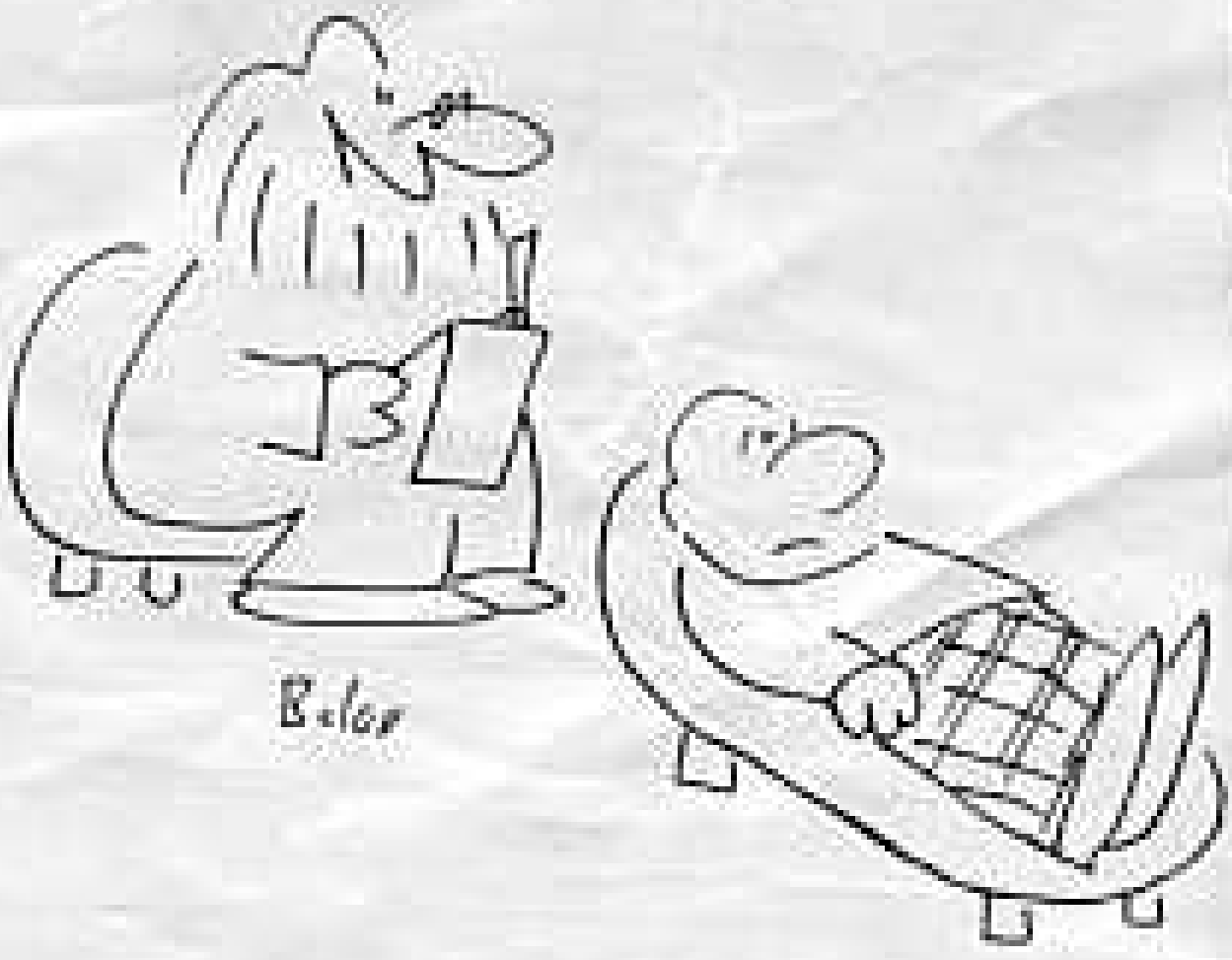
Alan S. Goldberg is a member of the bars of the District of Columbia, Massachusetts and Florida. Mr. Goldberg concentrates in the practice of business and administrative law including the delivery of health care and information technology. Goulston & Storrs provides creative solutions in the areas of real estate, taxation, estate planning, bankruptcy, health care and medical devices, litigation, and complex business transactions nationally, and internationally via a London, UK office.

Mr. Goldberg's introduction to health law occurred in the 1960s, during the dawning of the Medicare and Medicaid programs era as a judge advocate and prosecuting attorney in the United States Navy, and Mr. Goldberg was also involved in investigative actions relating to the USS Pueblo and the Sea-lab project. Mr. Goldberg joined Goulston & Storrs in 1967 upon graduation from Boston College Law School, where he was a member of the Law Review and received an academic scholarship, and as a Lecturer in Law presented a course in land finance. In 1978 Mr. Goldberg received an LL.M. (Taxation) from Boston University School of Law. Mr. Goldberg is an Adjunct Professor of Law at University of Maryland School of Law and Mr. Goldberg also taught at Boston's Suffolk University Law School. He is a a Past President of National Health Lawyers Association ('91-'92); served on its Board of Directors from 1981 to 1993; and served as an Internet advisor to the Health Lawyers Board. Mr. Goldberg received the National Health Lawyers Association David J. Greenburg Service Award in 1996.

Mr. Goldberg has published extensively on a broad range of health law, and many other legal issues and has frequently lectured for American Health Lawyers Association and slso for many bar and for other associations; the Massachusetts Hospital Association, Dental Society, Medical Society, and Long Term Care Foundation, the American Telemedicine Association, the Workgroup For Electronic Data Interchange, the Healthcare Information and Management Systems Society, and for governmental and other organizations and he participates in many national teleconferences as a moderator and a lecturer.

Mr. Goldberg was the moderator of the Health Law Forum computer on-line feature of CounselConnect; he is the Editor of a law and computer technology column entitled "The Computer Wizard" published by the American Bar Association's Business Law Section magazine "Business Law Today"; and he is the founding moderator of the American Health Lawyers Association Health Information and Technology Internet listserv. Mr. Goldberg has presented loss prevention seminars relating to technology issues to the membership of Attorneys' Liability Assurance Society. Among Mr. Goldberg's current interests are national and international challenges and opportunities involving the application of technology to the practice of law and medicine and to the delivery of healthcare, including issues involving the Internet, security and encryption, privacy and confidentiality, software licensing and devices, corporate compliance programs, and telemedicine. Mr. Goldberg has served as Vice Chair of the American Health Lawyers Association Health Information and Technology Practice Group, and Chair of the American Bar Association Health Law Section's e-Health & Privacy Interest Group; and he cochairs The National HIPAA Summit series of events and originated the HIPAA HERO® teaching methodology.

Mr. Goldberg is the Webmaster of ***http://www.healthlawyer.com***; and agoldberg@goulstorrs.com is his e-mail address and Mr. Goldberg is now resident in the Washington, DC office of Goulston & Storrs.



"Actually, according to the test results, your low self-esteem is right on the money."

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191

104th Congress

REVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

...

"Part C--Administrative Simplification

"Sec. 1176. General penalty for failure to comply with requirements and standards.

"Sec. 1177. Wrongful disclosure of individually identifiable health information.

"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.

"(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.

"(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.

"(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.

"(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.

"(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.

"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."