# Federal Agencies Diverge on the Application of HIPAA's Civil and Criminal Penalties

***By John Aloysius Cogan, Jr., Esq.***

The two federal agencies charged with enforcing the privacy provisions of the Health insurance Portability and Accountability Act of 1996 (HIPAA) have taken diverging approaches to the enforcement of HIPAA. As a result, the field of possible targets for a government enforcement action has been expanded to include persons and businesses not originally thought to be covered by HIPAA. This change raises oversight and compliance issues for nearly every business or person that may have access to health information related to an individual, referred to by HIPAA as "protected health information" (PHI). In addition, the employees of such businesses are now at risk under HIPAA's criminal provisions. This new development means that businesses thought previously to be exempt from HIPAA should consider implementing a training program and taking steps to establish oversight of any activity involving the use or disclosure of PHI.

## Differing Views by HHS and DOJ

Since the initial compliance date for the HIPAA Privacy Rule, the United States Department of Health and Human Services (HHS), the federal agency charged with the civil enforcement of HIPAA, has taken the position that only so-called "covered entities" are subject to civil penalties under HIPAA. "Covered entities" (CEs) include not only health care providers and health care clearinghouses (entities that convert data from one format to another for billing or other purposes), but also health plans. Conversely, HHS has made clear that persons and entities with access to PHI, but not falling within the definition of a CE, are not subject to civil penalties. These non-CEs include employees, vendors, and third-party administrators. Now, the Department of Justice (DOJ), the federal agency charged with enforcement of HIPAA's criminal provisions, has taken a radically different position with respect to persons and entities subject to penalties under HIPAA's criminal provisions.

For nearly a year now, DOJ attorneys have suggested that HIPAA's criminal penalties are applicable to anyone violating HIPAA, not just CEs. Under this interpretation of HIPAA, employees, business associates, and anyone else who knowingly uses or discloses PHI in a manner prohibited by HIPAA is subject to criminal penalties. DOJ recently applied this broad enforcement theory by indicting a non-CE for a HIPAA violation.

## DOJ Lowers the Boom On a Non-CE

On August 19, 2004, a former cancer clinic employee pleaded guilty in federal court to wrongful disclosure of PHI for economic gain. In his plea agreement, the employee admitted that he had obtained a cancer patient's PHI, including the patient's name, date of birth and social security number, and had disclosed that information in order to obtain credit cards in the patient's name. The employee used the cards to purchase thousands of dollars worth of various items for his personal use.

The most interesting aspect of this prosecution is that the employee is not a CE. Thus, while the employee was exempt from any civil penalty under HIPAA, he now faces 10 to 16 months in prison under HIPAA's criminal provisions.

## Implications of the First Prosecution of a HIPAA Violation

The first HIPAA guilty plea should serve as a warning to both CEs and non-CEs alike. Businesses that have access to PHI must take steps to assess (or re-assess) their level of HIPAA compliance. Those businesses should also ensure that their employees observe HIPAA's requirements. In short, anyone who handles PHI—regardless of their status as a CE—must formulate and adhere to policies and procedures that meet HIPAA's requirements.

***This article appeared in the October 2004 edition of New England In-House.***