HHS News

FOR IMMEDIATE RELEASE
Thursday, July 17, 2008

HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information

The U.S. Department of Health & Human Services (HHS) has entered into a Resolution Agreement with Seattle-based Providence Health & Services (Providence) to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. In the agreement, Providence agrees to pay $100,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against theft or loss.

The Privacy and Security Rules are enforced by HHS' Office for Civil Rights (OCR) and the Centers for Medicare & Medicaid Services (CMS). The Privacy and Security Rules require health plans, health care clearinghouses and most health care providers (covered entities) to safeguard the privacy of certain individually identifiable health information and meet additional security standards for patient information maintained in electronic form. The Resolution Agreement relates to Providence's loss of electronic backup media and laptop computers containing individually identifiable health information in 2005 and 2006.

Winston Wilkinson, the director of the OCR, stated, "We are committed to effective enforcement of health information privacy and security protections for consumers. Other covered entities that are not in compliance with the Privacy and Security Rules may face similar action."

While OCR and CMS have successfully resolved over 6,700 Privacy and Security Rule cases by requiring the entities to make systemic changes to their health information privacy and security practices, this is the first time HHS has required a Resolution Agreement from a covered entity. Providence's cooperation with OCR and CMS allowed HHS to resolve this case without the need to impose a civil money penalty.

Director Wilkinson noted, "We commend Providence for their cooperation during the course of the investigation and for their voluntary implementation of comprehensive and system-wide improvements to protect individually identifiable health information."

The incidents giving rise to the agreement involved two entities within the Providence health system, Providence Home and Community Services and Providence Hospice and Home Care. On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the Providence premises and were left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients. HHS received over 30 complaints

about the stolen tapes and disks, submitted after Providence, pursuant to state notification laws, informed patients of the theft. Providence also reported the stolen media to HHS. OCR and CMS together focused their investigations on Providence's failure to implement policies and procedures to safeguard this information.

Under the Resolution Agreement, Providence agrees to pay a $100,000 resolution amount to HHS and implement a robust Corrective Action Plan that requires: revising its policies and procedures regarding physical and technical safeguards (e.g., encryption) governing off-site transport and storage of electronic media containing patient information, subject to HHS approval; training workforce members on the safeguards; conducting audits and site visits of facilities; and submitting compliance reports to HHS for a period of three years.

"The protection of patient information is a top priority for Providence Health & Services," stated Providence's Chief Information Security Officer Eric Cowperthwaite. "Since these incidents occurred, we have reinforced our security protocols and implemented new data protection measures. Under the terms of the agreement, we will continue to implement appropriate policies, procedures and training."

Kerry Weems, the acting administrator of CMS, commented, "This resolution confirms that effective compliance means more than just having written policies and procedures. To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features."

The Resolution Agreement and Corrective Action Plan can be found on the OCR Web site at http://www.hhs.gov/ocr/privacy/enforcement/.