Cynthia Marcotte Stamer's
H.R. & BENEFITS E-NEWS

SMALL HEALTH PLANS HIPAA PRIVACY NOTICE REMINDER DUE APRIL 14; FIRST CRIMINAL HIPAA VERDICT HIGHLIGHTS IMPORTANCE OF APPROPRIATE HIPAA & OTHER DATA SECURITY PRACTICES

Tuesday, April 10, 2007

Employers and union sponsors and administrators of small health plans (those with annual receipts of $5 million or less) should take steps to ensure that their health plan meets its April 14, 2007 deadline for sending the reminder notices concerning their health plan's privacy practices required by the Health Insurance Portability & Accountability Act (HIPAA). Other health plans generally were required to provide such reminders by April 14, 2006.

The deadline for providing the required reminder coincides with the third anniversary of the HIPAA-imposed compliance deadline for small health plans to adopt and follow HIPAA-compliant policies ("Privacy Practices") governing the use, access and disclosure of certain individually identifiable personal health information ("PHI") created or received by or on behalf of the health plan. Based on the published guidance provided by OCR Frequently Asked Question (FAQ) 1065 and Privacy Regulation 164.520(c)(1) health plans can select among various options for satisfying the reminder notice requirement. Indeed, some health plans that include appropriate information in their annual enrollment information may already have fulfilled the reminder notice requirement through those materials. To avoid unintentionally violating the reminder notice requirement, however, health plans should not assume their health plan compliance. Rather, they should review their existing notices to confirm compliance with both the reminder notification requirement and otherwise applicable HIPAA mandates.

The requirement to provide a reminder notification about a health plan's Privacy Practices is part of the detailed and far-reaching requirements regulating the use, access, protection and disclosure of PHI that generally became effective for health plans, health care providers and health care clearinghouses on April 14, 2003. HIPAA generally requires that health plans provide reminder notifications of their Privacy Practices at least once every three years, beginning on the third anniversary of the health plan's initial deadline for compliance with HIPAA's privacy rules.

Health plans, other than small health plans, initially were required to distribute a Notice of Privacy Practices to subscribers and enrollees and otherwise comply with HIPAA's medical privacy rules by April 14, 2003. However, HIPAA delayed the initial deadline for small health plans to comply with HIPAA and first distribute their Notices of Privacy Practices until April 14, 2004. Consequently, small health plans have until April 14, 2007 to provide the required triennial reminder notice.

Since HIPAA originally took effect, the Department of Health & Human Services (HHS) has issued various guidance supplementing and clarifying its initially published final HIPAA regulations. In addition to specific technical guidance, this includes a final rule detailing the bases and procedures for imposing civil money penalties on health plans and other covered entities that violate any of the HIPAA Administrative Simplification Rules.

According to data reported in its 2006 Fiscal Year Budget, HHS has reported that it has received more than 10,000 complaints and HHS has identified HIPAA enforcement as a current agency priority.

Noncompliance with HIPAA's medical privacy mandates may subject health plans and other covered entities to substantial civil and/or criminal penalties. While HHS statistics reflect that most complaints to date have been resolved without the imposition of substantial civil or criminal penalties, the Justice Department's announcement earlier this year that it obtained the first criminal jury conviction for violation of the HIPAA privacy rules from a Florida jury on January 24, 2007 provides an important reminder that health plans and other health industry entities should not overlook the importance of maintaining HIPAA compliance and otherwise taking appropriate steps to protect the sensitive health and other personal information about participants and beneficiaries created or accessed by their health plan against improper use, access or disclosure.

In *U.S. v. Ferrer*, a Florida jury found defendant Fernando Ferrer, Jr. guilty of 1 count of wrongful disclosure of individually identifiable health information in violation of HIPAA, 5 counts of aggravated identity theft, 1 count of

© 2007 by Cynthia Marcotte Stamer, P.C. All rights reserved.

computer fraud, and 1 count of conspiring to defraud the United States.[1] Ferrer, the owner of a health claims administration company, misappropriated the personal data of more than 1,100 patients of the Cleveland Clinic through a Cleveland Clinic employee, Isis Machado. The misappropriated information included patients' names, birth dates, Social Security numbers, Medicare identification numbers and addresses. Ferrer and Machado used the misappropriated data to submit more than $7 million in fraudulent Medicare claims, with approximately $2.5 million paid to providers and suppliers. Machado, who was Ferrer's cousin, pled guilty on January 12, 2007 to conspiring with Ferrer to steal and misuse the data and testified against Ferrer at trial.

The *Ferrer* case demonstrates the risk health plans and other covered entities face under HIPAA and other federal criminal laws if they fail to take appropriate steps to protect sensitive data and information or fail to monitor and promptly address security breaches or other illegal acts by employees or other service providers. It also provides a cautionary reminder to employers that they and their employees may face prosecution under Federal law if members of their staff improperly use or access their health plan's protected health information. While HHS has announced that it generally will not pursue prosecution of employers sponsoring health plans for violations of HIPAA's privacy requirements, employers and others may face criminal and/or civil prosecution for wrongful use of this information under Federal or state identity theft, cyber crime and other laws. Therefore, all health plans and their sponsors should take appropriate steps to ensure that they have in effect, and properly administer appropriate practices to prevent and redress potential wrongful uses and disclosures of their health plan's PHI as well as other protected personal information.

These recent decisions, as well as the announcement by Texas Attorney General Abbott last week that he was filing suit against Radio Shack for allegedly failing to appropriately safeguard personal information collected by one of its retail stores in violation of a 2005 Texas identity theft statute, also illustrate that responsibility to protect sensitive data and take other appropriate actions to guard against identity theft or other cybercrimes are not restricted to covered entities under HIPAA. Rather, businesses and business leaders acting as employers or in other capacities can become subject to civil and/or criminal liability if their organizations fail to take appropriate steps to protect sensitive data, to regulate its use, and/or to redress breaches of these required safeguards.

Compliance with applicable notification risks generally is only a small part of this process. Health plans, employers, other businesses, and their leaders need to ensure that their organizations have implemented and are administering appropriate compliance programs to comply with these applicable regulations and manage liability exposures. In most instance, organizations affected by these regulations also need to conduct regular training and oversight to meet their compliance responsibilities and mitigate their liability risks.

Businesses and other organizations interested in learning more about what their organizations should do to manage their identity theft, data security and cybercrime risks and liabilities can find helpful information in a series of articles authored by Cynthia Marcotte Stamer. Ms. Stamer works extensively with health plan and other employee benefit and human resources clients, as well as health care, banking and financial services and other clients on developing appropriate data security, privacy, cybercrime and other internal control and risk management strategies. She also has authored numerous publications addressing compliance and risk management under HIPAA and other data security and cybercrime regulations, and other related employee benefits, human resources, privacy and corporate compliance matters including her articles on "Keeping Lists Within The Law" and "Establishing a Data-Protection Policy" recently published in the March and April, 2007 issues of Western Association News Magazine. She also is the author of "Chapter 35 -Medical Privacy" published in ERISA Litigation (BNA) (2006-2004); "Personal Identity Management" published in the May, 2005 issue of MD News; "Cybercrime and Identity Theft: Health Information Security Beyond HIPAA," published in the May, 2005 issue of ABA Health eSource; "Privacy and Securities Standards - A Brief Nutshell," published in the February, 2005 issue of the BNA Journal of Tax Management & Compensation; "Employers face new health plan privacy rules required by HIPAA," published in the February 13, 2004 issue of the Houston Business Journal and a plethora of other training programs and other materials. Many of these and other helpful materials are available for review under the Publications link at located http*://cynthiastamer.com/articles.asp* or by contacting Ms. Stamer via e-mail or telephone. She also regularly conducts training on these matters.

For specific information about your organization's specific responsibilities under HIPAA's privacy rules, the 2005 Texas identity theft law, HIPAA, or other relevant federal or state laws and regulations, please contact Ms. Stamer. We hope that this information is useful to you. If you have questions about your company's privacy and security risk and exposures, or other human resources, employee benefit or other operational risks or internal controls practices, or to request publications, information about upcoming programs, or other materials, please contact: Cynthia Marcotte Stamer, P.C., Member, Glast, Phillips & Murray, P.C., 2200 One Galleria Tower, 13355 Noel Road, LB 48,

[1] *U.S. v. Ferrer*, No. 06-cr-60261-JIC (Jan. 24, 2007).

© 2007 by Cynthia Marcotte Stamer, P.C. All rights reserved.

and Dallas, Texas 75240. Telephone (972) 419-7188. E-mail cstamer@gpm-law.com.

For other helpful resources and information about data security and HIPAA, employee benefits and human resources matters, go to CynthiaStamer.com or contact Ms. Stamer. If you or someone else you know would like to receive future Alerts or announcements about other developments, publications or programs, please be sure that we have your current contact information – including your preferred e-mail – by registering on our website at cynthiastamer.com or by providing that information to us via telephone, fax or e-mail using the above contact information.

IMPORTANT NOTICES REGARDING THIS COMMUNICATION

This publication is provided by Cynthia Marcotte Stamer, P.C. for general informational and educational purposes to clients and other interested persons. Neither its distribution to any party nor any statement or information it contains is intended to or shall be construed as establishing an attorney-client relationship or to constitute legal advice. Readers also are cautioned that the information in this publication may not apply to all situations. Consequently, readers must not rely upon this publication or information it contains as a substitute for competent individualized legal advice about the specific circumstances of the reader. If you have received this publication in error or do not wish to receive these in the future, please notify us of your preferences to the attention of Ms. Stamer via email, fax, regular mail or telephone.

REMINDER ABOUT ELECTRONIC COMMUNICATION SECURITY: E-mail and other electronic communication may not be secure unless appropriate encryption methods are used. Therefore, they may present heightened risks of security breaches of the communication. Electronic communications also generally are subject to discovery on the same terms as other communications. Please consider carefully these concerns before communicating by e-mail or other electronic means. If you wish for us to communicate with you by means other than e-mail or wish for us to arrange for encryption of our e-mail communications, please contact us at 972.419.7188.

IMPORTANT NOTICE REGARDING TRANSMISSIONS OF PROTECTED HEALTH INFORMATION: Protected Health Information (PHI) is individually identifiable health information. Any PHI contained in this e-mail is intended only for the intended recipient and is disseminated subject to the understanding that all requirements of HIPAA and other applicable laws for this disclosure have been met. If this communication contains PHI, you are receiving this information subject to the obligation to maintain it in a secure and confidential manner. Re-disclosure without additional consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties as described in state/federal law. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of this information is strictly prohibited. If you have received this message in error, please notify the sender immediately to arrange for return or destruction.

ANTISPAM NOTICE: Pursuant to the CAN-SPAM Act, this communication may be considered an advertisement or solicitation. If you would prefer not to receive future marketing and promotional mailings or to provide other directions about the tailoring of messages directed to your attention, please send an email with the word “unsubscribe” in its subject heading to cstamer@gpm-law.com or otherwise contact us via postal mail to Cynthia Marcotte Stamer, Member, Glast, Phillips, & Murray, P.C., 2200 One Galleria Tower, 13355 Noel Road, L.B. 48, Dallas, Texas, 75240, Attention: Cynthia Marcotte Stamer, P.C.

CIRCULAR 230 NOTICE: The following disclaimer is included to comply with and in response to U.S. Treasury Department Circular 230 Regulations. ANY STATEMENTS CONTAINED HEREIN ARE NOT INTENDED OR WRITTEN BY THE WRITER TO BE USED, AND NOTHING CONTAINED HEREIN CAN BE USED BY YOU OR ANY OTHER PERSON, FOR THE PURPOSE OF (1) AVOIDING PENALTIES THAT MAY BE IMPOSED UNDER FEDERAL TAX LAW, OR (2) PROMOTING, MARKETING OR RECOMMENDING TO ANOTHER PARTY ANY TAX-RELATED TRANSACTION OR MATTER ADDRESSED HEREIN.

© 2007 by Cynthia Marcotte Stamer, P.C. All rights reserved.