

HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), also known as HIPAA, was enacted as part of a broad Congressional attempt at incremental healthcare reform. The "Administrative Simplification" aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients.

These standards are designed to:

Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions.

Protect the security and confidentiality of electronic health information.

The requirements outlined by the law and the regulations promulgated by DHHS are far-reaching--all healthcare organizations that maintain or transmit electronic health information must comply. This includes health plans, healthcare clearinghouses, and healthcare providers, from large integrated delivery networks to individual physician offices. After the final standards are adopted, small health plans have 36 months to comply. Others, including healthcare providers, must comply within 24 months.

HIPAA Compliance and PedCath7

Scientific Software Solutions has taken a multi-level approach to ensure that the new PedCath7 satisfies the HIPAA privacy regulations.

1. Our assumptions about your institution's HIPAA compliance

HIPAA requires certain physical safeguards to guard data integrity, confidentiality, and availability. These safeguards protect physical computer systems and related buildings and equipment from fire and other environmental hazards as well as intrusion. The use of locks, keys and administrative measures used to control access to computer systems and facilities are also included.

At a minimum, all health plans, clearinghouses, and healthcare providers that transmit or maintain electronic health information must conduct a risk assessment and develop a security plan to protect this information. They must also document these measures, keep them current and train their employees on appropriate security procedures.

We assume your institution or office complies with these requirements and that PedCath is installed behind your hospital firewall.

2. Technical security mechanisms.

These include processes used to prevent unauthorized access to data transmitted over a communications network.

2a) User Validation - PedCath7 validates who is using the software with sign-in and encrypted password procedures. 2b) Need-to-know Access - PedCath7 has 6 different user levels. Each user is assigned an appropriate level, ranging from no access to full administrative access.

3. Audit Trail - PedCath7 keeps an audit trail log, which records who accesses what information and when. PedCath7 records every access (including read-only access).

4. Standardized Codes for Diagnosis, inpatient services, procedures and physician services - The new regulations are an effort to reduce paper work and increase efficiency and accuracy through the use of standardized financial and administrative transactions and data elements for transactions. HIPAA will change this practice by requiring payers to accept the following transaction standards for EDI:

Diagnoses and inpatient hospital services: International Classification of Diseases, 9th edition, Clinical Modification (ICD-9-CM). The standard will migrate to ICD-10 whenever the new system is ready for adoption.

Procedures: ICD-9-CM Volume 3 and HCFA Common Procedural Coding System (HCPCS)

Physician services: Current Procedural Terminology (CPT)

Each of the above standard code sets is supported by PedCath7.

5. Unique Identifiers

HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services (patients). Only the patient identifier affects PedCath. This is the most controversial of the proposed identifiers and is on hold pending privacy legislation. However, industry experts speculate that the identifier will consist of approximately ten numeric digits with a check digit.

In the interim, PedCath allows for two unique patient identifiers. One is your institution's Medical Record Number (MRN) and allows up to 12 alpha-numeric characters. The other is an internal PedCath index number, seen as the first of 2 numbers to the right of the Edit Cath button on the Browse screen.

6. Implementation Strategy

Even though HIPAA standards are still being finalized, healthcare organizations must move quickly to develop and implement compliance plans. Accordingly, Scientific Software Solutions recommends that PedCath users follow the following procedures.

Obtain copies of the proposed rules from the Department of Health and Human Services' comprehensive HIPAA website. Go to <http://aspe.os.dhhs.gov/admnsimp/>

Identify key individuals in your organization to spearhead compliance efforts. Let us know who we should contact as regulations evolve.

Educate your staff, physicians and other key constituents about HIPAA.

Sign up with Scientific Software Solutions for e-mail notification of the latest developments.

Make sure your PedCath7 annual license is maintained. PedCath7 requires a current license to assure continued HIPAA compliance. Make sure we have up-to-date contact information on whom to notify when annual license fees are due.

Important Information for PedCath3 users.

PedCath3 IS NOT HIPAA COMPLIANT.

Please contact us at 1-434-293-7661

or HIPAA@PedHeart.com for additional information about your mission critical software.