CCH Healthcare Compliance LETTER

Volume 7, Issue 1 www.cchgroup.com January 12, 2004

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments or questions regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Sharon Sofinski, Coordinating Editor, at sofinsks@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

Entities covered by HIPAA must be cautious when disclosing PHI, panel says

by Catherine Hubbard, MA, Contributing Editor

Health care entities covered by the Health Insurance Portability and Accountability Act (HIPAA) privacy rule may disclose personal health information (PHI) for several reasons, including law enforcement, disease control and prevention of crimes. But entities must be careful that their disclosures meet the exceptions contained in the rule, according to government experts and a lawyer who spoke during a recent conference call briefing. "If you are considering disclosing, you have to look at all the qualifications," cautioned Janet Newberg, chair of the Health Law Section at Felhaber Larson Fenlon and Vogt, St. Paul, Minnesota. She spoke during a December 16 conference call sponsored by the Health Care Compliance Association.

Under HIPAA, covered entities may disclose PHI for treatment, payment and health care operations, or for vital statistics (birth and death) reports. They also may pass on health information in cases of suspected abuse, neglect or domestic violence. In that case, Newberg said, they can pass on health information to an authorized government authority, if the victim agrees to the disclosure, or if law requires the disclosure. "If you are contemplating disclosing information about a patient who appears to be a victim of abuse, neglect or domestic violence, you have to look at all of the [HIPAA] qualifications," she cautioned.

One area that has caused a lot of confusion is disclosures for judicial and administrative proceedings, Newberg said. A covered entity may disclose PHI in the course of any judicial or administrative proceeding in response to a court order, a subpoena, a discovery request or other lawful purposes, said Newberg. Yet only court orders issued by judges and judicial officers count, Newberg said, not simple subpoenas.

The way a covered entity can disclose PHI differs, depending on the request, Newberg said. "It's important to recognize what is a court and order and what it isn't," she emphasized. An individual suing to obtain PHI has "more hoops to jump through in order to get the information," she said.

If the requester lacks the signature of a judge or judicial officer, covered entities may disclose PHI only if they had satisfactory assurance the requester had engaged in reasonable efforts to either notify the patient of the request or to obtain a protective order directly from the court, Newberg said. Satisfactory assurance means there is a written statement and documentation that the requester tried to notify the patient, the notice included information about the litigation or proceeding, the patient's time to object has expired and the patient either didn't object or any

objections were resolved by the court, she explained.

These sticky issues surrounding subpoenas and discovery requests are illustrated by the Kobe Bryant case (State of Colorado, County of Eagle against Kobe Bean Bryant), in which Bryant was charged with sexually assaulting a hotel worker, Newberg said, noting that the defense team has sought the alleged victim's medical records, both from before and after the alleged crime took place. "If that type of subpoena had come to your hospital or clinic, the defense team would have had to provide you with satisfactory assurance that they have notified the woman, that she knows what the litigation is about and that she's had the opportunity to object, etc.," she said. The requester can also provide assurance they have engaged in reasonable efforts to obtain a protective order, she noted. "If they do that, then they don't necessarily have to give satisfactory assurance they have tried to notify the patient of the subpoena," she said.

State preemption. Newberg also advised listeners to beware of state privacy laws. "Watch out for state law provisions," she said, noting HIPAA governs unless a conflicting state law relating to the privacy of PHI is more stringent. For example, she said, Minnesota prohibits release of PHI without a signed consent from the patient, except in limited circumstances. "We have to be constantly looking both at HIPAA and the Minnesota statute," she said.

"State preemption is one of the areas that is most likely to end up in litigation," said Ian C. Smith DeWaal, senior counsel to the Department of Justice Criminal Division, Fraud Section. He said questions about whether a state or federal law prevails will have to be answered in court. Nevertheless, when a federal subpoena is involved, he said, "The HIPAA preemption standard is not going to change the prior standards established under the Supremacy Clause." In those cases, regardless of state privacy law, the federal subpoena is supreme and must be complied with, he said. When there's a conflict, either the DOJ will move to enforce its subpoena or the covered entity will move to quash the subpoena, he said. He noted that he was speaking on his own behalf.

OIG authority. Anne MacArthur, senior counsel at the Health and Human Services Office of the Inspector General (HHS OIG), said the privacy rule permits covered entities to disclose PHI in response to IG subpoenas without patient consent for investigative and enforcement purposes. "The OIG will work with covered entities to allay concerns about an IG subpoena; however, when necessary, we will take action to enforce our subpoenas," she said. Covered entities should contact the office if they have questions about disclosure of PHI related to an IG subpoena from the HHS OIG, she said.

"The privacy rule permits covered entities to disclose PHI in response to IG subpoenas without patient consent for investigative and enforcement purposes."

MacArthur noted the OIG is authorized to issue subpoenas for PHI under the IG Act of 1978. HIPAA disclosures can be for civil, administrative or criminal investigations or proceedings, she noted. "We have a fairly broad range of things we look at," she said. Health oversight activities under HIPAA also include audits, fraud investigations, inspections and licensure or disciplinary actions. "There are a lot of activities that you might not think come under health oversight, that do," she said.

MacArthur also clarified that the OIG works with other agencies, including the FBI, when its health oversight activities touch upon multiple public benefits. For example, often when people use a fraudulent Social Security Number, they commit fraud in more than one area, such as the Medicaid system, which is run by both the federal and state governments, and in the food stamp program run by the Agricultural Department, she said. "We find that when there is one false Social Security Number or group of numbers, there's multiple frauds," she noted. ■

CCH Washington Bureau, January 5, 2004

CCH Healthcare 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 Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Judgment upholding hospital's tax-exempt status reversed

Joint ventures between tax-exempt and for-profit health entities are increasingly common and have generated tough tax questions. That controversy was raised another level when the Fifth Circuit Court of Appeals recently vacated summary judgment granting a hospital's claim for a tax refund after the IRS revoked its tax-exempt status because it had partnered with a for-profit health care company (*St. David's Health Care System*, CA-5, 2003-2 USTC ¶50,713). The Fifth Circuit found that the IRS raised material issues of fact regarding whether the partnership interfered with the hospital's ability to operate exclusively for exempt purposes.

The hospital operated for many years as a nonprofit. For most of its existence, it was recognized as tax-exempt under Code Sec. 501(c)(3). Due to financial difficulties in the health care industry in the 1990s, the hospital decided to consolidate with a for-profit health care organization.

The IRS audited the hospital and determined that it no longer qualified for tax-exempt status because it had ceded control over its operations to the for-profit entity. Both the hospital and the IRS filed motions for summary judgment in district court, which granted the hospital's motion and ordered a tax refund. The IRS appealed to the Fifth Circuit.

Tax-exempt status. To qualify for Code Sec. 501(c)(3) tax-exempt status, the hospital was required to show that it was organized and operated exclusively for a charitable purpose. To pass the operational test, the hospital had to show that it:

- engaged primarily in activities that accomplished its exempt purpose;
- did not have net earnings that inured to the benefit of private shareholders or individuals;
- did not expend a substantial part of its resources attempting to influence legislation or political campaigns; and
- served a valid purpose and conferred a public benefit.

IRS position. The IRS argued that the hospital failed the first prong of the operational test because, since partnering with a for-profit company, its primary purpose was no longer charitable.

The IRS did not contend that tax-exempt status is automatically lost when a partnership is formed with a for-profit entity. Rather, it argued that a nonprofit loses its tax exemption if it gives control over the partnership to a for-profit entity. In the IRS's view, when a nonprofit cedes control, it can no longer ensure that its partnership activities primarily further its charitable purpose.

Hospital's position. The hospital argued that it passed the operational test because its activities, via the partnership, contributed to its charitable purpose of providing health care to all persons.

Disagreeing with the hospital, the appellate court observed that even if the hospital performed charitable services, it would not qualify for Code Sec. 501(c)(3) status if its activities substantially furthered the profit-seeking interests of its partner. The key issue, in the appellate court's opinion, was whether the partnership with a for-profit company interfered with the hospital's ability to operate exclusively for exempt purposes.

Control issues. Rev. Rul. 98-15 addresses how a charitable hospital can retain its tax-exempt status when it forms a partnership with a for-profit entity. A nonprofit can demonstrate control by showing that the partnership's founding documents expressly state that it has a charitable purpose and it will take priority over all other concerns; the partnership agreement gives the nonprofit organization a majority vote on the partnership's board of directors; and the partnership is managed by an independent company not affiliated with the for-profit entity.

In vacating summary judgment, the Fifth Circuit ruled that there were outstanding issues of material fact concerning the nonprofit's level of control in the joint venture. The court cited flaws in the partnership agreement; the nonprofit's level of power (or lack thereof) within the partnership; and conflict of interest between the for-profit partner and a management service that had a long-term contract at the hospital and the for-profit company.

The appellate court observed that even if the hospital performed charitable services, it would not qualify for Code Sec. 501(c)(3) status if its activities substantially furthered the profit-seeking interests of its partner. The key issue, in the appellate court's opinion, was whether the partnership with a for-profit company interfered with the hospital's ability to operate exclusively for exempt purposes. Until those issues were explored, the question of control could not be resolved. ■

CCH Washington Bureau, December 12, 2003

Corporate responsibility issues for board members and senior executives of nonprofit corporations in a post–Sarbanes-Oxley Act environment

by Cynthia F. Reaves, Esq.

Congress enacted the Sarbanes-Oxley Act of 2002 ("SOA" or the "Act")[1] in response to the collapse of both Enron and WorldCom corporations and the subsequent loss in investor trust and confidence in publicly traded companies, in general. The Act requires companies whose securities are publicly traded to comply with various corporate responsibility, disclosure and audit rules. In the months since the Act was passed, the Securities and Exchange Commission (the "SEC") has promulgated rules and regulations which are designed to implement the requirements of the Act. Several states also have proposed or enacted legislation to impose similar requirements.

This article will provide a brief overview of the origins and requirements of the Sarbanes-Oxley Act as it applies to publicly traded organizations. It also will discuss how the Act might apply to nonprofit companies. Finally, this article will discuss the effect the Act may be expected to have upon the roles and responsibilities of nonprofit boards of directors and senior managers as they manage nonprofit entities.

By its terms, the Act applies only to publicly traded companies. However, the implications of the Act are likely to resonate directly and indirectly throughout the business world, including in the nonprofit environment. At its core, the SOA was conceived as a set of legal reforms in response to: (1) corporate accounting controversies which were found in publicly traded companies, (2) the need to protect the interests of investors, and (3) the need to provide stability to financial markets. The Act established a new oversight mechanism for the public accounting profession, created new rules for the auditor/client relationship, and instituted new criminal penalties for corporate finance-related crimes. It also established corporate responsibility procedures for executive and board conduct, assigned new ethical obligations to corporate counsel, and provided new protections for investors. The Act applies only to publicly traded companies.

However, along with the regulatory review and oversight rules for public companies which were put in place with the enactment of the SOA, there was also a corresponding increase in the responsibilities which were imposed upon directors and senior executives of publicly traded companies. This increased scrutiny has also extended to nonprofit corporations and the managers and executives who lead those organizations. Indeed, the Attorneys General of several states have applied Sarbanes-Oxley-type provisions to the operations of nonprofit corporations and, in the case of New York, have proposed that rules specifically modeled after the Act be applied to the activities of such entities. For this reason, the leadership of nonprofit organizations should understand the increased responsibilities and obligations which are likely to be imposed upon their activities. At the very least, nonprofit organization leaders might choose to look at these guidelines as a benchmark by which to measure their performance.

The Sarbanes-Oxley Act

The SOA has requirements for public companies which can be roughly divided into three parts—corporate responsibility and governance, auditor independence, and enhanced disclosure. The Act also provides for additional federal oversight of public companies and penalties for noncompliance. In particular, the corporate responsibility rules under the Act: (1) include rules for corporate audit committees, (2) outline issues relating to corporate responsibility for financial reports, (3) discuss corporate bonus and profit compensation arrangements, (4) outline rules relating to insider trading, and (5) set forth guidelines relating to interactions with company auditors. These rules have the most noticeable impact for senior managers and board members with respect to the operation of their companies because of the direct impact on the roles and responsibilities that these individuals have with respect to managing the affairs of a company. While the other rules do indeed impact upon

corporate operations, those changes are more likely to be felt by the key operational staff members with responsibility over a particular area. For example, the requirements for enhanced financial disclosure will directly impact upon the senior financial and operational officers, but will also greatly impact the managers who are responsible for compiling and disclosing information. In short, the entire organizational structure will be impacted by the implications of the Act.

The Application of Specific SOA Rules to Nonprofit Corporations

The Act sets forth a number of rules which apply to publicly traded companies. However, certain of the new rules and reporting requirements can be applied to nonprofit company activities. If a nonprofit company wanted to be proactive with respect to its corporate responsibility obligations, the governing board of the entity might choose to adopt rules which mirror the obligations imposed upon publicly traded corporations by the Act. The following rules, derived from the SOA, should be considered by nonprofit organizations in establishing a corporate responsibility program. While such rules are not, by law, imposed upon nonprofits, the SOA guidelines provide a helpful framework within which to establish a program for those organizations choosing to do so:

1. **Audit Committee.** A dedicated audit committee of the Board should be established to oversee accounting and financial reporting matters and to review the adequacy of internal controls. This committee should give focus to all financial matters, including risks that are particular to such organization. Importantly, such a committee should have at least one person who is a financial expert (i.e., someone with an understanding of GAAP and financial statements). It has been suggested that an audit committee without a financial expert could hire one as a consultant and thereby comply with the spirit of the SOA. This is a change for many nonprofit corporations which might not have, as a practice, selected leaders based upon their ability to manage complex finances. Rather, nonprofits have characteristically sought out community leaders and those able to assist in fundraising and development efforts. Consequently, it has become increasingly important that senior executives and company leadership have an understanding of the financial records of a nonprofit entity. Compliance with the SOA rules would dictate that financial experts serve key roles in the management of a nonprofit entity.
2. **Code of Ethics.** Public companies must disclose whether their senior financial executives are subject to a code of ethics. Nonprofits should develop such codes to promote honest and ethical conduct, compliance with laws and regulations and full and fair disclosure of information. In this regard, many nonprofits adopted such policies as part of developing corporate compliance programs. Furthermore, the IRS has long required that 501(c)(3) organizations adopt a substantial conflict of interest policy in order to be tax-exempt. Consequently, it is possible that the adoption of such a policy will be unnecessary, but merely an opportunity to revisit and refine an existing policy. Interestingly, however, there may be some nonprofit entities which are unaware of these requirements and will develop these policies for the first time.
3. **Corporate Responsibility for Financial Reports.** A nonprofit organization should develop an internal process which would facilitate the ability of the principal executive officers of a nonprofit corporation to certify the corporation's periodic financial reports in the event that nonprofit organizations are required to implement certifications standards which are similar to those set forth in the SOA. The SOA requires that certain senior managers of public companies certify that the financial statements fairly present the financial conditions of their companies. These executives must review their companies' internal controls and report on their adequacy. Indeed, certifications such as those called for by the SOA are beginning to be requested of nonprofit corporations by third parties such as lenders or underwriters in the normal course of business. For nonprofit organization leaders, this requirement is substantial. Care should be taken in placing the burden of this responsibility upon senior leaders of smaller nonprofit entities. While large nonprofit corporations should be able to respond to this requirement, smaller ones may not have the resources available to senior management to make such a certification meaningful.
4. **Annual Reports.** Nonprofits are required to file annual reports and to make such reports widely available to the public. Nonprofit corporations should use the annual report as an opportunity to communicate important information to the public about their charitable activities and should consider providing disclosure on governance matters and the procedures being used to ensure that the financial condition is understood by the board and management and is transparent to third parties who may review such reports or publications. Such a disclosure can serve to enhance public confidence in the financial disclosures of a company.
5. **Auditor Independence.** Nonprofits should confirm that their auditors are in compliance with all new professional rules, including those being established by the Public Accounting Oversight Board. These rules include strict independence requirements. The nonprofit organization should consider implementing policies to ensure that non-audit consulting services that cannot be purchased by public companies from their auditors similarly cannot be bought by it from its auditor. This will require the senior leadership of a nonprofit to include rules relating to conflicts of its outside vendors with respect to the financial and reporting requirements of the organization.

6. **Retaliation against Whistleblowers.** The SOA makes it a crime to retaliate against a "whistleblower" who reports information about the commission of any federal offense. "Retaliation" includes interference with a person's employment:

   Whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both.

   There have been various other laws penalizing retaliators but the SOA raises the stakes by making retaliation a crime. In this regard, the rules function in the same way that health regulatory rules do with respect to the reporting of health care fraud and abuse. As a practical matter, the nonprofit organization must create systems by which abuse may be reported, investigated, corrected and, if appropriate, prosecuted. This requirement puts a burden upon nonprofit organization leaders to develop the systems and create the environment which would encourage the reporting of prohibited behavior. Most importantly, however, the systems, once in place, must be monitored and the organization is under an obligation to address any issues which are raised. This requirement, therefore, could be said to put the organization, and its organizational managers, on notice of any fraudulent behavior and to produce account for those instances in which it may have failed to follow-up on complaints if there is a break in the system.
7. **Destruction of Records.** The SOA creates a new federal crime for the destruction or alteration of records during a federal investigation. Its application is not limited to for-profit entities. In this regard, some commentators have suggested that nonprofit entities are subject to the requirements of the Act. However, some nonprofits such as healthcare institutions are already subject to federal laws that penalize the destruction of records. Adoption of such a rule, therefore, should not be unusual for a nonprofit health care entity. Senior management would therefore be charged with establishing rules regarding the appropriate management of materials, including for the destruction of such items.
8. **Loans to Executives.** The SOA prohibits personal loans or other extensions of credit to directors and executive officers. This could be difficult for some nonprofits that use mortgage loans or guarantees or similar "perquisites" as part of compensation to induce executives to relocate and join organizations. Indeed, the IRS has provided guidance which describes when such programs are appropriate. Consequently, organizational leaders should revisit these policies to ensure compliance with current IRS standards. In this regard, existing exempt organization rules might provide greater flexibility to nonprofit organizations.
9. **Executive Compensation.** SOA sets forth strict rules regarding executive compensation, including rules requiring executives to repay bonuses in cases of fraud. Nonprofit organizations are accustomed to the strict scrutiny under which their compensation arrangements are reviewed. Consequently, while it is likely that executive compensation arrangements will be subject to strict scrutiny in the times ahead, nonprofit corporations should be well-versed in the applicable rules regarding the documentation of the reasonableness of compensation. Boards of nonprofits should review their compensation systems in order to determine whether they are reasonable, provide appropriate and adequate documentation and are sufficiently transparent to all constituencies and regulatory bodies.

State Rules May Dictate Nonprofit Compliance

While SOA applies to publicly traded companies, some state attorneys general have taken steps to apply Sarbanes-type requirements to the operations and activities of nonprofit organizations. This provides an additional reason why it may be prudent for nonprofit corporations to adopt SOA-type rules to govern their operations. For example, Minnesota Attorney General Mike Hatch released a report entitled "Corporate Responsibility" in which he outlined proposals for corporate audits and engaging and overseeing auditors for a company.[2] Some of the proposals which Attorney General Hatch outlined in his report were more restrictive than those set forth in the SOA. These rules would apply to all companies operating in Minnesota, not just those which are publicly traded.

In January 2003, the New York Attorney General proposed reforms designed to strengthen New York's corporate accountability laws. The stated desire was to close the types of loopholes that allowed abuses to go undetected at major corporations and to provide protections against abuses by nonprofit corporations. In this regard, the New York Attorney General noted that the SOA protections only applied to companies listed on a major stock exchange and not to their nonprofit counterparts. In public comments he stated that he was seeking to protect not only investors but charitable donors as well. As a result, New York became among the first states to propose to apply SOA-type reporting requirements to nonprofit corporate activity.

Finally, the Governor of the State of Michigan appears to have taken an interest in insuring that corporations which do business with the state operate with regard to the highest ethical standards. In her first day in office, Governor Jennifer Granholm signed Executive Order Number 2003-1: Procurement of Goods and Services from Vendors in Compliance with State and Federal Law. The order allows the State to revoke, suspend or prohibit contracting privileges with the State for those vendors which (within the past three years) have been convicted of certain criminal offenses, including an offense which negatively reflects on the vendor's business integrity. Thus, we see another example in which a state is seeking to regulate the corporate integrity of businesses, whether organized on a for-profit or nonprofit basis.

Nonprofit Organization Response to the SOA

Nonprofit organizations and their managers may desire to be proactive in responding to the reporting requirements of SOA by adopting policies and procedures which reflect a public disclosure requirements of SOA. This is because the SOA rules, in effect,

establish a standard of conduct in the reporting and disclosure requirements of corporations and businesses generally. In this regard, nonprofit organizations are not above financial scandal. Indeed, nonprofit organizations have experienced unfavorable media attention in recent years. Further, in the current economic climate, some nonprofits may not have enough income to support their current activities. This may result in scrutiny of their financial records. An enhanced public disclosure strategy would help the organization and its managers respond to public inquiries.

Some of the SOA policies which a nonprofit could adopt include the establishment of an audit committee and the adoption of a policy in support of a corporate responsibility program. An audit committee should include at least one member who is familiar with the review of financial records and reporting. A corporate responsibility program could include some or all of the topic areas discussed above, including how the organization will address executive compensation, audits and financial reviews, loans to executives, and whistleblower reporting and actions. Also, a nonprofit organization should review its conflicts of interest policy to determine whether it is appropriate and likely to assist the governing board in isolating potential conflicts of interest and managing such conflicts through to resolution. The governing board of the organization should make sure that there are conflict statements completed with respect to each director.

Conclusion

The promulgation of rules which affect the operations of publicly traded corporations under the Sarbanes-Oxley Act will likely have an impact upon the operations of nonprofit organizations as well. Specifically, the rules which relate to the audit functions of a public company could apply with equal relevance to the operations of nonprofit entities. Further, the guidelines relating to the payment of certain amounts to senior executives is reminiscent of private inurement rules to which nonprofit organizations are already subject. In this regard, some nonprofit organizations have determined to adopt rules which mirror the guidelines established under SOA. In so doing, these organizations are taking a prudent step in conforming to rules which are likely to be looked to as the standard of care for all corporations in the near future. ■

[1] Sarbanes-Oxley Act of 2002 §§ 302-04, 1106, Pub. L. No. 107-204, 116 Stat. 745.

[2] A copy of the report may be found at: http://www.ag.state.mn.us/pdf/corporate_responsibilities_report.pdf.

Cynthia F. Reaves is a partner at Honigman Miller Schwartz and Cohn LLP, and a member of the CCH Healthcare Compliance Editorial Advisory Board.

Fraud & Abuse

No anti-kickback sanctions for hospital-medical group merger

by Richard C. Sarhaddi, Esq., Contributing Editor

In a recently issued advisory opinion, the OIG concluded that it would not impose exclusionary or civil monetary sanctions against either the hospital (Hospital) or the medical group (Group) (collectively, the Requestors) concerning a proposed transaction (Proposal) that would merge the two entities. The OIG came to this conclusion notwithstanding its view that the Proposal could potentially generate prohibited remuneration under the anti-kickback statute if the requisite intent to induce or reward referrals of federal health care program business were present.

The Requestors were once a single entity, but were separated in 1963 when the Hospital was donated to a non-profit corporation. A third entity, a retirement plan and trust for the Group's employees, which owns the building in which the Group is located and leases it to the Group, will also play a role in the merger. The Requestors' plan is a simple merger of the two entities and includes exclusive professional service and administrative service agreements between the Hospital and Group. All of the payment arrangements in the Proposal are consistent with fair market value in arm's-length transactions.

The OIG explained that the transfer of the Group's assets to the Hospital would suggest a potential for remuneration, but emphasized that unless there is some referral of business from the Hospital to the Group in exchange for the Group's assets or remuneration from the Hospital to the Group for its referral of patients to the Hospital, the Proposal would "generate little concern." The OIG focused on three potential sources of remuneration between the parties: (1) the exclusive PSA for services provided at the Hospital clinic, (2) the administrative services agreement, and (3) the purchase of the Group's building.

The OIG concluded that the PSA is unlikely to result in appreciable new business for the Group because the vast majority of patients serviced by the Group at the Hospital will be the Group's current patients. In addition, the PSA provides for a substantially similar compensation package for the Group's practitioners, and all payments made to the Group under the PSA will be consistent with fair market value in arm's-length transactions, as will the amounts that the Group will pay the Hospital under the administrative services agreement. Therefore, the OIG found that there was a low risk of prohibited remuneration associated with this merger transaction, and would not subject the Requestors to administrative sanctions related to the Proposal.

The key to the OIG's decision was that the transactions between the Group and the Hospital would be consistent with fair market value in arm's-length transactions, which severely limited the potential for abusive remuneration activity between the Group and Hospital. The prior relationship between the two entities and the fact that the Group's practitioners would be largely treating the same patients as they did in their previous business arrangement also weighed heavily in the OIG's conclusion. ■

OIG Advisory Opinion 03-15, December 18, 2003, ¶150,212

Suspect ID theft? Report it to the police, experts say

by Catherine Hubbard, MA, Contributing Editor

ID theft victims should report the crime to police as soon as they're aware of a privacy breach. That way they can avoid being punished for the fraudsters' crimes. The recently enacted Fair and Accurate Credit Transactions Act (HR 2622, PL 108-159) requires credit reporting agencies to block or omit information resulting from an identity theft, as long as the consumer has filed a police report.

"It goes completely off the consumer's report and the dispute process is finished," according to Betsy Broder, Assistant Director for the Division of Planning and Information of the Federal Trade Commission's (FTC) Bureau of Consumer Protection. "The police report initiative simplifies a lot of the tasks consumers otherwise would have to take," she said during a December 2 teleconference sponsored by the Health Care Compliance Association. She also recommended that victims obtain a copy of the police report. If a copy is not available, the victim should at least get the report number, said the FTC on its website.

Deal with ID theft head on. Broder said health care organizations also should contact their local police departments whenever a patient tells them their identity has been stolen. After all, she said, the breach might not be an isolated incident. "They may be part of a larger organization."

In addition, instead of sweeping a breach under the carpet, organizations should use the incident as an opportunity to teach employees better privacy practices, said Broder. Often organizations approach the FTC months after a breach, when an ID theft is reported in the press, she said. "The problems are so much worse then, from a public relations, law enforcement and consumer protection perspective," she said.

David Orbuch, executive vice president of compliance and public policy at Allina Hospitals & Clinics, Minneapolis, Minnesota, added that when Allina notifies people of a potential breach, they don't complain, but appreciate the warning.

Broder also advised health care organizations to:

- Direct victims to credit reporting agencies. "If someone contacts you and says your information was the source of ID theft or it has to do with health care treatment, you want to direct them to the credit reporting agencies," she said. "It's likely their information is being used in more than one place."
- Shred rather than discard health care documents. "People easily go through your dumpsters and pull out a treasure trove of data," said Broder.
- Make personally identifiable information available only on a need-to-know basis. "Who are the employees who can look at health records and Social Security Numbers?" she asked.
- Instruct employees and individuals to use strong passwords on accounts (not mother's maiden name), secure personal information from others, keep virus software updated, use a firewall (especially with a 24/7 connection) and encrypt personal information before sending it over the Internet, using secure sites.
- Conduct background checks on employees. In once case an employee at an insurance company in Texas processed a health insurance claim of someone with the same name in Maryland. "She swiped that [social security] number and went to town," Broder said. "Employee security is of the utmost importance," she said.
- Be wary of phishing and pretexting. ID thiefs can pose as health care suppliers and ask to "confirm" names, account numbers and billing addresses, using the information for fraudulent purchases.
- Use the FTC's website (www.ftc.gov) and hotline (877-ID-THEFT) as resources for preventing and responding to ID theft. She also advised companies to refer victims to the FTC's resources. "You want to direct them to the resources available through the FTC so they can immediately contact credit reporting agencies and see if other fraudulent accounts have been opened," she said.
- Download the standard form ID theft affidavit from the FTC site and have it on hand when a person says an identity thief is obtaining health care services under a false name. This form relieves consumers from having to file different forms for each institution affected, Broder said. "We have developed a standard form affidavit, which should be used to dispute accounts at each institution where fraudulent accounts have been opened." She noted that law enforcers and major creditors are using the form. "This ID theft affidavit will do the job."

Health information is susceptible. "Health care organizations are at risk and are very susceptible to ID theft," said Jennifer O'Brien, director of corporate compliance with Allina Hospitals & Clinics, who also participated in the call. "We're looking at how to safeguard patients' as well as employees' SSNs," she said. Allina is working to change reliance on SSNs as an identifier, she said. Patient SSNs are used for billing, insurance cards and registration, she said. Hospitals also collect the SSNs of employees for tax purposes, she noted.

Allina also regularly assesses employee access to patient health information, O'Brien said. "We're trying to make sure we're giving them the minimum amount of access that they need." Health care entities must make sure that when employees leave, their access is terminated. Likewise, when an employee changes jobs within the organization, their access should be reassessed, she said. O'Brien suggested providers review the access both temporary employees and volunteers have to health information and SSNs. ■

CCH Washington Bureau, December 31, 2003