



PCA and HIPAA Compliance

Practical Computer Applications Inc (PCA) provides database application software consulting, design and development engineering services to enable public and private healthcare product and service providers to comply with the HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA).

Information that is protected under HIPAA includes individually identifiable information that is transmitted or maintained in any form or medium that is created or received by the covered entity, that relates to the physical or mental health of an individual or payment for the provision of health care to an individual, and could be used to identify the person. Examples of protected health information include:

- Patient name
- Geographic subdivisions smaller than a state
- Dates, including birth date, admission date, discharge date, date of death, all ages over 89
- Telephone and fax numbers
- Email addresses
- Social Security numbers
- Medical record and account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric indicators
- Photographs
- Unique identifying number, characteristic, or code

PCA adheres to a number of business and technology practices to insure HIPAA-compliance when implementing custom database application solutions for public and private healthcare product and service providers, including:

Smart Client Architecture

PCA's Smart Client application architecture — based upon the Microsoft SQL Server 2005 and .Net 2.0 Framework — supports HIPAA standards for electronic information storage, encryption, transfer and processing of patient-sensitive healthcare and patient data. Data storage, transfer and access are essential considerations in designing modern, healthcare databases and advanced applications. Full compliance of HIPAA regulations require organizations to maintain rigorous policies and procedures in data handling as well as technically secure infrastructure. Global language within the specification also points out the value of Audit Trails and holistic Data Integrity as primary business considerations.



Secure Data Transport Layer

Smart Client applications connect to a SQL Server database through the standard Ports 80 and 443. Port 443 is used with secure encrypted SSL for data where HIPAA compliance is mandated. All data packets transmitted between the database and the application are compressed in a binary format, hence unintelligible to any intrusion or sniffer that may inadvertently (or purposefully) be exposed to one or more data packets. PCA's compression also substantially improves application performance. Further, Smart Clients function well in standard HTTP, HTTPS, SSL, VPN and Digital Certificate environments.

User Access and Security

Smart Client applications use a standard, Admin-managed, Role-based Security framework to manage all End User access to and use-privileges within the application. Security settings are stored in the SQL Server database. Administrators can assign and manage different use-privileges to different healthcare practice workers e.g. Physicians, Nurses, Case-management Workers, etc.

Server Database/SQL Storage and Encryption

Server based database security and management is a core consideration in the HIPAA requirements. MS SQL Server fully complies with technical requirements for server-side data storage. Data elements for HIPAA patient and case data can be stored, tracked and secured in any variety of methods supported by SQL Server.

Client Data Storage and Encryption

MS Smart Client architecture provides considerable power for processing on a users' PC, once application data is delivered from a SQL database through a secure transfer process. Specific patient or medical data is received from the (SQL) server for various user-related needs; data input, refinement, and reporting for example. During this time, a secure connection is maintained between the Server and Client application. Application data only exists on the Client PC during the application session. Once a User logs-out (or following a pre-determined time of inactivity), *all* the application data is removed from the local computer.

Automated Application Deployment and Maintenance

Smart Client applications can be deployed to any PC that is connected to the Internet/Intranet and capable of supporting the .Net Application framework. Once deployed, Smart Client software applications automatically update themselves to the latest version of Application that resides on the centralized server. This simplified deployment helps to ensure that users have the latest version of the application as well significantly lowering IT deployment and maintenance costs.