

The Challenge of Protecting Electronic Medical Data

medXchange

**META DATA BASE AND INFORMATION SYSTEM
FOR MEDICAL AND HEALTH MANAGEMENT**

MedXchange AG

Tel: +41 (0)1 212 44 46
Fax: +41 (0)1 212 44 45

Augustinergasse 17
CH-8001 Zurich, Switzerland

www.medxchange.org
info@medxchange.org

Data Protection Law

International data protection laws have a number of provisions to ensure personal health data can be accessed and viewed by the individual and that any health data divulged to a third party is anonymous and cannot be associated with an individual. The following provisions are generally covered in international and national data protection laws.

Processing Personal Data

Personal health data should only be stored on the express consent of the individual and the healthcare professional. This health data is stored in such a manner that it contains no nominative information and cannot be traced to the individual.

Data Accuracy

Registered healthcare professionals with the express permission of the individual should enter all medical data. The individual should be able consult his own medical information and request the healthcare professional for any rectification of inaccurate medical data in the case of a contest. The individual can authorize any participating Healthcare Professional to access and update his medical data. This includes a replacing Healthcare Professional, a Healthcare specialist or a Healthcare Professional in another geography or country.

Trans-border Data Flows

As long as electronic medical data is stored anonymously, there are no legal restrictions on storing medical data outside national borders for the purpose of processing or statistical research.

Right of Access

The individual should be able to directly or indirectly access his own medical data unless restricted by the Healthcare Professional. The individual owns, and should be able to manage and control all information within his/her health record with the input of a healthcare professional for medical credibility and accuracy.

Non-disclosure of Data

Medical data should not be nominative and is only identifiable by codes known only to the individual and the healthcare professional of choice. Medical data can only be disclosed with the express permission and under control of the individual.

Infringement of privacy

Anonymous medical data is processed for statistical and research purposes. Medical data and statistics cannot be linked to an individual.

Implementing a Secure Electronic Medical Record

To maintain strict confidentiality of individual health data, a number of technologies and platforms have been developed by *medXchange* to provide a highly secure environment.

Anonymity

The information collected, other than information strictly limited to emergency situations, does not contain any nominative information such as name, address or any other identifying information in order to ensure anonymity. Therefore, a medical documentation and data cannot be linked to an individual. The only identifier stored on the database is the confidential code and password of an individual. With the omission of nominative data, *medXchange* is able to guarantee the security and privacy of individual health information.

Health Data Access Management

medXchange applies the following principles to Health and Medical Data access management.

- ✍ The individual is the owner of his medical information and must give his consent to a Healthcare Professional to access and update this information.
- ✍ Only the individual or a registered and/or accredited healthcare professional can consult individual Health Data.
- ✍ Only an individual may enter and modify personal health data of his/her own record.
- ✍ The detailed health and medical data of an individual may be viewed, entered and modified by a registered healthcare professional with the express consent of the individual. The healthcare professional requires both his own access code and the individual's access code to view and modify individual health data. An individual is immediately informed when a change has been applied to his/her record.
- ✍ All changes and updates to an individual's medical data are tracked and the individual is notified by e-mail that changes have been made and by whom. The change notifications are tracked and can be traced at any time on request.
- ✍ In the case of a lost Health Key, the owner's record can be traced through his Health number and password and a new Health Key issued.
- ✍ An individual can terminate his participation in the Health Key at any time and "lock" his health data by changing his password and PIN number.
- ✍ Since we do not store nominative information, in the case of a corporate health program or a health insurance program, the employer or health insurer is not aware if an individual has consulted a Healthcare Professional to complete his medical data or his Medical Emergency information.

Health SmartCard

medXchange uses industry standard SmartCard technology to optimize Internet transactions with advanced security and confidentiality features. The SmartCard applications can be imbedded in any industry standard multi-application SmartCard such as those issued by VISA, Master Card and American Express. Java-based plug in SmartCard technology is used to enable the individual and the healthcare professional to access individual health data and emergency medical data. SmartCard technology is also used to enable statistical reports for pharmaceutical companies, conduct e-commerce, manage claims processing and reimbursement, and act as a quality control agent.

Medical information is not stored on the card. Instead, the Health SmartCard technology “unlocks” an active server that stores the information. Under certain conditions, the system can be accessed using logins and passwords. The *medXchange* proprietary license system uses a technologically advanced approach to guarantee data is secure and information regarding an individual's health is totally confidential.