"Who Goes To Jail?"
A Guide for HIPAA Privacy Officers

By Edward F. Malone, Esq.
Jenner & Block, LLC
Chicago, Illinois

1. OVERVIEW OF HIPAA'S PRIVACY REGULATIONS

On December 28, 2000, the Department of Health and Human Services (HHS) published the final Standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 65 Fed. Reg. 82462 (2000) . These new regulations, which are aimed at protecting confidential health information, must be fully implemented by covered entities by April 14, 2003. Under HIPAA, Congress has provided for either civil or criminal penalties for a violation of the regulations. These enforcement provisions have been codified at 42 U.S.C.A. §§ 1320d-5 to 1320d-6. An understanding of the basics of the enforcement provisions of HIPAA is essential to the position of Privacy Officer, as the Privacy Officer will be responsible for compliance with the regulations, and could ultimately be held to answer for a violation of the regulations. This outline is intended to provide Privacy Officers with an overview of the enforcement provisions of HIPAA and an understanding of the possible consequences of a violation of the regulations.

2. HIPAA PROTECTS INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (45 C.F.R. §§ 164.500, 164.501, 164.514)

1. Protected Health Information (PHI). The privacy regulations cover all individually identifiable information that is transmitted or maintained in electronic, paper, oral, or any other form or medium.

2. Individually Identifiable Information is information that:

    1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

    2. Relates to the past, present, or future physical or mental health care of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care of an individual; and

    3. Can identify, or be used to identify, an individual.

3. Unprotected Health Information. The privacy rule does not apply to:

    1. Health information that does not identify an individual and for which there is no reasonable basis to believe the information can be used to identify an individual.

2. Certain educational records covered by the Family Educational Right and Privacy Act or otherwise described therein.

3. WHO IS SUBJECT TO HIPAA'S PRIVACY REGULATIONS? (45 C.F.R. §§ 160.102, 160.103)

1. Covered Entities. The regulations apply to covered entities, which include:

1. Health plans, which are plans that provide or pay the cost of medical care;

2. Health care clearinghouses, which are entities that process health information from a covered entity; and

3. Health care providers, which are providers of medical or health services that transmit health information in electronic form for billing or for transferring funds for payment.

2. Business Associates. The privacy regulations also apply indirectly to business associates – third parties who may receive PHI from covered entities.

4. HIPAA PROHIBITS DISCLOSURE OF PHI

1. Basic Standard. Covered entities may not use or disclose PHI, except as specifically permitted or required by the regulations. Major permitted and required uses and disclosures of PHI are:

1. Permitted Uses and Disclosures

1. To the individual;

2. With the consent, authorization or agreement of the individual;

3. In certain other circumstances specified in the rule where consent or authorization is not required, including disclosure to business associates.

2. Required Disclosures

1. To the individual when requested in accordance with the requirements of the rule;

2. When required by the Secretary of HHS to investigate or enforce compliance with the requirements of the rule.

2. Minimum Necessary Requirement (45 C.F.R. 164.502(b)). When using or disclosing protected health information, a covered entity must make reasonable efforts to limit disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

5. THE ENFORCEMENT PROVISIONS: 42 U.S.C. §§ 1320d-5 & 1320d-6

The enforcement provisions are not regulations issued by HHS, but rather are Congressionally promulgated statutes that can be found in Title 42 of the United States Code. The relevant sections are generally worded and provide for enforcement through either civil or criminal remedies. Essentially, the enforcement provisions make it unlawful to violate any section of the Regulations and provide criminal penalties for certain wrongful disclosures of protected health information. In the first instance, enforcement will be undertaken by the Office of Civil Rights (OCR) of HHS. If OCR determines that criminal conduct has occurred, it will refer the matter to the Department of Justice.

1. General Penalty for Failure to Comply with Requirements and Standards – 42 U.S.C. § 1320d-5. Under this section, any person who violates any provision of the rules issued by HHS can be penalized not more than $100 for each such violation. Under this section, civil fines are capped at $25,000 per calendar year for each provision of the HIPAA standards that are violated. These civil penalties are also subject to the following limitations:

    1. A penalty may not be imposed under this subsection with respect to an act if the act constitutes an offense punishable under section 1320d-6 (the criminal provision);

    2. A penalty may not be imposed under this subsection if the person can establish to the satisfaction of the Secretary of HHS that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that they violated the provision;

    3. A penalty may not be imposed under this subsection if the failure to comply was due to reasonable cause and not to willful neglect and the failure to comply is corrected within a thirty day time period.

2. Wrongful Disclosure of Individually Identifiable Health Information – 42 U.S.C. § 1320d-6(a). This section of the Code makes it a federal criminal offense to commit any of the following three acts:

    1. To knowingly and in violation of the regulations use or cause to be used a unique health identifier;

    2. To knowingly and in violation of the regulations obtain individually identifiable health information relating to an individual; or

3. To knowingly and in violation of the regulations disclose individually identifiable health information to another person.

Note regarding the criminal enforcement provision requirement that the act be done knowingly and in violation of the regulations:

The use of the word "knowingly" denotes an intention by Congress that the statute can only be violated by a person who does one of the three prohibited acts listed above with the knowledge of the fact that they are doing it. By way of example, a person who accidentally or inadvertently discloses PHI does not do so "knowingly." Therefore, for any person to be criminally convicted, they must have the requisite state of mind. This is in contrast to the civil enforcement provision, which punishes any violation of the regulations, even if accidental or unintentional. In the criminal context, the state of mind required is that the act be done knowingly. A person acts knowingly in regard to a particular fact if: (1) he is aware of the fact; (2) he correctly believes in the existence of the fact; or (3) he accurately suspects that the fact exists and he purposely avoids learning that his suspicions are accurate.

Be careful not to confuse knowledge of a fact with knowledge of the law. The requirement that an act be done "knowingly" does not require that the guilty party knows that they are breaking the law. Rather, a person commits an act "knowingly" when it is done purposefully; that is, the act is a product of a conscious design, intent or plan that it be done. Horne v. State of Indiana, 445 N.E.2d 976 (1983).

In addition to the requirement that the prohibited act be done knowingly, the statute also requires that the act be done in a way that violates the regulations. Because HIPAA's restrictions on disclosure depend in part on who is disclosing the information, who is receiving it, and for what purpose, a disclosure that is permissive for one person could subject another to criminal liability.

3. Criminal Penalties for a Violation of 42 U.S.C. § 1320d-6. Section 1320d-6(b) sets forth the maximum penalties allowable for a violation of § 1320-6(a). Upon conviction, the actual sentence imposed is determined under the Federal Sentencing Guidelines. The Guidelines will be discussed in Section VIII, *infra*. Under § 1320d-6(b), any person who violates subsection (a) shall:

1. Be fined not more than $50,000, imprisoned not more than one year, or both;

2. If the offense is committed under false pretenses,[1] be fined not more than

$100,000, imprisoned not more than 5 years, or both;

3. 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, be fined not more than $250,000, imprisoned not more than 10 years, or both.

6. OTHER STATUTES THAT COULD LEAD TO FURTHER CRIMINAL OR CIVIL LIABILITY FOR VIOLATING HIPAA

1. Wire and Mail Fraud Statutes. A person who has made a wrongful disclosure of private health information may find themselves charged with a mail fraud or wire fraud in addition to a violation of 42 U.S.C. 1320d-6, if the wrongful disclosure was committed under false pretenses.

    1. The mail fraud statute, 18 U.S.C. § 1341 (1994), and the wire fraud statute, 18 U.S.C. 1343 (1994), prohibit the use of the mails or electronic wires to carry out a scheme to defraud a victim of his money or property. It is not important that the scheme actually succeeds in defrauding the victim of his money or property; it is enough that the defendant devise the scheme and make use of the mails or electronic wires to carry it out. Depending on whether a court determines that PHI constitutes "property", a person who uses false pretenses to commit a violation of 42 U.S.C. 1320d-6 may be charged with mail or wire fraud if they use the mails or electronic wires to facilitate the commission of the offense.

    2. The statutes provide that a defendant found guilty of mail or wire fraud shall be subject to a fine of up to $1,000, a prison term of up to 5 years, or both. Furthermore, each use of the mail or of a wire constitutes a separate offense, and thus, can constitute a separate count in the indictment.

2. False Claims Act. The False Claims Act, 31 U.S.C. §3729 (1994), punishes a defendant for knowingly or with reckless disregard for the truth, making false statements to the government in connection with a claim for money or reimbursement. The False Claims Act can apply even when the actual request for payment is neither false nor fraudulent. Liability can be imposed when a defendant, as required by the government, certifies that it is in compliance with a separate statute, law or regulation in order to obtain payment when it is in fact not in compliance with that statute, law or regulation.

    1. It is likely, that in order to be reimbursed by Medicare, the government may require a certification from the requesting entity that it is in compliance with HIPAA. If the health care provider, insurance company or HMO that is submitting the Medicare claim knows or should have known that they have

disclosed PHI and nevertheless signs such a certification, that covered entity could have a complaint brought against them under the False Claims Act.

2. The False Claims Act provides for a civil penalty of not less than $5,000 and not more than $10,000 plus three times the amount of damages which the government sustains because of the false claim. In addition, the government can also bring criminal charges under 18 U.S.C. § 1001 (1994), which prohibits making any false statements to the government.

7. POTENTIAL BASES FOR CRIMINAL LIABILITY

1. Employee Liability for Employee's Own Conduct. An individual is criminally accountable for his or her own actions, even when those actions are performed for the benefit of the employer or in the individual's official capacity. Furthermore, an employee cannot escape liability on the ground that his or her conduct was ordered by a supervisor. Finally, an individual can be criminally liable even when the employee does not personally perform the wrongful act; as in any other context, an employee may be liable for conspiracy or aiding and abetting.

2. Liability of Privacy Officers. Privacy Officers are not exposed to a greater risk of criminal liability than other employees solely on the basis of their position as a Privacy Officer. Unlike the corporation as an entity, the Privacy Officer cannot be held criminally liable for another employee's criminal act. A Privacy Officer cannot be held criminally liable for a criminal violation committed on "their watch" unless they themselves also participated in the criminal act through planning, participating in, or covering up its commission.

3. Corporate Liability for Acts of Employees. Corporations are generally considered subject to criminal statutes unless the statute specifically provides otherwise. A corporation can be held criminally liable for an act if an officer, employee or agent commits a crime within the scope of his actual or apparent authority with the intent to benefit the corporation, regardless of whether the corporation actually benefitted and regardless of whether the employee also intended to benefit himself.

4. Concurrent Liability of Employees and Corporation. Conviction of either the corporation or the employee does not preclude conviction of the other. Acquittal of corporate agents does not preclude a finding of corporate liability. Similarly, an employee may be convicted even though the corporation charged on the basis of that employee's actions is acquitted.

8. THE FEDERAL SENTENCING GUIDELINES

In federal court, sentences for violations of criminal statutes are determined by the judge under the Federal Sentencing Guidelines promulgated by the United States Sentencing Commission. The aim of the Guidelines is to make uniform the punishment that is applied to similarly situated defendants upon conviction. To achieve this result, the Guidelines apply an almost mechanical approach to determining a sentence. The two most important considerations in this approach are the offense level and criminal history category.

1. Determining the Offense Level. To determine the offense level, a judge selects the applicable guideline section that corresponds with the defendant's relevant conduct, determines the base level from that section, and then adjusts that offense level for any specific offense characteristics contained in that particular section. Under the Guidelines, the offense level is assigned a numerical value between 1 and 43.

2. Determining Criminal History Category. In determining the defendant's criminal history category, the sentencing judge assigns the defendant criminal history points based upon the defendant's past criminal conduct. The points are then totaled up and the defendant is assigned a criminal history category. The criminal history categories range from I - VI.

3. Determining the Sentence. Once the judge has determined the total offense level and the criminal history category, the sentencing judge simply matches these two figures up in the sentencing table and identifies the appropriate sentencing range. Within this range, the judge must then choose a sentence that is consistent with the overall goal of the Guidelines. The judge is allowed limited discretion to depart from the applicable sentencing range if the court finds that the case includes an aggravating or mitigating circumstance that the Sentencing Commission did not adequately consider or if the government makes a motion for downward departure based on substantial assistance. Pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a judge cannot depart upward beyond the statutory maximum.

4. Probable Sentencing for Violations of 42 U.S.C. § 1320d-6. The Guidelines have not yet assigned an offense level to violations of 42 U.S.C. § 1320d-6. It is likely, however, that the offense level will be comparable to the levels assigned for comparable crimes. The section currently in the Guidelines that is most comparable to a violation of 42 U.S.C. § 1320d-6 is Part H (3) dealing with privacy and eavesdropping. Section 2H3.1 defines the offense level for a crime dealing with interception of communications or eavesdropping. Section 2H3.1 assigns crimes of this type a base offense level of 9. If the purpose of the punishable conduct was to obtain direct or indirect commercial advantage or economic gain, the offense level is increased by three levels to 12.

    1. Under the Guidelines, an offense level of 9 has a sentencing range of between 4 and 27 months of imprisonment depending on the defendant's criminal

history category. The sentencing range for a defendant with a criminal history category of I (the lowest) is between 4 and 10 months of imprisonment.

2. Under the Guidelines, an offense level of 12 has a sentencing range of between 10 and 37 months of imprisonment depending on the defendant's criminal history category. The sentencing range for a defendant with a criminal history category of I (the lowest) is between 10 and 16 months of imprisonment.

3. If the criminal defendant is an organization, the Guidelines likewise proscribe a method for determining the organization's sentence. First the offense level is used to determine the base fine. An offense level of 9 carries a base fine of $15,000. An offense level of 12 carries a base fine of $40,000. Next, the court determines the organization's culpability score. A variety of factors including involvement in or tolerance of criminal activity, prior history, violation of an order, obstruction of justice and cooperation are used to arrive at the culpability score. The culpability score is then used to determine a minimum and maximum multiplier. The multiplier is then multiplied by the base fine to determine a final fine range. The multipliers range from a minimum of 0.05 to a maximum of 4.00.

9. MINIMIZING CORPORATE EXPOSURE TO CIVIL AND CRIMINAL LIABILITY BY CONDUCTING INTERNAL INVESTIGATIONS

No matter how much effort is spent on prevention, no corporation is immune from employee misconduct. Once misconduct is suspected, the next step is to determine what occurred. An internal corporate investigation is a factual and legal inquiry into possible illegal conduct by a corporation and its employees, performed by investigators authorized by the corporation itself. This section reviews reasons for initiating an internal investigation and practical considerations governing their implementation and the use of their results.

1. Reasons for Conducting an Internal Investigation.

1. Ensuring Compliance with the Regulations. As part of the compliance program imposed by the regulations, covered entities are expected to process complaints, apply appropriate sanctions against its employees, and mitigate any harmful effects that result from the use or disclosure of protected health information. An internal investigation will assist the corporation in determining the extent of potential criminal or civil liability so that it can make informed decisions for dealing with these situations.

2. Information Gathering – Determining the Facts and Available Defenses. Without knowledge of the underlying facts and the available defenses that those facts permit, the corporation will be impaired in its effort to negotiate a favorable resolution of any violation and in its efforts to defend itself at trial.

Through development of the facts and an analysis of the applicable law, an internal investigation will assist the corporation in determining how to respond to charges of wrongdoing and how to prevent future recurrences.

3. Use in Negotiations with the Government. If the corporation effectively investigates its own misconduct, it may persuade the government not to conduct a separate intrusive investigation or at least to reduce the scope of its investigation. A thorough investigation, combined with voluntary disclosure, may also be the determinative factor in convincing the government not to bring criminal charges or other proceedings.

4. Use at Sentencing. If despite all efforts to the contrary, the corporation is convicted of a crime, the internal investigation may be presented at sentencing as a mitigating factor to reduce the culpability score and accordingly the eventual sentence.

5. Public Relations. The corporation can use an internal investigation to minimize the PR impact of any wrongdoing. The investigation distances the corporation from any wrongful acts by its employees, and the very fact that it has been launched demonstrates the corporation's good faith. Such good faith efforts may also help to restore or maintain investor confidence.

2. Costs and Risks Associated with Conducting an Internal Investigations.

1. Expense. Internal investigations can be very costly, particularly if outside counsel is used and there are a large number of witnesses and relevant documents. In addition to the costs of outside professionals, the corporation may lose employee time and productivity from the diversion of resources and a possible loss of morale.

2. Disclosure of Information. It is likely that the results of the investigation will be disclosed to the government, potential plaintiffs, or to the public. Plaintiffs may be able to use the resulting report as a guide to litigation and as evidence of wrongdoing. Even in absence of such disclosure, however, such plaintiffs still may be able to gain the necessary information through discovery.

3. Triggering Enforcement Actions. Although the government seeks to encourage voluntary disclosures, there is no guarantee that voluntary disclosure will immunize the corporation from an enforcement action or induce government leniency. Disclosure of the results could bring about civil or criminal litigation that would otherwise not occur.

4. Triggering Collateral Litigation. A corporation that investigates misconduct and follows through on the results of the investigation may find itself subject to other lawsuits, particularly by employees that were disciplined.

3. Best Practices – Conducting Internal Investigations so as to Maximize Benefits and Minimize Risks.

1. Inside v. Outside Counsel. Counsel should have the primary role in overseeing the investigation. This will maximize confidentiality through the availability of attorney-client and work product privileges. Where the misconduct involved is not substantial, the investigation may be conducted by in-house counsel. In more significant cases, it is best for the investigation to be conducted or overseen by outside counsel, particularly where in-house counsel may be a witness or where senior management is implicated. Although in-house counsel bring familiarity with the company and its programs and thus are more readily accepted by employees, outside counsel may bring greater objectivity and credibility due to their relative lack of familiarity with the company and their reduced self-interest in validating the conduct. Finally, outside counsel may have a greater ability to achieve confidentiality because there is a reduced risk that communications will be perceived as involving business advice rather than legal advice.

2. Maintaining Confidentiality – Cloak Investigation with Privilege. The investigation should be initiated under circumstances that make it clear that it is for the purpose of providing legal advice rather than just investigation of facts or business advice. As few non-attorneys as possible should be involved. Non-legal personnel should be directly supervised by attorneys. If non-legal outside experts are necessary, they should be hired by counsel rather than by the corporation. All privileged communications should be clearly marked to indicate "privileged attorney client communication" and recipients as well as all employees should be given instructions concerning the need for confidentiality.

3. Document Review. Relevant documents should often be reviewed before employees are interviewed. The documents may guide counsel's strategy by identifying the important witnesses and focusing the questions that must be asked during interviews. Document review procedures should be structured in such a way as to avoid later duplication in the event of eventual litigation. Furthermore, it is essential to prevent the destruction of possibly relevant documents. The destruction of relevant documents will be interpreted – by the government, by courts or by the public as an admission of culpability.

4. Witness Interviews. In a large scale investigation in which middle or lower level employees will be interviewed, it is often advisable to provide employees with written information concerning the purpose and circumstances of the interview. Employees should generally be told the following before any interview:

1. Counsel represents solely the corporation and is conducting the interview for the sole purposes of formulating legal advice for the corporation;

2. Counsel has determined that it is necessary to talk with the employee in order to formulate legal advice for the corporation;

3. The employee will be asked about certain matters relevant to the investigation and he or she is expected to cooperate fully and to provide complete and accurate information;

4. The investigation is highly confidential, and the information provided by the employee is confidential and will be kept in confidential files, but the corporation itself will determine whether to keep the information confidential and may ultimately decide to disclose it; and

5. The employee should not disclose confidential information to anyone without the consent of the appropriate official (such as in-house counsel).

Interviews should be conducted by counsel. Counsel should take notes of interviews and incorporate in these notes their impressions, analyses and opinions. In some instances, particularly where the employee is likely to have engaged in criminal conduct and the corporation wants to protect its ability to use the employee statement in subsequent litigation against the employee, the investigator may wish to suggest that the employee consult an attorney. More often, the investigators should be neutral on this point and should particularly avoid discouraging the employee from consulting an attorney. Finally, refusal of an employee to cooperate in an internal investigation is generally an appropriate ground for discharge.

5. Dealing with a Simultaneous Government Investigation. Employees should be directed to compile documents responsive to subpoenas and deliver them to counsel for delivery to the government. Counsel should actively and closely supervise this process. In advance of government interviews, employees should be informed that the government may wish to interview them in connection with an investigation and that the corporation is represented by counsel in that investigation. The employees should be told of any arrangements the corporation has made for providing independent counsel to employees. The corporation should explain the role of counsel and make clear that decisions concerning consultation with independent counsel rests with the employees. Finally, employees should be told to be truthful during the interview.

6. Using Experts. Although it may sometimes be helpful to have experts available to assist counsel in reviewing and analyzing documents or preparing

for witness interviews, the use of outside experts increases the possibility of involuntary disclosure of sensitive information. Such experts should accordingly be retained only when absolutely necessary. In order to minimize the possibility of waiver, care should be taken to ensure that if experts are employed, they are retained by and are responsible only to the attorneys conducting the investigation.

7. Representing Employees - Conflict Concerns. There is an inherent potential for a conflict of interest between the corporation and its employees. Accordingly, counsel performing the investigation should represent the corporation alone. If it is later determined that there is no conflict of interest, the corporation's counsel may be able to represent employees as well during subsequent judicial proceedings.

8. Preparing the Investigative Report. At the conclusion of the investigation, a written report is normally prepared addressed to the individual or committee which ordered the internal investigation. The report generally will summarize the circumstances which led to the investigation; detail the investigative steps which were taken; summarize the facts revealed by the investigation; analyze the applicable law; develop the arguments for and against liability, prosecution, or sanctions; identify internal policies, procedures or practices which led to the events or which could be improved to prevent future violations; and recommend any appropriate remedial actions. The report should also describe facts and circumstances that reflect well on the corporation. Eventual disclosure of the report will then include positive evidence that may influence the government or a court. For example, the report may show how the corporation’s compliance program was effective in discovering and addressing the violation.

9. Benefits of Disclosure of the Results of an Investigation. There is no general duty to disclose misconduct to the government. The corporation may still have reason, however, to make a voluntary disclosure of the results of the internal investigation. In keeping with the government’s emphasis on encouraging internal investigations, many government agencies, including the Department of Justice, have developed policies in which voluntary disclosures are rewarded. HHS may develop such a policy in connection with its HIPAA enforcement. Failure to disclose any violation uncovered by the investigation may also create potential dangers that far outweigh the corporation's short-term interest in confidentiality. If wrongdoing does surface, the corporation will lose the benefits of cooperation and will instead be faced with the aggravating circumstance of having engaged in a "cover-up." Furthermore, the failure to report the incident may create an environment in which employees take legal obligations less seriously and future misconduct may become more likely. Finally, subsequent violations will be more damaging than they otherwise would be, and the corporation will be less able to

convince the government or a court that it has an effective compliance program.

10. Risks of Disclosure of the Results of an Investigation. Voluntary disclosure of the results of an investigation may subject the company, officers and/or employees to criminal liability and/or civil sanctions that otherwise would not arise. Furthermore, the corporation must consider the possibility that the government will not factor in the voluntary disclosure, and will nevertheless proceed with full criminal prosecution. Finally, there may also be a chilling effect on employees whose answers may be less forthcoming if they know that their answers will, or may, be disclosed.

10. APPLICATION TO A HYPOTHETICAL SITUATION

A hypothetical fact pattern will be handed out at this point in the presentation. The hypothetical will confront the privacy officers with a situation in which they are alerted to the possibility of a HIPAA violation by an employee. The application will discuss liability issues and will provide practical advice on handling a hypothetical internal investigation.

660673 v2