



HHS Issues Guidance on the Protection of Personally Identifiable Health Information

In compliance with the American Recovery and Reinvestment Act ("ARRA"), HHS issued guidance today on technology and methods for protecting personally identifiable healthcare information by encrypting or destroying it so that it is rendered "unusable, unreadable, or indecipherable to unauthorized individuals." HHS was required to publish this guidance by April 18, 2009.

The HHS guidance provides steps entities can take to ensure personal health information is secure and establishes the trigger for notification following a breach. ARRA requires both HHS and the FTC to issue "breach notification" regulations within 180 days of enactment of the bill. The HHS regulation will govern entities covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the FTC regulation will govern vendors of personal health records and certain other entities not covered by HIPAA.

The guidance, developed by the HHS Office for Civil Rights, Office of the National Coordinator for Health Information Technology, and Centers for Medicare & Medicaid Services, can be found at the following address: www.hhs.gov/ocr/privacy.