On June 1, 2005, the U.S. Department of Justice ("DOJ"), through the Office of Legal Counsel, issued an Opinion generally limiting the scope of most criminal enforcement under the HIPAA Administrative Simplification rules. While many view the Opinion as the correct interpretation of HIPAA's statutory language, the resulting limitation on enforcement may well make it more difficult for covered entities to carry out the obligations imposed on them by HIPAA to protect the privacy and security of individually identifiable health information.

The Opinion, which is binding on the executive branch of the government, but not on judges, was issued at the request of Alex M. Azar, General Counsel of the Department of Health and Human Services ("HHS"), and Timothy J. Coleman, Senior Counsel to the Deputy Attorney General, and addressed two questions:

- Whether the only persons who may be directly liable for criminal enforcement are those persons to whom the substantive requirements apply, e.g., covered entities such as health plans, health care clearinghouses, health care providers and Medicare prescription drug card sponsors, or whether this provision may also make other persons directly liable, particularly those who obtain protected health information in a manner that causes the covered entity to release the information in violation of HIPAA.

- Whether the "knowingly" element of the HIPAA statute requires only proof of knowledge of the facts constituting the offense or whether this element requires proof of knowledge that the conduct was contrary to the statute or its implementing regulations.
BACKGROUND

The HIPAA statute sets forth a tiered penalty scheme. On the low end, misdemeanors are punishable by a fine of not more than $50,000 and/or imprisonment for not more than one year. If an offense is committed "under false pretenses," violations are punishable by a fine of not more than $100,000 and/or imprisonment for not more than five years. For felony offenses committed "with intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," violations are punishable by fines of up to $250,000 and/or imprisonment of up to ten years. The threat of potential criminal enforcement has been one of the significant motivators in covered entities' compliance efforts.

The only criminal action under HIPAA to date involved an employee of a covered entity, not a covered entity. On November 5, 2004, Richard Gibson, former employee at the Seattle Cancer Care Alliance, was sentenced to sixteen months in federal prison after admitting that he obtained a cancer patient's identity information while he was employed at the facility, and that he used that information to get four credit cards in the patient's name, and to accumulate more than $9,000 in debt in the patient's name. At the time of this enforcement action, there was considerable surprise that the DOJ would choose as its first enforcement action under HIPAA an action against an employee of a covered entity.

THE DOJ'S POSITION

1. **Who May be Prosecuted?**

According to the DOJ Opinion, only covered entities -- health plans, health care clearinghouses, health care providers and Medicare prescription drug card sponsors -- may be prosecuted for violations of HIPAA. Other persons cannot violate HIPAA directly because it "simply does not apply to them."

Nevertheless, the Opinion identifies certain situations where employees may be prosecuted directly under HIPAA. Where the covered entity is not an individual, "general principles of corporate criminal liability will determine the entity's liability and the potential liability of particular individuals who act for the covered entity." While the Opinion declined to elaborate those principles, it cited to Kathleen F. Brickley's treatise on Corporate Criminal Liability, noting that the "conduct of an entity's agents may be imputed to the entity when the agents act on its behalf." Further, the Opinion recognized that, in certain circumstances, the criminal liability of an entity may be attributed to individuals in managerial roles, including individuals with no direct involvement in the offense.

Lastly, the Opinion noted that individuals -- including employees and individuals outside the covered entity -- who may not be prosecuted directly under HIPAA may be prosecuted under principles either of aiding and abetting liability and of conspiracy liability. Although the Opinion declined to elaborate on the contours of this liability, it appears that the DOJ left the door open to prosecute employees who flagrantly cause a
covered entity to violate the statute. Further, in a footnote, the Opinion commented that individual conduct that may not violate HIPAA could violate other federal laws, such as identity theft or fraudulent access of a computer.

2. What is a "Knowing" Violation?

In responding to this question, the Opinion noted that the HIPAA statute prescribes criminal sanctions when a person who knowingly and in violation of this part --

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

Consistent with its ordinary meaning, "the 'knowingly' element is best read to require only proof of knowledge of the facts that constitute the offense." According to the DOJ Opinion, a plain reading of the statute indicates that a person need not know that commission of an act violates HIPAA in order to satisfy the "knowingly" element of the offense. Rather, to incur criminal liability, a defendant need have knowledge only of one of these facts that constitute the offense.

IMPACT OF THIS OPINION

1. Only Covered Entities May Be Prosecuted Under the HIPAA Statute

The DOJ Opinion rules out prosecutions of most employees -- a widely-debated issue since the Gibson case. Thus, where rogue employees act solely for personal gain, in the future it will be harder for prosecutors to prosecute these employees under HIPAA. However, it is likely that egregious cases such as the Gibson case will be prosecuted under other statutes. One recent example occurred at St. Luke's Hospital in St. Louis, where a nurse used her access to patient record information to obtain identity information about two patients in order to obtain credit accounts with which she made purchases. The nurse pleaded guilty to misuse of a social security number and now faces a maximum penalty of 5 years in prison and/or a fine of $250,000 -- sanctions quite similar to those available under HIPAA.

2. Certain Management Employees May Be Subject to Criminal Liability

The most ambiguous part of the DOJ Opinion involves the criminal liability of a covered entity's directors, officers, and agents. The Opinion noted that criminal liability may be attributed to individuals in managerial roles who actually have no direct involvement in an offense. One frequently posed question has been the liability of the Privacy or Security Office for HIPAA violations. To the extent that a "director, officer or
employee" is responsible for the controlling of illegal conduct (i.e., the privacy officer), it is unclear whether criminal prosecution will target such "responsible corporate officers" for criminal violations of employees who cannot be prosecuted under HIPAA.

3. Employees May Face Prosecution Under Other Statutes

As demonstrated by the St. Luke's case, prosecutors are beginning to use other statutes to prosecute privacy and security-related crimes. Depending on the relevant state law, these could include common-law invasion of privacy, computer invasion of privacy, identity theft, mail and wire fraud, and common-law fraud. The DOJ Opinion itself noted that conduct that violated HIPAA's privacy and security rules could, under the right circumstances, be prosecuted under other federal statutes, such as identity theft and fraudulent access of a computer. Thus, even where individual employees may not be prosecuted under HIPAA, they may well be liable under other federal and state laws.

4. Additional Pressure on Covered Entities to Motivate Employees

The general lack of enforcement of HIPAA, together with this Opinion, may remove the fear of HIPAA from many employees and place more pressure on covered entities and their management to institute aggressive internal policies for enforcing HIPAA. However, in light of the wide publicity being given to security breaches in the financial sector and the heightened awareness of health-related privacy and security, it is likely that prosecutors will find other means of prosecuting violations of the HIPAA statute. In their training, covered entity employers would be well advised to make their employees aware that the government has many weapons in its arsenal for pursuing individuals who violate HIPAA -- and it is likely to use them.

*                    *                    *                    *                    *

MCARE NEWS FOR PA HEALTHCARE PROVIDERS

By: Frances R. Roggenbaum, Esquire
1900 Market Street • Philadelphia PA, 19103
717.975.8806 • Fax: 717.975.8772 or froggenbaum@cozen.com

Pennsylvania's MCARE Act provides for two significant changes to mandated medical malpractice insurance to occur as of January 1, 2006. Based upon a recent decision by the PA Insurance Commissioner, only one of the two changes be implemented.

MCARE FUND PHASE-OUT

The MCARE Act provides for a two-step MCARE Fund phase-out, with the first step (an increase in mandated basic coverage limits from $500,000 to $750,000) to occur January 1, 2006 - but only if the PA
Insurance Commissioner determines that there is adequate insurance capacity in Pennsylvania. The Commissioner issued her "capacity" decision on July 8, 2005 (the decision, entitled Findings in Medical Malpractice Insurance Capacity Study, can be found on the PA Insurance Department website at www.ins.state.pa.us). While Commissioner Koken noted improvements in the medical malpractice marketplace since 2002, she decided that there is not sufficient additional capacity in Pennsylvania to increase the amount of mandated basic limits coverage that healthcare providers must purchase from insurers or self-insure. A number of the state's insurers, including provider-owned RRGs, had expressed concern that any decision to increase the amount of mandated basic limits coverage would strain existing insurer capacity and increase reinsurance and premium costs. Thus, the mandated basic limits will remain at $500,000 - at least until the Commissioner makes another capacity assessment in 2007.

EXTINGUISHMENT OF MCARE "TAIL" COVERAGE

Since 1976, Pennsylvania medical malpractice insurers and self-insureds have had some protection from the "long-tail" nature of medical malpractice claims. The MCARE Fund (previously CAT Fund) has provided first dollar coverage for both the claim payments and defense costs for any claim filed against a health care provider more than 4 years after the date of the incident that caused the claim. This protection will no longer exist under any insurance policy issued on or after January 1, 2006 and for any claim against a health care provider filed more than 4 years after an incident that occurs on or after January 1, 2006. Health care providers should expect premium increases to reflect insurer obligations for claims previously covered exclusively by the MCARE Fund. However, because the MCARE Fund will continue to be responsible for "tail" claims that occurred on or before December 31, 2005, providers should not expect a corresponding decrease in the MCARE assessment until the Fund's responsibility for these claims is extinguished. Thus, health care providers may experience higher combined insurance and MCARE costs until this phase-out is complete.

Ms. Roggenbaum joined the firm in May 2005 and concentrates her practice on the corporate, transactional, and regulatory aspects of the insurance industry. She provides regulatory advice to our insurance company clients and assistance to businesses in their self-insurance and risk management strategies. Prior to joining the firm, Ms. Roggenbaum was a partner at Saul Ewing, LLP in Harrisburg.