# eHealthcare and Electronic Health Records

October 2010

gemalto
security to be free

**About Gemalto**

Gemalto is the leader in digital security with pro forma 2009 annual revenue of €1.65 billion, operations in 85 countries and over 10,000 employees.

Gemalto provides end-to-end digital security solutions, from the development of software applications to design and production of secure personal devices such as smart cards, SIM cards, ePassports, eID cards and tokens, as well as the deployment of managed services for its customers.

More than 1 billion people worldwide use the company's products and services. In the public sector, Gemalto contributes to over 50 national programs**.** Gemalto takes an active part in 14 national eID initiatives and nine major eHealthcare programs around the world.

In 2005, Gemalto began producing ePassports for Sweden, Norway and Denmark. Currently, Gemalto is an official supplier to more than 20 national ePassport programs including those of Ivory Coast, Estonia, France, India (diplomatic passports), Italy, Portugal, Qatar, Singapore, Slovenia and the United States.

www.gemalto.com

**Gemalto's eHealthcare credentials**

Gemalto's credentials to discuss these issues are based on the fact that we have delivered the core technical solution to 10 national eHealthcare programs currently operating around the world. We believe that this gives us excellent insight into the technology, its applications and the social implications of its use. Gemalto is also an active contributor to standardization bodies, both at the European and international levels.

# eHealthcare
# and Electronic Health Records

**Eric Billiaert & Stefane Mouille**

**October 2010**

## eHealthcare solutions: putting the patient at the center of modernization

The healthcare sector holds an important place in society, as evidenced by the funding it is appropriated, the role the state plays and the large number of third parties in widely ranging fields that it involves.

Because medical advances have resulted in increased life expectancies—and because citizens are being actively encouraged to take personal responsibility for their health—the number of people in need of medical care has increased. As a result, public healthcare systems are coming under severe financial strain.

With such high demand for medical care, health services and related public-sector services are overwhelmed and spend more time managing records than treating patients. Unless effective solutions are found to cope with this high demand, the system will ultimately suffer from an erosion of its credibility.

The first major challenge is to process administrative tasks faster and more efficiently, reducing the number of intermediate steps. The goal is to provide a single point of access where the patient will only pay his deductible, as determined by the principle of the third-party payer.

Most eGovernment programs in this area aim to facilitate the exchange of information, allowing medical professionals to concentrate on care and treatment rather than paperwork, especially through:

- Significantly faster registration of patients at clinics and hospitals. This can be crucial, as the time that elapses before a patient is seen can directly impact the effectiveness of some treatments.

- No up-front fees to pay at most health centers, with costs paid directly by health insurance authorities.

The next stage in the restructuring of the relationship between patients, healthcare practitioners and public-sector authorities is unquestionably the introduction of Electronic Health Records (EHR) to store the patient's electronic medical history efficiently and securely.

EHR enables healthcare practitioners to access a patient's medical history immediately regardless of their location, thereby avoiding delay in urgent situations and optimizing quality of service. EHR stores records on the patient's visits to his current general practitioner, as well as any other general practitioners or specialists he has seen or is currently seeing. This enables a full medical history to be compiled on the card's microchip from the date it is issued.

Using eHealth cards brings numerous benefits from an administrative point of view. Countries that have adopted this technology have observed a significant decrease in fraudulent reimbursement claims, as well as smoother, more efficient interaction between patients, healthcare practitioners and health insurance authorities.

*"The French, for example, have used the Carte Vitale since 1998 and have 67 percent fewer administrative personnel per building than a comparable American establishment."*

—Newsweek, February 2010

In 2009, over 1 billion electronic claims were processed in France (85% of total), saving an estimated 3 billion sheets of paper.

Benefits for government bodies and public health authorities are staggering when a nationwide EHR program is implemented.

With the integration of different medical fields, comprehensive views of the patients' health with interaction between sub-cases from different fields, better management of the adverse effects of medication (called iatrogenicity), better statistical or even epidemiological visibility, EHR enables the creation of more reliable decision-making tools and the dissemination of standardized practices.

Iatrogenicity (inadvertent causation of illness by medical treatment) is not an anecdotal subject. In the United States, the total number of iatrogenic deaths in 2001 was 783,936. By contrast, the number of deaths due to heart disease reached 699,697, and the number of deaths due to cancer reached 553,251 (source: American Iatrogenic Association 2002). In France, in 2004 the number of iatrogenic deaths was over 10,000 and a 3.19% annual hospital occupancy rate was attributable to errors treating patients and administering medication.

## Purpose of EHR

Storing and providing secure, patient-centric health-related information is a common goal. Many implementation projects target electronic storage and support remote access. EHR can be generally defined as patient-centric computerized healthcare data, gathered from multiple organizations and potentially accessible from different locations.

## User expectations

Many users are unaware of precisely which data their existing eHealth smart card manages. In France, many bearers believe the *Carte Vitale* contains information on their blood group, yet in fact the card only manages entitlement to coverage, serving as a means of payment to some extent. Similarly, in Belgium, where 9 million eID cards have been issued, citizens believe that the national ID card contains some medical data when in fact, it does not (source: INDIGOV 2009). In fact, there is a clear expectation from the public to be able to carry basic medical data on such cards.

The design or implementation of multiple EHR projects is currently underway. The majority will be launched at the regional or organizational level, with far fewer at the national level. These projects all face the same challenges, having more to do with legal and political issues than the enabling technologies that they leverage. Many experts with a global view of healthcare agree, however, that there is a substantial economic case for wide-scale use of EHR. Taking for granted that these non-technology-related issues will be overcome, and assuming that medical professionals will cooperate, we would like to present an overview of the five key topics to be dealt with in any EHR system:

- Responsibility of authors for EHR entries
- Identification of the patient and healthcare practitioner
- Privacy of personal data
- Quality of content
- EHR infrastructure

**Responsibility of authors for EHR entries**

The chief objective of EHR is to enable healthcare practitioners currently treating a patient to access the patient's medical history. In this sense, the "EHR reader transfers some liability to the EHR.

To ensure that EHR entries can be traced to a legitimate source, the name of the author must also appear in the entry. The same identity requirements for patients are also valid for healthcare practitioners entering data into the EHR. Healthcare practitioner identification procedures must therefore be devised with the same care and attention.

Very often, users of existing IT systems in healthcare are not technically authenticated. As one example, an individual with the proper permissions could very well log on to IT systems, allowing colleagues and assistants to either share the session or use his login ID. Data entry processes are sometimes unclear and data sources not separated with respect to data authenticity. Furthermore, there is no common legal framework addressing the validity of EHR entries. For each of these reasons, physicians cannot rely on the validity of EHR. As a result, in a critical situation, a healthcare practitioner would not base vital decisions on an EHR.

Physician orders, exams, test reports and medical summaries are all considered medical records. As such, they are also legal documents that must be certified by the issuing party and stored on record in unaltered form. Based on further regulations, technical means for identification/authentication (such as cryptography) may serve as a basis for a limited transfer of liability from the reader of an EHR entry to its responsible author, who should be distinguished from the data enterer, the observer of the clinical findings being reported and the legal entity.

The authors of EHR entries must be assured of the validity, availability and longevity of their entries into the EHR, as they may wish to submit these entries as evidence in legal disputes. Authentication of authors is therefore only one aspect. There must also be legal framework enabling submission of authenticated EHR as evidence in a medical malpractice case.

A detailed process clarification of EHR data entry in accordance with a cross-organizational contract or legislation in effect would then be necessary to effectively transfer liability from the current medical practitioner to other EHR authors.

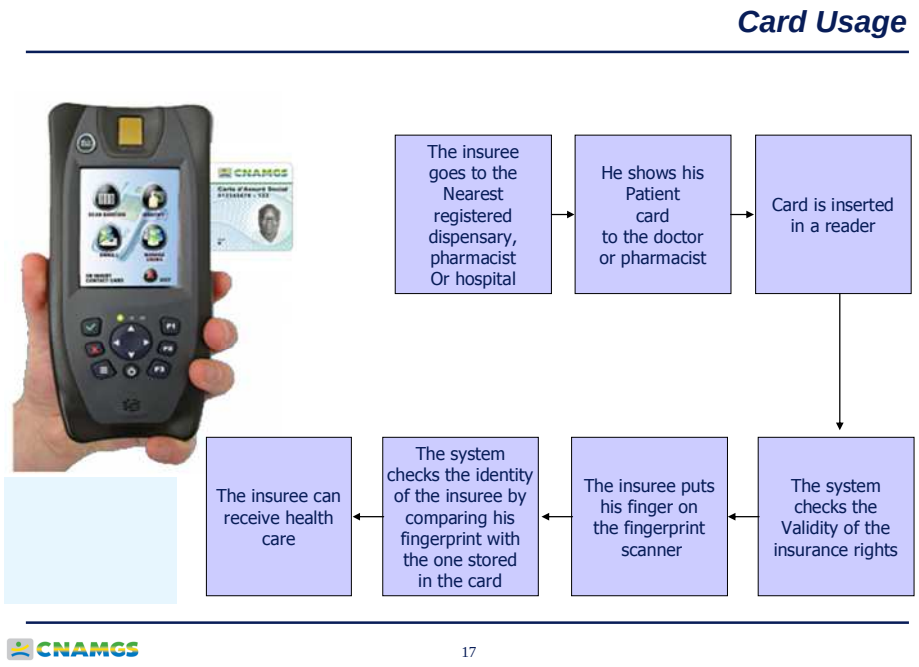

In France, 98% of pharmacists and over 82% of general practitioners use the *SESAM Vitale* system. Transactions are validated when the patient and practitioner cards are inserted at the same time. A national EHR project has been in the works for many years, but no legal framework has been set up as of yet.

The preferable identification token choice at the moment is the smart card (HPRO, 2009 http://www.ehealthforum.cz/files/presentation_hpro-card.pdf).

## Identification of the patient and healthcare practitioner

Uniquely identifying patients is an absolute prerequisite to operating an EHR system, which stores and retrieves patient-related data.

Patient identification is first needed to match a person to a file (or multiple instances of a file). Identification under different settings may mean different things and may require different organizational and technology solutions. Another dimension of identification is authorization, which is discussed in the passage on privacy. Patient identification is required for data mapping of the individual and related EHR entries. Neither the data mapping nor the identifier must necessarily form part of these EHR entries. Mapping can be performed through direct attributes (biometric features such as fingerprints and portraits) or through indirect attributes.




In Gabon, biometric match-on-card enables highly secure patient identification without a central fingerprint database, as authentication is performed off-line. Well before the program started, it was clear that the necessary measures should be implemented to secure access to the health coverage program. Unauthorized use of services by citizens from neighboring countries could lead to its collapse through the fraudulent use of rights. Beneficiaries must be identified individually in order to restrict access to care. Non-transferable identification has been implemented using a Gabonese individual health insurance number.

Identification can be managed to be unique (i.e. issued for a single person) either globally, or within a certain scope, which is the overall organization/area in which that identifier is unique. Implementing a unique identity therefore requires some authority operating a scheme to create unique identifiers, one or more identity issuers and one or more directories for lookup purposes. The scope of that authority is the maximum scope of the related EHR.

Any EHR has to be based on unique patient identification, which ideally—but not necessarily—is invariable over the patient's lifetime. That patient identifier only needs to be unique for a given set of patients being managed by that EHR system (back-end identification).

**Boualem Touati, IT Director for Algeria's universal healthcare plan (*Caisse Nationale des Assurances Sociales*, or CNAS)**

*"The key to this in my view is the need for robust identification so that we can answer the question, 'Who is paying for whom and for what?' It is essential for better rationalization of health expenditure and for authentication purposes. Above all, it is better for the sustainability of the universal health care plan. It would be illusory to think that the supply of services could remain anonymous. Secondly, this identification highlights the importance of the original identity data, including the central element providing proof of authenticity of the identity, which is the extract from the civil register. Finally, the unique identification efforts, such as those that we have made within the universal health care plan in Algeria, must be interoperable with other national projects, by pooling identifiers and management of processes. Obviously, we must avoid the duplication of technologies, registering processes, verification, identity management, etc., for major forthcoming national projects, such as the national eID program."*

As one example, Germany's health insurance card (*Krankenversicherten Karte*, or KVK) presents a unique example. When used together with the identifier of the related health insurance (*Krankenkasse*), it confirms that the bearer is insured and entitled to coverage. The KVK & Kassen-Nr. are not invariable, however, as the bearer can user the same card to obtain coverage from another health insurance company. Likewise, ISO 21549 and the European Health Insurance Card (EHIC) are based on identifiers derived from the health insurance contract. The numbers used as potential identifiers are not invariable even though they provide a simple scheme to unique identification. Although the recently approved eEHIC CWA (eEHIC, 2009) has provisions for unique citizen identification, from a political point of view it is not meant to be an identification card, but rather an entitlement card.

Provided that a unique, exclusive alphanumeric patient identifier is invariable and will never be used again (e.g. once the patient has passed away) such a patient identifier can be used as the primary key in an IT system. Note that most regulations somehow limit or even prohibit the use of personal identifiers with global (not restricted to a single contract) applications and/or long-term storage.

## Privacy of personal data

The organizations and individuals responsible for the management of EHR data are required to ensure that adequate protection is established and that access to the information is granted only to authorized parties. It should also be noted that hard-copy healthcare data have always presented risks in the area of privacy.

As of September 2010, the new CHIFA eHealthcare system in Algeria is running in all of the country's 48 districts, with over 4.5 million CHIFA cards delivered. The plan's 13,000 practitioners are identified using tokens (micro-processor-based USB dongles). No EHR system is in place yet but the card does contain records of the patient's blood group, allergies, chronic diseases and related treatment.

Due to regulatory compliance (e.g. Healthcare Insurance Portability and Accountability Act Directive 95/46/EC) and similar requirements, providers and operating organizations must implement appropriate measures, document and assess them. In many cases, directors and leading executives are personally liable for IT safety and security.

The privacy of personal health data is supported by authorized access to data and functions, as well as secure storage of EHR. Authorized access requires patient authentication, as well as authentication of the healthcare practitioner in need of access to the patient's EHR. Assuming that the patient identification has been authenticated, the healthcare practitioner accessing data and functions of an EHR must also be authenticated.

One foundation of secure EHR systems is the individual healthcare practitioner account and its assignment to groups, which may serve as the basis for granting permissions to access health-related data and to use healthcare IT services processing such data. Like the implementation of patient identification, either biometric or symbolic information or a token (hardware powered by a microprocessor; refer to passage on Algerian token) can be used to log in, as previously discussed.

Authorizing healthcare staff to use data and services can be achieved by setting permissions for directories of the underlying operating system or plugged-in directory services communicating with the computing platform through standard protocols (e.g. LDAP).

Although privacy is the subject of much public debate, it should be noted that privacy protection is already in place in many national eBanking, eID and eHealth schemes delivering robust eServices.

Protection of privacy and the authenticity of health-related data are currently supported by local signature/encryption algorithms in a public key infrastructure. Both are implemented using IT and communication systems. Because an identity infrastructure is needed for both patients and healthcare practitioners, a Public Key Infrastructure (PKI)—certificate and private key issuers and public key lookup—can be added as an extension to that identity infrastructure.

Breaking down and separating the data handled by various organizations—data that only taken together make up sensitive information—is another potential measure to increase security.

Privacy-preserving credentials developed recently by Gemalto also address the challenge of accessing a restricted eService without disclosing users' private data to the service provider. These credentials prove that the user fulfils the profile access criteria, preventing any other party from acquiring knowledge about the very nature of the service requested by the patient, practitioners or staff.

Slovenia has implemented a PKI-based eHealthcare infrastructure, the technical infrastructure for EHR. Gemalto's Sealys Health Insurance cards are the first of their kind in Europe to feature its Java-based Sealys Multi App ID to further secure a fully on-line system with digital signatures for healthcare practitioners.

*"The goal of our strategic e-Health 2010 plan is to join up health information systems nationwide, thus ensuring that electronic services and transparent information can be provided to all stakeholders in secure, efficient fashion. Apparently it is very difficult for large countries to introduce the second generation of health cards integrating digital certificates in addition to current functionalities. Slovenia, as a small country is certainly more agile. After a thorough two-year preparation phase, we embarked on this change in March 2009 and are on schedule to finish by 2010. I would say that the key challenges of our overhaul include active participation of all stakeholders, swift execution of changes without disruption of service and the introduction of acceptable, manageable and up-to-date ICT solutions. Key to the successful running of the operation is also the fact that the new system is fully backward compatible with existing infrastructure."*

—Marjan Sušelj, Director, HIC System Sector, from January 2010 on acting as director of Ljubljana regional unit at the Health Insurance Institute of Slovenia

**Quality of content**

To be useful and meaningful, data stored in EHR must be structured and employ consistent medical terminology and semantics. To be practical, the custom view must be flexible enough to enable personalization and filtering.

The data must be arranged in structured fashion, using only approved terminology throughout. Usage of approved medical terminology enables medical records to be generated in standardized format. These are required to implement automated searches and medical processing (e.g. drug interaction check, medical/workflow guidance, reporting, reimbursement and search/index/query).

With regard to EHR, medical terminology is classified according to a taxonomic scheme. Each class represents conceptual knowledge in the field of medicine. The meaning of each term is determined by syntactic and semantic characteristics. The full set of terms—without regard to semantics—is referred to as the nomenclature.

Nomenclature should naturally remain independent of context (time, location or organization). The origin of a term should always be displayed so that the user knows to which nomenclature the given codes belong. Nomenclature typically evolves by archiving old entries and adding new ones. In some cases, old entries are removed or even re-integrated into a different class. A version number along with the nomenclature identifier enable detection of such discrepancies.

Limited nomenclature comprising only a few terms may not be precise enough to capture the physician's intention. The rather general terms provided by limited nomenclature would need to be accompanied by a plain text statement. In this instance, a portion of the health record reflects all applicable terms, while the open-field statement is presented separately. In some cases, the terms composing existing nomenclature can be refined using modifiers.

Extensive nomenclature (comprising a large number of terms) may present different codes for the same medical condition, so that multiple terms for a single medical finding are listed in a given patient's EHR. In fact, multiple physicians might diagnose different findings based on the same symptoms. A single complaint can therefore be the root of multiple entries in the patient's EHR.

Semantic interoperability is crucial to ensure that users reading EHR entries understand the author's intended meaning. Using and understanding symbols in a common way requires support for common use and interpretations of symbols for instances and conditions. This entails providing not only registries, catalogs and Master Patient Indexes (MPIs), but also explanations on the meaning of each identifier and term.

Within the geographical and organizational scope of an EHR system, all parties involved must be able to understand the meaning of identifiers and terms. Such an understanding cannot be achieved with purely formalized and technical material. Instead, plain text definitions supported by examples and training materials are required.

Plain text definitions and explanations of the respective information models would appear to offer the only solution for semantic interoperability, i.e. for migrating or mapping encoded data from one conceptual model to another.

Instead of copying voluminous medical records to the customer's IT system, a custom view has to be created, which shows a reduced subset of references into the respective patient's ePHR. Based on metadata and keywords, either a human expert or a query interface can create such a custom view and then provide links to the original EHR data. While customer IT systems (at the general practitioner's office or in the hospital) may help in narrowing the results of querying an EHR system, it takes a healthcare practitioner's judgment to disregard past events which he considers irrelevant versus highlighting important facts recorded in the EHR system, as part of the patient's relevant medical history.

**EHR infrastructure**

EHR can be seen as a collection of medical content entries stored in decentralized systems. These decentralized systems must be up and running, meeting performance requirements that are proportional to the overall system requirements.

The EHR system infrastructure will then have to provide a certain level of performance, a set level of availability at remote locations and long-term storage of the EHR.

The potential load an EHR system must handle will hinge on the number of point-of-care workplaces equipped to access the EHR system, the number of patients with EHR entries stored in that system and the size of those EHR files. Taking into account the EHR system's required response time, the processing power needed for the servers in an EHR system plus the required networking bandwidth can be deducted. Cryptographic measures for encryption and authentication take another toll, both on computing power and bandwidth.

Typically, 24/7 availability for EHR functionality is needed, which can only be provided by professional hosting organizations. With decentralized systems, the probability of a single server—required to send out an important EHR entry—is higher but the overall availability is better via redundancy.

Long-term storage and secure archiving require an experienced and reliable IT service provider. The IT department of a hospital or a regional healthcare organization, or a trusted commercial hosting service can fulfill this role.

Experience from EHR projects shows that from a semantic point-of-view, maintaining nationwide centralized EHR would be less useful than connecting federated systems and allowing queries for patient-related data across multiple EHR systems.

The ongoing debate on decentralization will be settled by a local, regional or global decision that has to be made for each type of information, based on its respective properties and usage.

In February 2010, Gemalto announced that Bulgaria has begun deploying its smart cards to secure access to personal health records for the country's military personnel and family members.



In Bulgaria, Gemalto delivered double-slot readers, smart cards and related middleware to KIM-2000, a local company specialized in eHealth projects. KIM-2000 acts as prime contractor for the electronic health record system commissioned by the Military Medical Academy. Under the authority of the Ministry of Defense, the Military Medical Academy is the organization in charge of medical care for the Bulgarian Armed Forces.

This innovative system optimizes medical treatments, simplifies and modernizes procedures and increases security for accessing health information.

The Gemalto card is compliant with the Identification Authentication Signature (IAS) European standard to ensure the highest level of security for accessing personal electronic health records. The patient and the healthcare practitioner simultaneously insert their cards into the double-entry Gemalto reader and type in their PIN code to enable viewing or modifying of the medical file, which is stored on a highly secure IT infrastructure. The patient can also view his personal data online, using the Gemalto reader and card to authenticate.

The personal electronic health record is a complete electronic archive of the patient's medical history. It stores all existing medical documentation, including laboratory tests and results, X-ray pictures, all visual tests, electronic prescriptions, etc. It also contains the patient's blood group, allergies and genetic predisposition to diseases, physicals, surgery and all useful medical information.

The personal electronic health record enables healthcare practitioners to immediately access a patient's medical data and therefore, make more accurate decisions, especially in emergency situations. A special emergency section in the electronic health record contains the most vital information for these situations.

## Conclusion

- There is a real need for and expectations from patients to have EHR in place, working properly and securely. Pregnant women and patients suffering from serious illnesses are among those who most frequently voice their concern.

- All parties will benefit from optimized medical treatments, simplified and modernized procedures and increased security and privacy.

- While dependably accurate identification and authentication for patients and health professionals seems like something that should already exist in healthcare, this is not yet the case in many countries.

- Much emphasis has been placed on the need to implement electronic health records at the regional and national levels. But this is putting the cart before the horse. Accurately linking patients and professionals with personal medical information is the first step to be taken in EHR projects.

- The actual implementation of eHealthcare as well as eServices—including eIdentification, eSignature and eAuthentication in European countries and beyond—demonstrates that the key components (smart cards, PKI infrastructure, authentication, etc.) of an EHR solution involve technologies that are mature, robust and unquestionably capable of delivering the results required.

# Bibliography


- eHealth Case Studies from www.epractice.eu
- Patient Identity in eHealth; 2006/2007 http://ec.europa.eu/information_society/activities/health/docs/studies/patientehealth-fp6book.pdf
- Economic Impact of Interoperable Electronic Health Records and ePrescription in Europe; 2008/2009 http://ec.europa.eu/information_society/activities/health/docs/studies/ehr_impact-study-present.pdf
- Electronic Health Record Standards - A Brief Overview, Conference Paper for Information Processing in the Service of Mankind and Health; ITI 4th International Conference on Information and Communications Technology; Eichelberg, M., et al.; 2006
- eHealth Priorities and Strategies in European Countries; European Commission; 2007
- Effective Healthcare Identity management; Smart Card Alliance; March 2009 http://www.smart cardalliance.org/resources/pdf/Healthcare_Identity_Brief.pdf
- eGovernment 2.0: Identification, Security and Trust, Exploring European Avenues; Gemalto & YeMa Consultants; September 2007
- eGov 2.0: The Keys to success; Gemalto & YeMa Consultants; June 2009
- The Perfect Storm for Electronic Health Records; January 2007 http://www.himss.org/content/files/08_column_ehr.pdf

The world leader in digital security

www.gemalto.com

gemalto
security to be free