



The Use of Pearl Echo to Assist in Compliance with

The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996. The intent of HIPAA is to improve the portability, continuity and accessibility of health insurance coverage. Subtitle F of HIPAA, Administrative Simplification, encourages the development of health information systems in order to facilitate the electronic transmission of certain health information. In creating such systems, the health care provider is required to maintain technical and physical safeguards to ensure the confidentiality and unauthorized disclosure of patient information.

Confidentiality

Pearl Echo's control profiles provide healthcare providers with the ability to define rules determining which users have access to specific areas of the organization's intranet. By creating access profiles within Pearl Echo, health providers will not only be able to control which individuals have access to patient data through the organization's intranet, but will be able to audit who, internally, is attempting to erroneously access patient data. Subtitle F of HIPAA specifically delineates security standards that address the value of audit trails in computerized record systems.

Disclosure

Disclosure of patient data can take on many forms including the electronic transmission of nonpublic personal information through e-mail, chat rooms, instant messaging and public news group postings. Pearl Echo's keyword blocking capability can be employed to prevent the dissemination of personal information through any of these protocols. Pearl Echo can also be used to monitor the communications of individuals in order to identify the intent to access and distribute nonpublic personal information before it occurs.

Individuals who wrongfully disclose a patient's health information are subject to fines ranging to \$250,000 and prison time ranging to 10 years. Pearl Echo's archival capability can be employed by organizations to easily and cost effectively provide proof of internal controls that prohibit general access to patient related information and to disprove allegations of improper disclosure through electronic communications.



REFERENCE:

Law: Health Insurance Portability and Accountability Act
Bill Number: H.R.3103
Year: 1996

WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

` SEC. 1177. (a) OFFENSE- 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,

shall be punished as provided in subsection (b).

` (b) PENALTIES- A person described in subsection (a) shall--

` (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;

` (2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and

` (3) if the offense is committed with 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) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION- The term `individually identifiable health information' means any information, including demographic information collected from an individual, that--

` (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

` (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

` (i) identifies the individual; or

` (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

` (d) SECURITY STANDARDS FOR HEALTH INFORMATION-

` (1) SECURITY STANDARDS- The Secretary shall adopt security standards that--

` (A) take into account--

- ` (i) the technical capabilities of record systems used to maintain health information;
- ` (ii) the costs of security measures;
- ` (iii) the need for training persons who have access to health information;
- ` (iv) the value of audit trails in computerized record systems; and
- ` (v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and
- ` (B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.
- ` (2) SAFEGUARDS- Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--
 - ` (A) to ensure the integrity and confidentiality of the information;
 - ` (B) to protect against any reasonably anticipated--
 - ` (i) threats or hazards to the security or integrity of the information; and
 - ` (ii) unauthorized uses or disclosures of the information; and
 - ` (C) otherwise to ensure compliance with this part by the officers and employees of such person.