CCH Health Care Compliance LETTER

Volume 8, Issue 17 health.cch.com August 22, 2005

Submission of Articles. Requests for information about article submission guidelines should be sent directly to Andra Popa at popaa@cch.com.

Comments? Please direct any questions or comments regarding articles appearing in the newsletter to the e-mail address above.

For more information about the CCH Health Care Compliance Portfolio, please visit our online store at http://health.cch.com.

Ensuring compliance program effectiveness: Lessons learned from CMS pilot

by Catherine Hubbard, M.A., Contributing Editor

Based on preliminary observations of CMS' pilot program, there are a series of steps that compliance officers can take to ensure compliance program effectiveness, according to Lisa Eggleston, a member of CMS' program integrity group.

As part of CMS' effectiveness pilot, 16 facilities from six states opened their doors to the agency to help discover what makes a compliance program most effective. Based on preliminary observations, Eggleston shared, CMS has learned that it is important to achieve buy-in from the top. "It is so crucial to have buy-in from senior management," she said during a recent Health Care Compliance Association audio conference.

In addition, Eggleston said, the compliance officer's role is crucial, Eggleston. "The compliance officer should be known in the organization," she said, stressing the importance of ongoing communication with the coding and reimbursement directors and human resources. At many of the facilities Eggleston visited, the compliance officer was present at orientation and annual training, so that individuals knew the compliance officer. "Compliance officers have to establish good working relationships across multiple departments," she said. Also, they must have access to board members and the CEO to discuss compliance issues, she said. "The compliance officer should have free reign when it comes to those kinds of discussions," she said.

CMS also has learned that the culture of a hospital is very different from other organizations, such as health plans or other financial institutions that may also need to have a compliance plan, Eggleston said. "Getting the compliance message to staff members can be somewhat of a challenge," she said, noting that medical staff understandably focuses much more on the health of patients than on organizational issues.

Other observations include:

- Hospitals that have a corporate integrity agreement requirement understand how important an effective compliance program is, said Eggleston.
- Compliance officers may hold multiple positions, especially in smaller facilities, while larger health systems may have separate compliance officers for each facility who report to a corporate compliance officer.
- The effectiveness of the compliance officer may be based on the personality of the compliance officer. If the right person does not take a strong leadership role, then the result may be weak policies and procedures or weak audit plans, Eggleston cautioned.

continued on page 2

- Hospitals must be attentive to its use of software and data, Eggleston said, adding that it's important for all departments that rely on software as an integral part of its job to require human oversight of the systems.
- Different departments that are conducting audits should share results in order to avoid audit duplication. "Communication is key," Eggleston said, stressing the importance of an integrated auditing approach.
- In the future, Eggleston said, CMS wants to develop a strategy to encourage other health care provider types, regardless of size, to adopt compliance programs. CMS would like to consider expanding the scope of the project to include additional facilities and geographic locations, she added. "We would like to observe more facilities and we would like to go to other geographic locations" she said.

CCH Washington Bureau, August 22, 2005

Tenet settles uninsured/ underinsured class action suit

by Andra Popa, J.D., LL.M

Uninsured and underinsured patients who filed a class action suit against Tenet Healthcare primarily alleging that the health care corporation charged unconscionable prices for medical care, products, and prescription drugs have entered into a settlement agreement with the corporation, as approved by the Supreme Court of California, County of Los Angeles. The corporation agreed to alter billing and collecion practices, bill the uninsured prices that do not exceed managed care rates, and disclose the estimated charges for treatment, including medical supplies, to all uninsured patients.

The settlement agreement terms focused on the following topics: (1) financial counseling, (2) fair treatment of the uninsured and underinsured, (3) charity care and government assistance programs, (4) reasonable payment terms, (5) collection actions, (6) disclosure of the cost of treatment, and (7) discounted pricing. The financial consulting terms Tenet agreed to in the settlement include:

- the provision of free financial counseling in plain English, or Spanish when appropriate, to all patients who request treatment at its hospitals, subject to the provisions of the Emergency Medical Treatment and Labor Act (EMTALA);
- the provision of training to financial counselors in hospitals;
- the provision of financial counseling to uninsured patients, including the discussion of their right to apply for financial assistance and charitable care, as well as delineating patient responsibility to complete documentation and inform their hospital of changes to their financial and/or insurance status;
- the assurance that uninsured patients will be aware that they have a right to be referred to an employee for financial counseling when applying for financial assistance programs;
- an estimation of the potential financial liabilities of the uninsured prior to treatment when possible;
- the notification to uninsured patients of the right to a finding on their financial assistance application within a reasonable time after a complete application is submitted.

In addition, the corporation agreed to designate an employee to monitor whether the uninsured are treated fairly and with respect during and after their experience at Tenet hospitals.

Among the most significant terms are those related to billing and reimbursement, including: charity care, payment terms, collection actions, and discounted pricing. While charitable care applications are being reviewed, Tenet agreed to place a hold on billing, the collection of fees, and collection actions as to any patient who has (1) applied for financial assistance and (2) submitted all related documentation, unless the bill is for a co-payment tied to a charity care program. Tenet agreed to ensure that credit reporting agencies that have been notified of late payments remove this information from the patient's credit report.

In addition, Tenet agreed to provide reasonable payment terms and simple, flexible payment schedules to all uninsured patients with a balance in excess of $1,000 dollars. As part of this agreement, Tenet may not charge interest on any payment plans that have been established and agreed to within 120 days of patient treatment and discharge. The corporation agreed to cap interest rates to the rate applicable by state law

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Andra Popa, J.D., LL.M

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard
Tax–Jeff Carlson, Steve Cooper

Designer
Patrick M. Gallagher

Comments from readers are welcome and should be directed to Andra Popa at popaa@cch.com, Tel. 847-267-2476, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

or 8 percent for payment plans that are established more than 120 days after treatment.

The settlement agreement prohibits the following collection actions without the express approval of the Chief Financial Officer or Chief Executive Officer of a hospital or another authorized individual: (1) foreclosures on property, (2) liens on property, (3) the garnishment of wages, and (4) the attachment or seizure of a bank account. Moreover, Tenet agreed to place restrictions on collection litigation involving the uninsured, including verifying whether the patient is employed and offering a settlement to all uninsured patients prior to litigation.

Finally, Tenet agreed to bill the uninsured and underinsured rates that do not exceed the highest rate it negotiates with any managed care plan. These rates will be available to all uninsured patients, regardless of income level.

Tenet Healthcare Cases II, Superior Court of California, County of Los Angeles, County Clerk Minutes, August 8, 2005.

New Medicare appeals process introduced

by Andra Popa, J.D., LL.M

Due to a new Medicare appeals process, Medicare beneficiaries, providers, and suppliers can expect the resolution of their fee-for-service Medicare claims within the 90-day timeframe required by the Medicare Prescription Drug, Improvement and Modernization Act of 2003 and the SCHIP Benefits Improvement and Protection Act of 2000 (BIPA).

As of July 1, 205, the Office of Medicare Hearings and Claims (OMHA), located within the Department of Health and Human Services (HHS), assumed responsibility for managing Medicare claims from the Social Security Administration. HHS Secretary Mike Leavitt stated that the goal "is to eliminate the need for an aged or disabled beneficiary to travel if other resources are available closer to home." Leavitt added that "as HHS assumes responsibility for handling Medicare hearings, we are committed to making the appeals process better, faster and more convenient for seniors and other people with Medicare."

To comply with BIPA time requirements, HHS will reduce the amount of time individuals spend in hearings by using video teleconferencing technology (VTC) coupled with a state-of-the-art electronic hearings process to provide individuals with greater access to the process. While VTC sites in over 1,000 cities nationwide are available, in-person hearings will also be offered to better accomodate all parties. If an individual requires an in-person hearing, the hearing will take place at the location that is most convenient for all parties, with HHS Administrative Law Judges traveling to locations around the country to conduct in-person hearings. In-person hearings may be held at local government facilities or other available sites. More information on the new Medicare appeals function is available at the OMHA Web site, www.hhs.gov/omha.

CMS Press Release, July 1, 2005.

Patient Safety Improvement Act signed

by Andra Popa, J.D., LL.M

Hospitals, physicians, health care professionals and entities will soon be able to voluntarily report information about health care errors to a confidential network of patient safety databases established by the Patient Safety and Quality Improvement Act of 2005 (Act).

The newly enated Act: (1) maintains Health Insurance Portability and Accountability Act (PubLNo 104-191) (HIPAA) protections, (2) defines privileged and confidential Patient Safety Work Product (PSWP), and (3) defines the circumstances in which PSWP may be disclosed without violating or waiving confidentiality and legal privilege. Patient Safety Organizations (PSOs), will be required to certify compliance with portions of the Act and submit subsequent certifications every three years. In addition, PSOs will collect national and regional error statistics, analyze patterns and trends, and provide feedback to providers. PSOs, which may be either public or private, may report non-identifiable PSWP to a national database.

continued on page 8

The privacy crime: Justice Department narrows the targets of HIPAA criminal prosecutions

by Jack A. Rovner

Only "covered entities"–and those individuals accountable under principles of corporate criminal liability for the violations of covered entities–can be prosecuted for committing the crimes established by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS"). That is the conclusion of a U.S. Department of Justice (DOJ) memorandum issued June 1, 2005 ("DOJ Memorandum").[1] This conclusion means that business associates (not otherwise themselves covered entities),[2] employees (not otherwise themselves accountable for the covered entity's violations), and other non-covered entities would not face prosecution under the HIPAA-AS criminal provisions, even though they misuse individually identifiable health information or unique health identifiers. That undermines the Seattle U.S. Attorney's August 2004 conviction under the HIPAA-AS criminal provisions of a covered entity's employee for theft of patient information. In that case, U.S. v. Gibson,[3] the employee pleaded guilty, and the covered entity that employed him was never charged. The DOJ Memorandum thus narrows the liability landscape for misuse of individually identifiable health information or unique health identifiers.

On the other hand, the DOJ Memorandum eases the proof needed to convict a covered entity under the HIPAA-AS criminal provisions. The DOJ Memorandum construes the knowledge element of the HIPAA-AS crimes to require only that a covered entity knew that it obtained or disclosed individually identifiable health information or used, or caused to be used, a unique health identifier. According to the DOJ Memorandum, there is no requirement to prove that the covered entity knew that such conduct constitutes a HIPAA-AS crime.

I. The HIPAA-AS crimes

HIPAA-AS added Part C to Title XI of the SSA to bring about "administrative simplification" to improve the Medicare and Medicaid Programs and "the efficiency and effectiveness of the health care delivery system."[4] These Administrative Simplification provisions have bestowed upon the health care industry the HIPAA-AS Rules which establish standards for electronic health care transactions, unique health identifiers for providers and employers (and will establish them for health plans), electronic health data security, and health information privacy.[5]

Section 1177 of Part C of Title XI of the SSA makes it a crime for "[a] person who knowingly and in violation of this part" does any of the following:

(1) "uses or causes to be used a unique health identifier;[6]
(2) obtains individually identifiable health information relating to an individual; or
(3) discloses individually identifiable health information to another person."

The punishment for these offenses is a fine up to $50,000, imprisonment up to 1 year, or both. The punishment increases to not more than $100,000, imprisonment up to 5 years, or both if the offense is committed under false pretenses, and to not more than $250,000, imprisonment up to 10 years, or both if the offense is committed "with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm."

Section 1176(b)(1) of Part C of Title XI of the SSA prohibits the imposition of civil penalties for an act that "constitutes an offense punishable under section 1177." Consequently, if the U.S. Department of Health and Human Services ("HHS"), which has civil enforcement responsibility for HIPAA-AS, is unable to obtain voluntary compliance to resolve misuse of individually identifiable health information or unique health identifiers, its enforcement option is limited to referring the matter to the DOJ for prosecution. If the DOJ declines or concludes it lacks jurisdiction to prosecute, there is no remedy under HIPAA-AS for the alleged misuse.

II. The "this part" ambiguity

The HIPAA-AS crimes apply to a "person" who knowingly and "in violation of this part" misuses individually identifiable health information or a unique health identifier. "This part" refers to Part C of Title XI of the Social Security Act (SSA) —the HIPAA Administrative Simplification provisions. Part C includes an "applicability" provision in Section 1172 that states that "[a]ny standard adopted under this part [C] shall apply, in whole or in part, to the following persons":

- "A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information in electronic form in connection with a transaction [regulated by the HIPAA-AS Rules]."[12]

To these, Congress added Medicare prescription drug card sponsors under the prescription drug card program established by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003.[13] These are the "covered entities" subject to HIPAA-AS.

The "standards" adopted under Part C, which Section 1172 applies to these covered entities, include "the purposes for which a unique health care identifier may be used."[14] The "standards" also include the provisions to protect the privacy of individually identifiable health information—the "Privacy Rule"[15] —adopted pursuant to HIPAA-AS § 264(c).[16] The Privacy Rule attaches to the activities regulated by Part C because its "standards" were adopted for "the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the SSA."[17] As covered entities must obtain and disclose individually identifiable health information and use or cause to be used unique health identifiers to conduct HIPAA-AS electronic transactions, they can do so "in violation of this part [C]." Accordingly, covered entities are clearly subject to the HIPAA-AS criminal provisions.

It is not clear, however, whether the HIPAA-AS criminal provisions stop with covered entities or reach all "persons." The HIPAA-AS criminal provisions mention neither "covered entities," nor the "standards" that relate to the use of unique health identifiers and the privacy of individually identifiable health information. Instead, the HIPAA-AS criminal provisions speak of "persons" who "obtain" or "disclose" individually identifiable health information or "use or cause to be used" unique health identifiers "in violation of this part [C]."

HIPAA-AS does not define "person," as it is used in its criminal provisions. Section 1172 suggests that "person" is much broader than covered entities by specifying that the HIPAA-AS "standards" apply only to that subgroup of "persons" who are health plans, health care clearinghouses, and health care providers who transmit HIPAA-AS electronic transactions. The SSA, which includes the HIPAA-AS criminal provisions, specifies that "person," when used in the SSA, means "an individual, a trust or estate, a partnership, or a corporation." "Corporation" includes "associations, joint-stock companies, and insurance companies." Indeed, HHS proposes an expansive definition of "person" for purposes of civil enforcement of HIPAA-AS standards to encompass "'a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private,' [to] clarif[y], consistent with the HIPAA provisions, that the term includes States and other public entities."[19]

These broad definitions of "person" suggest that any natural person or public or private organization may violate the HIPAA-AS criminal provisions by obtaining or disclosing individually identifiable health information or using, or causing to be used, unique health identifiers "in violation of this part [C]." Under this construction, a "person" who (or that) is not a covered entity could commit a HIPAA-AS crime by obtaining or disclosing individually identifiable health information for a purpose contrary to those permitted pursuant to Section 1173(a) of Part C, or by using or causing to be used a unique health identifier for a purpose other than those permitted pursuant to Section 1173(b) of Part C.

III. The Seattle prosecution

The U.S. Attorney in Seattle, Washington, plainly read the HIPAA-AS criminal provisions as applicable to "persons" beyond covered entities. In August 2004, the Seattle U.S. Attorney filed a criminal information against an employee of the Seattle Cancer Care Alliance, a health care provider subject to HIPAA-AS, for "knowingly and for a reason other than permitted by [HIPAA-AS] Part C disclos[ing] individually identifiable health information of . . . a patient receiving treatment at the health care provider at which [the employee] was employed, with intent to use that information for personal gain." The employee obtained the patient's name, date of birth, and Social Security number - demographic information - from the individually identifiable health information that the Seattle Cancer Care Alliance had collected from the patient, and disclosed that demographic information to get credit cards in the patient's name.

The employee pleaded guilty, so whether the HIPAA-AS criminal provisions are applicable to non-covered entities was not tested in court. Interviewed shortly after obtaining the conviction, the prosecuting assistant U.S. attorney stated that whether the employee "was or was not a covered entity under HIPAA was not a great concern." Acknowledging that the employee "could have [been] charged [with] unlawful identity theft," the assistant U.S. attorney instead chose the HIPAA-AS criminal provisions because "the health care connection made it important that a HIPAA crime should be charged."[22]

The assistant U.S. attorney further explained that, as "[t]he information clearly had been collected by the Seattle Cancer Alliance because the patient was being treated there, and so it was demographic information covered by HIPAA," its knowing use "for an improper purpose is a crime under HIPAA."[23] The Seattle U.S. Attorney's Office thus plainly considered that the inclusion of "demographic information collected from an individual" in the definition of individually identifiable health information means that name, address, birth date, Social Security number, and similar information associated with health information is fully protected by HIPAA-AS, even though only such demographic information and no health information is obtained or disclosed.

IV. The DOJ memorandum

The DOJ Memorandum addresses two issues:

(1) "whether the only persons who may be directly liable under section 1320d-6 [the HIPAA-AS crimes] are those persons to whom the substantive requirements of [HIPAA-AS] apply [i.e., covered entities] or whether this provision may also render directly liable other persons, particularly those who obtain protected health information in a manner that causes a [covered entity] to release information in violation of [HIPAA-AS];" and

(2) "whether the 'knowingly' element of section 1320d-6 requires proof of knowledge of the facts that constitute the offense or whether this element also requires proof of knowledge that the conduct was contrary to [HIPAA-AS]." (DOJ Mem. at 1.)

A. "Persons" subject to the HIPAA-AS criminal provisions

The DOJ Memorandum concludes that, "[b]ecause Part C makes the standards applicable only to covered entities and because it mandates compliance only by covered entities, only a covered entity may do one of the three listed acts [of the HIPAA-AS crimes] 'in violation of this part.'"[24] The DOJ Memorandum acknowledges that the "distinct prohibition on obtaining health information" of the HIPAA-AS criminal provisions could be construed "to reach the acquisition of health information by a person who is not a covered entity but who 'obtains' it from such an entity in a manner that causes the [covered] entity to violate Part C."[25] It rejects this construction on the proposition that the HIPAA-AS criminal prohibition on obtaining individually identifiable health information "merely reflects the fact that [HIPAA-AS and the HIPAA-AS Rules] limit the acquisition, as well as the disclosure and use, of information by covered entities."[26] That HIPAA-AS and the HIPAA-AS Rules "limit" a covered entity's acquisition of individually identifiable health information seems an unsatisfactory explanation of why the HIPAA-AS criminal prohibition does not also reach a non-covered entity's improper acquisition of individually identifiable health information from a covered entity.

The DOJ Memorandum also rejects that the HIPAA-AS criminal prohibition on using or causing to be used a unique health identifier could apply to non-covered entities who cause "a covered entity to 'use' unique health identifiers in violation of the part."[27] The DOJ Memorandum explains that this HIPAA-AS criminal prohibition "is better read to cover those instances in which a covered entity causes, in violation of the part, another person to use a unique health identifier, but where the covered entity itself did not use the identifier in an unauthorized manner."[28] This, too, seems an unsatisfactory explanation of why this HIPAA-AS criminal prohibition does not also apply to a non-covered entity who causes a covered entity to misuse unique health identifiers.

Officers, directors, and managers of organizational covered entities face personal criminal exposure under "principles of corporate criminal liability" for the HIPAA-AS crimes of the covered entities they manage, according to the DOJ Memorandum.[29] The DOJ Memorandum observes that "criminal liability of [an] entity has been attributed to individuals in managerial roles, including, at times, to individuals with no direct involvement in the offense."[30] These observations underscore the critical importance of effective compliance programs for organizations and the organization's officers, directors, and managers to avoid criminal liability.

Although, under the conclusions of the DOJ Memorandum, non-covered entities could not be directly prosecuted under the HIPAA-AS criminal provisions, the DOJ Memorandum explains that non-covered entities "may be prosecuted according to principles either of aiding or abetting liability or of conspiracy liability."[31] The DOJ Memorandum gives, as an example, "an individual who is not a covered entity who aids or conspires with a covered entity in the use of protected health information in a manner not authorized by the [HIPAA-AS Rules]."[32] The DOJ Memorandum also notes that non-covered entities may be charged under other federal laws, such as those punishing identity theft or fraudulent access to computers.[33]

B. "Knowingly" element of the HIPAA-AS criminal provisions

On the requirement that a person "knowingly" obtain or disclose individually identifiable heath information or "knowingly" use or cause to be used a unique health identifier to commit the HIPAA-AS crimes, the DOJ Memorandum concludes that the requirement is satisfied by "knowledge of the facts that constitute the offense," with no need for "proof of knowledge that the conduct was contrary to [HIPAA-AS or the HIPAA-AS Rules]."[34] According to the DOJ Memorandum, "[a] plain reading of the [statutory] text indicates that a person need not know that commission of an act described in [the HIPAA-AS criminal provisions] violates the law in

order to satisfy the 'knowingly' element of the offense."[35] It reaches this conclusion because "knowingly" modifies, not "in violation of this part," but "'uses or causes to be used,' 'obtains' and 'discloses.'"[36] Hence, there is no requirement that a person "know" that the misuse of individually identifiable health information or unique health identifiers violates "this part," that is, HIPAA-AS.

V. Conclusion

The DOJ Memorandum's conclusion that the HIPAA-AS criminal provisions apply only to covered entities, and their officers, directors, and managers accountable under principles of corporate criminal liability, appears to leave non-covered entities immune from HIPAA-AS prosecution. That would mean that business associates (not otherwise covered entities) and employees (not otherwise accountable for the covered entity's violations) are beyond the reach of the HIPAA-AS criminal provisions, notwithstanding that they improperly obtain or disclose individually identifiable health information or improperly use or cause to be used unique health identifiers. It would also mean that physicians and other health care providers who have never transmitted (or had transmitted on their behalf) electronic transactions regulated by the HIPAA-AS Rules are beyond the reach of the HIPAA-AS criminal provisions because these providers are not covered entities. This is a result at odds with the Seattle U.S. Attorney's August 2004 prosecution of a covered entity's employee, and thus questions its validity.

Nonetheless, as the DOJ Memorandum warns, criminal exposure continues for business associates, employees, and other non-covered entities that aid and abet or conspire with a covered entity to misuse individually identifiable health information or unique health identifiers. There is also direct criminal exposure under other federal laws, such as those prohibiting identity theft, fraudulent access to computers, or misappropriation of a public or private health plan's assets or property,[37] for business associates, employees, and other non-covered entities acting independently of covered entities. Hence, the conclusion of the DOJ Memorandum does not insulate non-covered entities from criminal exposure for misuse of individually identifiable health information or unique health identifiers; it just insulates them from direct exposure to the HIPAA-AS criminal provisions.

Because only the Justice Department may prosecute under the HIPAA-AS criminal provisions, if the U.S. Attorneys follow the DOJ Memorandum, no case may reach the courts for a judicial determination whether or not the HIPAA-AS criminal provisions apply to non-covered entities. But, if the DOJ Memorandum got congressional intent wrong, Congress may remedy the situation by amending the HIPAA-AS criminal provisions to make their application to all "persons" clear.

Jack A. Rovner is a partner and co-chair of the Health Law Practice Group of Neal, Gerber & Eisenberg LLP, Chicago, Illinois. Rovner's practice areas include health law, business counseling and transactions, antitrust, and commercial litigation. In 2002, he served as a member of the Secretary's Advisory Committee on Regulatory Reform of the U.S. Department of Health and Human Services, where he was a member of the Executive Committee and Chair of the Coordination Subcommittee. Mr. Rovner may be contacted at jrovner@ngelaw.com.

1 The DOJ Memorandum is available at <*www.usdoj.gov/olc/hipaa_final.htm.*>

2 A business associate is a person or organization that performs functions or activities for or on behalf of a covered entity that involve individually identifiable health information. 45 C.F.R. § 160.103 "business associate"). A covered entity may act as a business associate of another covered entity. 45 C.F.R. § 160.103 ("business associate" ¶ (3)).

3 No. CR04-0374 SRM, Information and Plea Agreement filed Aug. 18, 2004 (U.S. Dist. Ct., W.D. Wash.).

4 Pub. L. No. 104-191, § 261, 110 Stat. 2021 (1996).

5 *See* 45 C.F.R. Parts 160-64.

6 HIPAA-AS directs HHS to "adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system," and to "specify the purposes for which a unique health identifier may be used." 42 U.S.C. § 1320d-2(b). HHS has issued standards for unique health care provider and employer identifiers. *See* 45 C.F.R. Part 162, Subparts D and F. HHS has yet to propose standards for a unique health plan identifier. Congress has blocked issuance of unique health identifiers for individuals "until legislation is enacted specifically approving the standard." Pub. L. No. 105-277, § 516, 112 Stat. 2681-386 (1998).

7 Individually identifiable health information is "any information, including demographic information collected from an individual, that: (A)"is created or received by a health care provider, health plan, employer, or health care clearinghouse;" and (B) "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- (i) "identifies the individual;" or (ii) "with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. § 1320d(6).

8 42 U.S.C. § 1320d-6(a).

9 42 U.S.C. § 1320d-6(b).

10 42 U.S.C. § 1320d-5(b)(1).

11 42 U.S.C. § 1320d-5(a). The proposed HIPAA-AS enforcement rule would, accordingly, recognize as an affirmative defense to imposition of civil monetary penalties that "[t]he violation is an act punishable under 42 U.S.C. 1320d-6." 70 Fed. Reg. 20223, 20253 (Apr. 18, 2005) (proposed 45 C.F.R. § 160.410(b)(1)).

12 42 U.S.C. § 1320d-1(a).

13 42 U.S.C. § 1395w-141(h)(6)(A).

14 42 U.S.C. § 1320d-2(b)(2).

15 45 C.F.R. Part 164, Subpart E.

16 Pub. L. No. 104-191, § 264(c), 110 Stat. 2033 (1996). HIPAA-AS § 264(c) required HHS to issue the Privacy Rule if Congress failed to enact "legislation governing standards with respect to the privacy of individually identifiable health information" by August 21, 1999. Congress never enacted that legislation.

17 Pub. L. No. 104-191, § 264(c), 110 Stat. 2033 (1996). SSA § 1173(a) requires the issuance of "standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically." 42 U.S.C. § 1320d-2(a). The "health information"

On The Front Lines (cont.)

to be exchanged in these electronic transactions is defined such that it encompasses individually identifiable health information. *See* 42 U.S.C. § 1320d(4).

[18] 42 U.S.C. §§ 1301(a)(3), (4).

[19] 70 Fed. Reg. at 20228; *See id*, at 20250 (proposed 45 C.F.R. § 160.103 ("person")).

[20] Information ¶ 1, *U.S. v. Gibson,* No. CR04-0374 RSM (U.S. Dist. Ct., W.D. Wash., Aug. 18, 2004).

[21] Interview with Susan Loitz, Assistant U.S. Attorney, by Alan S. Goldberg, 1 ABA Health eSource No. 2 (Oct. 2004), *available at* , <http://www.abanet.org/health/esource/vol1no2/loitz.html>.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 5.

[25] *Id.* at 6.

[26] *Id.*

[27] *Id.* at 6 n. 4.

[28] *Id.*

[29] *Id.* at 9.

[30] *Id.*

[31] *Id.*

[32] *Id.* at 9.

[33] *Id.*

[34] *Id.* at 1.

[35] *Id.* at 10-11.

[36] *Id.* at 11.

[37] *See* 18 U.S.C. § 669.

Trends (cont.)

PSWP is not subject to criminal, civil, administrative, or disciplinary hearing subpoenas, orders, discovery proceedings, certain disclosures, and may not be admitted as evidence in such proceedings. Information related to a crime or an event reasonably believed to be a crime is not PSWP and may be disclosed to law enforcement authorities. Accrediting agencies are not permitted to take accrediting actions against providers based on their good faith participation in the reporting of PSWP information.

The Act imposes a maximum civil monetary penalty of $10,000 for each instance in which a person discloses PSWP in knowing or reckless violation of a portion of the Act. Although the Act became effective upon signing, the reporting system infrastructure must be developed and implemented.

Patient Safety Improvement Act, S. 544, H.R. 3205, July 29, 2005.

HIPAA

CMS ends contingency for non-HIPAA compliant Medicare claims

by Sheila Lynch-Afryl, J.D., Contributing Editor

CMS announced that it will not process electronic Medicare claims submitted for payment October 1, 2005, that fail to comply with the Health Insurance Portability and Accountability Act of 1996 (PubLNo 104-191) (HIPAA). Claims that do not meet these standards will not be processed and will be returned to the filer for re-submission.

As of June 2005, .5 percent of Medicare fee-for-service providers submitted non-HIPAA-compliant electronic claims. "We are firmly committed to an interoperable electronic health care system, and the close-to-100-percent compliance with HIPAA standards for claims shows that the health care industry shares this commitment," CMS Administrator Mark B. McClellan, M.D., Ph.D., commented.

Contingency plan. This action ends a portion of a CMS HIPAA contingency plan that has been in effect since October 16, 2003. Although the law required all payors to conduct HIPAA-compliant transactions by the October 2003 date, only 31 percent of Medicare claims were compliant at the time. To address this problem, CMS established a contingency plan that allowed its trading partners to submit claims in electronic formats currently in use. A July 24, 2003, enforcement guidance, however, directed covered entities to make reasonable and diligent efforts to comply with the contingency plan.

The contingency continues for other electronic health care transactions, but CMS plans to end the contingency plan for these transactions in the near future. The remittance advice transaction is the next HIPAA transaction for which CMS expects to end its contingency plan.

CMS Release, Aug. 4, 2005