Methods Inf Med; Vol. 43 (2), pp. 124-132; 2004

The strategic approach of managing healthcare data exchange in Austria

G. Duftschmid, T. Wrba, W. Gall, W. Dorda

University of Vienna, Department of Medical Computer Sciences,
Spitalgasse 23, A-1090 Vienna, Austria
{georg.duftschmid, thomas.wrba, walter.gall, wolfgang.dorda}@akh-wien.ac.at
www.akh-wien.ac.at/imc/

Address requests for reprints and correspondence to:

Georg Duftschmid

University of Vienna, Department of Medical Computer Sciences,
Spitalgasse 23, A-1090 Vienna, Austria
Tel.: +43-1-40400 / 6696
Fax.: +43-1-40400 / 6697

Email: georg.duftschmid@akh-wien.ac.at

Summary

Objectives: The exchange of electronic medical data between healthcare providers constitutes an integral part of modern medicine, and its importance is growing. Efficient application on a national level requires a uniform approach to the management of healthcare data exchange, avoiding isolated solutions that are expensive and also incompatible.

Methods: In this communication we explain the basic concepts of establishing a nationwide framework to guide healthcare data exchange in Austria. To achieve this goal, a three-step approach was adopted: (i) creating general guidelines to direct electronic medical data exchange; (ii) defining detailed standards for electronic messages; (iii) organizing pilot projects to implement these standards, and further improving the general guidelines based on the results of the pilot projects.

Results: We present the MAGDA-LENA framework which guides healthcare data exchange in Austria, and compare it with the US framework HIPAA. We describe several communication scenarios for which concrete message standards were developed in recent years, based on the MAGDA-LENA framework. We further discuss the implementation of these standards in four pilot projects.

Conclusions: The strategic approach of managing healthcare data exchange presented in this paper is expected to have a substantial impact on medical informatics in Austria over the next few years.

Keywords (MeSH): Computer Communication Networks, Telemedicine, Policy Making, Health Insurance Portability and Accountability Act (HIPAA)

1 Introduction

In contemporary specialized medicine, the efficiency of close cooperation between experts depends on optimizing the exchange of information. Clinical data networks form an integral part of the modern healthcare infrastructure. Among other things, they create a basis for various applications in telemedicine and for healthcare messaging (e.g., patient referral, clinical observation reports, billing by computer).

Analogous to the international trend, the electronic interchange of patient data has been rapidly growing in Austria over the last years. For want of a uniform approach, local implementations have given rise to a plethora of incomplete and isolated solutions. Besides, the Austrian healthcare system is highly decentralized, falling into largely independent structures. Consequently, a large number of heterogeneous approaches to electronic data exchange exist. These approaches differ in terms of the intensity of use as well as technical principles.

In 1995 the Austrian minister of health set up the STRING (German acronym for "Standards and Guidelines for the employment of informatics in Austrian health care") commission, an advisory panel of experts[i] undertaking to address these issues. The STRING commission has since coordinated the strategic buildup of an Austrian healthcare information exchange initiative by adopting a three-step approach (see Fig. 1).

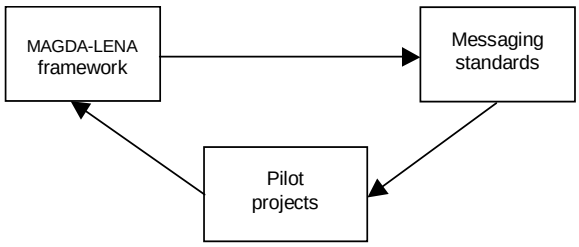

Fig. 1: The STRING approach for building up an Austrian healthcare information exchange network

[i] The members of the STRING commission are H. Burggasser, W. Dorda, J. Gambal, G. Gell, H. Ingruber, W. Kotschy, E. Leitgeb, J. Mittheisz, K. Pfeiffer, O. Pjeta, M. Pregartbauer and H. Tinhofer

In the first step, a general framework named MAGDA-LENA (German acronym for "Austrian logical and electronic network for medico-administrative clinical data exchange") has been set up, which includes the actual methodology used to develop the network. Following the MAGDA-LENA specifications, detailed standards for electronic messages are developed in step two. Finally, pilot projects are promoted, based on the message standards, and their results are used to further develop the MAGDA-LENA framework.

In the present article we shall discuss this three-step approach in detail. The paper is organized as follows: Section 2 presents a brief discussion of national and international efforts made in the domain of standardizing electronic health data interchange. Section 3 introduces the MAGDA-LENA framework (i.e. the actual methodology used to develop the Austrian logical network for healthcare information exchange). A number of real-life pilot projects in which several standards based on the MAGDA-LENA framework were implemented will be presented in section 4. A comparison of the MAGDA-LENA and HIPAA frameworks is presented in section 5, and the conclusion in section 6.

2 Related work

In this section we will first outline the United States' Health Insurance Portability & Accountability Act (HIPAA), which constitutes a regulation for the healthcare sector, comparable to the Austrian MAGDA-LENA framework. We will then give an overview of European initiatives in the domain of health data exchange and finally describe several groups which play an important role in national and international standardization.

2.1 The HIPAA framework in the United States

The Health Insurance Portability & Accountability Act (HIPAA) of 1996 introduced several administrative simplifications in the US healthcare system, requiring, among other features, more efficiency in healthcare delivery by standardizing electronic data interchange (1). The HIPAA provisions apply to all i) health plans, ii) health care clearinghouses, and iii) health care providers that conduct any of the transactions addressed in the Transaction Rule (see below) in electronic form. These entities are referred to as "covered entities" within HIPAA. The HIPAA provisions are worked out by the US Department of Health and Human Services (HHS) in the form of rules, each with a specific compliance deadline.

They are organized in four parts:

1. *Electronic Health Transaction Standards* prescribes a set of formats developed by the American National Standards Institute (ANSI), which have to be uniformly applied within eight explicitly listed electronic transactions related to health care claims or equivalent encounter information, health plan eligibility, referral certification and authorization, health care claim status, enrolment and disenrolment in a health plan, health care payment and remittance advice, health plan premium payments, and coordination of benefits. Further, a code set is prescribed, consisting of a choice of medical coding systems that must be used within the above mentioned message formats (e.g., ICD-9-CM has to be used to code health problems and procedures). Based on this part, the *Transaction Rule* was published. It is effective since October 16, 2002 for most covered entities. Small health plans which were excepted from this deadline have to comply by October 16, 2003.

2. *Unique Identifiers* aims at defining distinctive IDs for healthcare providers, employers, health plans, and patients. This should resolve problems resulting from the use of several different ID numbers, which are permitted by the current healthcare system. So far only the *Unique Employer Identifier Rule* has been published in its final form, with the compliance deadline of July 30, 2004 for most covered entities. It recommends the use of the taxpayer identification number, which is assigned by the Internal Revenue Service of the US Department of Treasury. Small health plans which are excepted from this deadline have to comply by July 30, 2005.

3. *Security of Health Information Standards* will provide a uniform level of protection of all "electronic protected health information" (EPHI), i.e. all electronic health information that can be linked to an individual. The compliance date for the final *Security Rule* was set to April 21, 2005 for most covered entities. Small health plans which were excepted from this deadline have to comply by April 21, 2006. The *Security Rule* requires covered entities to ensure the confidentiality, integrity, and availability of all EPHI that they create, receive, maintain, or transmit. Apart from technical provisions concerning, among others aspects, transmission security and the implementation of access control and audit control mechanisms, the installation of various administrative (e.g., sanction policy) and physical (e.g., facility access controls) safeguards is also prescribed.

4. *Privacy and Confidentiality Standards* is concerned with the question as to who has the right to access personally identifiable health information. This part has lead to the publication of the *Privacy Rule*, which is effective since April 14, 2003. The *Privacy Rule* creates, for the first time, a comprehensive national standard to protect individuals' medical records and other personal health information. It seeks to give patients more control over their health information, sets boundaries on the use and release of health records, and establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.

Severe civil and criminal penalties have been specified for noncompliance. The penalties and procedures of their enforcement will be published in the *Enforcement Rule*. Currently this rule is represented by the so-called *Interim Final Enforcement Rule*, which authorizes the HHS to impose on any person who violates a HIPAA provision a penalty of not more than US $ 100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement during a calendar year may not exceed US $ 25,000. The general approach of the HHS to enforcement is to promote voluntary compliance with the rules through technical assistance. The process is primarily complaint-driven and consists of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective plan of action.

2.2 European initiatives

In 1999 the European Commission (EC) launched the *eEurope* initiative (2), which has set the objective for the European Union (EU) to have, by 2005 "modern, online public services". As part of this initiative, the *E-Health* program (3) seeks to promote e-health services. A goal that has been set in this context in 2002 is to reach a common approach in the domains of patient identification and electronic health record architecture through standardization. Further, good practices concerning secure access to personal health information will be specified. By the end of 2005, EU members should develop health information networks between points of care (hospitals, laboratories and homes). Apart from the E-Health initiative, several research projects (e.g., SHINE, TRILOGY, CHIN, CoCo, NDSNET, SIREN, PICNIC) sponsored by the EU's framework programs addressed the development of healthcare data networks (4).

The Technical Committee TC 251 of the European Committee for Standardization (CEN) deals with the development of healthcare standards designed to ensure the comparability and inter-operability of independent clinical systems, and addresses several issues in the domain of healthcare data exchange. In contrast to MAGDA-LENA and HIPAA, these issues are treated separately in the form of individual standards or technical reports. A comprehensive work covering all aspects of healthcare data exchange is not provided. The working areas of the TC 251 include

- Message standards: Several messages have been standardized, covering different types of healthcare transactions (5). The CEN report 12587 describes a method for the development of new messages to support a uniform, consistent message design process.
- Communication security: The standards include ENV 13608 Security for healthcare communication, ENV 13729 Secure user identification for healthcare - Strong authentication using microprocessor cards, and ENV 12251 Secure user identification Management and security of authentication by passwords (5).
- Identifiers: In this domain, the new work item “Guidance on good practice for patient identification in the process of care” (6) was proposed in 2003.

In Denmark the *MedCom* initiative (7) was initiated in 1995 with the goal of setting up a national healthcare data network. The implementation of MedCom is widely advanced today, which is underlined by the fact that, in 2002, as much as 60% of healthcare communications in Denmark took place through the healthcare data network. A major issue addressed by MedCom was the development and implementation of message standards to support typical communication scenarios. MedCom’s strategy for extending the network is based on integrating existing intranets. As a prerequisite to become part of MedCom, a network has to fulfill the security requirements of the Danish Data Protection Agency. Currently, MedCom does not have legislative character. Participation in the network is voluntary for Danish healthcare providers.

HYGEIAnet (8) is a regional health information network being developed to provide an integrated environment for healthcare delivery in the island of Crete, Greece. One of its primary objectives is to implement an integrated electronic health record (9). Rather than using a message-based approach, the network is based on a federal approach that relies on services such as unique identification of patients, a common terminology component, a federal data model to which participants must map their local models, and security services (e.g., cryptography, digital signatures, and auditing mechanisms). Like MedCom, HYGEIAnet does not have legislative character.

2.3 Standardization in the domain of health data exchange

Intensive efforts are being made by several groups to standardize the exchange of health data. In the following we will give a brief overview of some of the important involved organizations:

The technical committee (TC) 215 (10) on health informatics of the International Standards Organization (ISO) deals with standardization in the area of health information and communication technology. In recent years its work groups submitted several proposals for international standards.

The TC 251 (11) of the European Committee for Standardization (CEN) deals with the development of healthcare standards and is addressed in section 2.2.

The specialized standardization committee FNA 238 on medical informatics of the Austrian Standards Institute (12) is a mirror group of CEN/TC 251 and ISO/TC 215, and coordinates national standardization projects. All activities of FNA 238 are conducted in strict conformity with the MAGDA-LENA framework.

Accredited by the American National Standards Institute (ANSI) in 1994, HL-7 is an organization dealing with the development of standards for data exchange in the healthcare arena. HL-7 version 3 (13) is built on a model-based object-oriented methodology for message development named *Message Development Framework* (14). The starting point for identifying relevant objects of newly developed messages is the *Reference Information Model*, which is a UML-based static object model that aims to integrate American health-sector entities relevant to clinical message exchange.

The openEHR foundation (15), which has emerged from the GEHR project (16), aims to promote and publish the formal specification of requirements for representing and communicating electronic health record (EHR) information. The GEHR methodology is based on two different tiers of modeling: The reference model (RM) provides a set of classes from which all elements of an EHR are to be instantiated. Archetypes constrain the possible instantiations of the RM to a subset of meaningful, agreed upon structures. All of openEHR's activities are related to different aspects of the EHR, whereas MAGDA-LENA is concerned with the transfer of any healthcare information, independent of the underlying data structure.

3 The MAGDA-LENA framework

MAGDA-LENA was developed by the STRING commission as the governing framework for electronic exchange of patient-related data in Austria; its first version was published in 1998. The MAGDA-LENA paper outlines the technical as well as organizational aspects governing the development of an Austrian healthcare information network which will allow patient-related multimedia information to be exchanged between both healthcare and social security facilities (i.e. service providers, administrators, insurers). Analogous to MedCom, MAGDA-LENA does not intend to build up a new independent network but to coordinate and make compatible the existing local networks. The exchange of healthcare information is to gradually unfold along the lines of the MAGDA-LENA framework in a coordinated manner to the point where all of Austria's healthcare and social security providers will be interlinked.

A more detailed version of MAGDA-LENA was adopted in 2000 following preliminary studies at the university departments of medical informatics in Graz, Innsbruck and Vienna. This second version of MAGDA-LENA can be viewed (in the German language) on the web (17).

The MAGDA-LENA framework will be integrated into a new Austrian law on health telematics, which is currently in preparation. Until this law becomes effective, MAGDA-LENA will have only recommendatory status. Therefore, no sanctions exist yet for non-compliance with MAGDA-LENA. In order to check compliance with MAGDA-LENA in the future, the MAGDA-LENA paper includes a formal conformity statement consisting of 20 items which cover the most essential points of all sections (e.g., "The participant / provider has to declare that he has implemented an internal security policy according to the recommendations in the corresponding MAGDA-LENA section. The essential points of this

policy have to be published and made accessible for communication partners."). According to the scope of the four MAGDA-LENA sections, the individual points of the conformity statement address network participants, providers, or both. At the moment, parties involved in healthcare data exchange may voluntarily authenticate the conformity statement to prove the future-oriented nature of their systems.

In the following we will discuss MAGDA-LENA's four key sections.

3.1 Message Contents, Models, Standards

The goal of this part is to promote the use of standardized message formats for the exchange of health information. Given the wide variety of parties communicating in the healthcare arena, these requirements should not be defined by the parties themselves on a bilateral basis, but should be based on global rules. In this context, intensive efforts are also being made internationally to develop general healthcare information models on which to base standard messages (13, 15, 18). By specifying a common methodology for the development of new message standards, MAGDA-LENA aims to achieve a high level of mutual compatibility within healthcare messages. The MAGDA-LENA framework prescribes that:

- Existing international or national standards related to medical informatics, which satisfy the particular requirements of a communication process, must necessarily be used. A list of currently available European and Austrian healthcare message standards is provided in the annex.
- If such standards are not available for a given area of application, messages must be developed along the procedural model defined in MAGDA-LENA to optimize their uniformity. This procedural model is based on related international effort (14, 19, 20) and specifies in detail seven steps for the development of healthcare messages.

3.2 Identification Variables

For secure data transmission in the healthcare arena, both the communicating parties and the transmitted data must be unambiguously identified. The purpose of this requirement is to preclude any kind of intentional (e.g., unauthorized sender) or unintentional (e.g., mixing up individuals) abuse. MAGDA-LENA requires communicating parties to be identified via registered directories and suggests the following directories for use:

- Physicians: Partner contract number (6 digits) of the Main Association of Austrian Security Institutions
- Pharmacies: Pharmacy company number (5 digits) issued by the General Salary Fund of Austrian Pharmacists
- Hospitals: Austrian hospital identification number (3 digits + 8 characters)
- Patients: Austrian Social Security Number (10 digits)

For the identification of transmitted documents, a corresponding document header is suggested, which should contain the ID of the sender, a time stamp, and the ID of the patient's stay during which the document was created, substantiated by additional attributes to allow unique identification of the document.

3.3 Data Privacy and Security

To comply with Austrian data privacy regulations, a uniform security policy that covers both organizational and technical measures must be implemented. In this context, MAGDA-LENA requires that the participants implement specific measures to achieve data privacy and security in the participants' internal domain as well as in their electronic communications with others. For this purpose, a list of obligatory security requirements is provided, which may be adapted in response to technological progress. They concern

- Encryption algorithms: For symmetric encryption the algorithms IDEA, 3DES, and AES are recommended, with a minimum key length of 80 bits.
- Encryption protocols: Depending on the required type of communication, the protocols S/MIME, SSL, TLS, and IPSEC are recommended.
- Electronic signature: Only secure signatures defined by the Austrian Signature Act (21) are accepted.

- Security tokens: Only processor cards may be used. The tokens may be unlocked by means of passwords or biometric approaches. The security requirements specified in the Austrian Signature Act, Austrian Signature Ordinance (22), and the ENV 13729 on strong authentication using microprocessor cards (5) have to be considered.
- Password systems: The security requirements specified in the ENV 12251 on identification and authentication by passwords (5) have to be considered.
- Further, MAGDA-LENA recommends the implementation of additional measures in the areas of extended access control, audit trail, local and remote system maintenance, and availability.

The section is concluded by a list of recommendations for an efficient security policy, concerning general issues (e.g., liabilities, sanctions), control mechanisms (e.g., communication control, comprehensive documentation, acknowledgement of receipt), physical safeguards (e.g., constructional requirements, secure net access, power supply, disposal of information), organizational topics (e.g., modeling of process, security-related roles, the required resources for each process), and personnel requirements (e.g., qualification, training, job rotation).

3.4 Network Providers and Nodes

The MAGDA-LENA framework also defines minimum standards to be honored by the network providers participating in the Austrian healthcare network, including guidelines concerning

- Contracts with clients: Specifications on availability, security, hotline, maintenance, accounting, and fees, have to be included. Contracts have to be time-limited and the early termination of contracts must be addressed.
- Technical issues: Minimum requirements on hardware (e.g., reliability through the use of main-, backup-, and control servers, and secure power supply), software (e.g., secure operating systems such as Windows or Unix; firewalls), disclosure of net architecture.
- Smooth cooperation of network operators: Router design and management.

- Smooth cooperation between network operators and clients: Logging of all data transfers, confirmation of receipt, access to international health data networks, communication standards, data exchange over the internet.
- Network interfaces: In particular, any modification of data in transfer, including their de- and re-encryption, is prohibited.

Network providers must also accept an evaluation of their business processes by an authorized agent of their contracting parties to check for their compliance with MAGDA-LENA.

4 Results

A number of standardization projects have been conducted under the auspices of the STRING commission to facilitate implementation of the MAGDA-LENA framework by collecting experience in real-life environments. The standardization projects described in the following were coordinated at the University of Vienna Institute of Medical Computer Sciences in strict compliance with the existing EU standards.

4.1 EDIVKA - data exchange between insurers and hospitals

The EDIVKA project aimed to standardize an annual 7 million communication events between Austrian hospitals and health insurers by substituting electronic data exchange, improving the quality of data (insurer's endorsement, payments, expenses, reimbursable services, etc.) and economizing the process of data collection. Although still being developed at the time, the MAGDA-LENA framework was first tested in practical operation during the EDIVKA project. The developed messages were derived from the corresponding European standard ENV 12612 *Messages for the Exchange of Healthcare Administrative Information* (5) and published as two Austrian national standards: K2201/1 (12) is concerned with communication in the context of a patient's hospitalization (notice of admission, insurer's endorsement), while K2201/2 (12) covers the domain of hospital discharge. Both of these standards have been successfully tested in a number of sub-projects on the basis of UN/EDIFACT and XML. In the EDIKOST project, for example, requests and confirmations for the take-over of costs for hospitalized patients by means of additional insurance contracts have been implemented within ten hospitals and all Austrian private health care insurance institutes. In the EDILEIST project, to cite another example, messages for the payment of

doctor's fees have been implemented for three hospitals. Currently, approximately a quarter of the communication events between Austrian hospitals and health insurers are handled electronically and this percentage is further growing.

4.2 MEDIX - clinical observation reporting and patient referral

The objective of the MEDIX project was to develop Austrian national standards for electronic transmission of clinical observation reports and patient referrals, based on the MAGDA-LENA framework. Thus, the MEDIX project lays the foundations for electronic data exchange between hospitals and physicians in private practice. Deriving from the relevant international standard ENV12538 *Medical Informatics – Messages for Referral, Discharge and Specialist Service Reporting (5),* the Austrian national standards K2202 *Patient referral* and K2203 *Patient discharge* were published (12).

4.3 EDIKUR - messages for spa and rehabilitation facilities

The objective of this project was to develop messages for the exchange of clinical and administrative data in the following domains: (a) endorsement of stay at a rehabilitation facility, (b) notice of reservation, admission or discharge, (c) request for and endorsement of extra services, and (d) charges and credits. Again, the message specifications in this project were derived from existing international standards, i.e. ENV12539 *Request and Report Messages for Diagnostic Service Departments* and ENV12612 *Messages for the Exchange of Healthcare Administrative Information (5).* The results were successfully tested and are being used by a key Austrian pension insurer in its communication with rehabilitation facilities.

4.4 EDI-HELP - accounting of care appliances and psychological diagnostics

This project aimed to develop messages for the electronic exchange of data in the context of (a) the accounting of healthcare appliances (communication partners include opticians, providers of hearing aids, inhalation devices, orthopedic material, and contact lenses on the one hand, and health insurers on the other) and (b) the endorsement and accounting of psychological diagnostics (communication partners are clinical psychologists and health insurers). To prove the concept, the results were implemented within a research project based on ebXML (23).

5 MAGDA-LENA versus HIPAA

The MAGDA-LENA framework is comparable with HIPAA in respect of its purpose and the covered domains. In the following we will discuss the main differences.

5.1 Legal liability

A general difference between the two frameworks is their legal liability. The HIPAA provisions have been formulated as legally binding rules, each with a specific compliance deadline. Some of the rules are already effective; others will become effective in the near future. Severe civil and criminal penalties have been specified for non-compliance. MAGDA-LENA, in contrast, currently only has recommendatory status. Although the framework has been integrated into a new Austrian law on health telematics, the law is currently still being processed; it is not yet effective.

5.2 Message standards

MAGDA-LENA's section on *Message Contents, Models, Standards* is similar in content to HIPAA's part one *Electronic Health Transaction Standards*, as both deal with the specification of standards for the exchange of health care information. The points of difference are as follows:

- HIPAA explicitly names a set of (mostly ASC X12) standards to be used in the processing of eight specific electronic transactions. MAGDA-LENA does not prescribe any particular standard but demands that existing national (Austrian) or international (CEN, ISO) standards satisfying the particular requirements of a transaction should be used. An overview of currently relevant standards is provided in the annex.
- MAGDA-LENA provides a method for the development of messages to be used when no suitable standards exist for a specific transaction. HIPAA does not include a comparable procedure. Instead, it lays open the guiding principles (a set of 10 criteria) that were used by the implementation team for the selection and evaluation of its standards.

- HIPAA prescribes a code set consisting of a choice of medical coding systems that must be used within the transactions covered by the *Transaction Rule*. MAGDA-LENA does not prescribe a specific code set but generally recommends the use of existing international or national coding systems if they are suitable for a specific application. All coding systems which are used have to be registered at the Austrian Ministry of health in order to achieve unique identification, including the specification of the organization which is responsible for the maintenance of the coding system.

In the domain *message standards*, HIPAA is more specific in its regulations than MAGDA-LENA. Consequently, HIPAA may be applied in a more "straightforward" manner, whereas MAGDA-LENA is less susceptible to change requirements and may therefore be expected to be more stable over time.

5.3 Identifiers

MAGDA-LENA's section on *identification variables* covers the same domain as HIPAA's part two *Unique Identifiers*, but differs in certain points:

- Whereas MAGDA-LENA recommends the use of the social security number for the identification of patients, HIPAA discourages the user from doing so. HIPAA considers the US's social security number unsuitable because of its multiple usage in other (e.g., credit and financial) domains, which would allow undesired linking with health information. In contrast, the Austrian social security number is meant to be used only in the health domain.

- For the identification of health care providers, HIPAA prescribes the introduction of the *National Provider Identifier* (NPI). Existing identification numbers assigned by different health plans to health care providers are not suitable, since providers who do business with multiple health plans have multiple identification numbers. MAGDA-LENA currently does not prescribe a new comprehensive identification system for all health care providers, but recommends the use of individual, existing identification schemes for different classes of health care providers (e.g., identification of physicians by their partner contract number of the Main Association of Austrian Security Institutions).

- HIPAA proposes a specific identifier for employers, namely the *Employer Identification Number* (EIN). MAGDA-LENA does not suggest a separate

identification system for employers, but includes them in the general identification scheme for all participants of the health data network. To distinguish between different types of network participants, each participant's role will be specified by the Austrian Ministry of Health.

- In contrast to HIPAA, MAGDA-LENA includes specifications about the unique identification of health documents.

In the *identifier* domain, MAGDA-LENA currently follows the strategy of using existing identification schemes wherever possible. This makes the MAGDA-LENA identifiers immediately applicable, but entails that several shortcomings of existing identifiers are inherited. HIPAA makes a big effort to develop new, universal identification schemes for various players in the healthcare arena. Although this process will require some more time (currently only the *Unique Employer Identifier Rule* is final), it affords an opportunity to correct various shortcomings of existing identifiers.

5.4 Privacy and security

As regards content, MAGDA-LENA's section on *data privacy and security* is similar to HIPAA's *Security* and *Privacy Rules*. HIPAA's *Privacy Rule* even legitimates Austrian healthcare institutions to exchange personal health data with US partners, although this is otherwise prohibited by European law: Under the EU's *Directive on Data Protection* (24), on which MAGDA-LENA's section on *data privacy and security* is based, the communication of personal health data to a non-EU country is only allowed if this country can ensure an "adequate level of data protection" as determined by the EC. The US's *Safe Harbor Privacy Principles* (25) were accepted by the EC to provide adequate protection. As the HIPAA *Privacy Rule* is consistent with the *Safe Harbor Principles*, the exchange of personal health data between Austrian (European) and US institutions is allowed, provided that the other prerequisites (e.g., patient consent) are fulfilled.

However, apart from the fact that MAGDA-LENA merges the topics *privacy* and *security* within a single section whereas HIPAA covers them within two separate rules, a few other less obvious differences deserve to be mentioned:

- MAGDA-LENA provides concrete guidelines as to how to technically implement data privacy and security, recommending, amongst other aspects, specific encryption algorithms and protocols. HIPAA's *Security Rule* rather offers high-level guidance, essentially providing a model for information security with less specific guidance on how to implement the model.
- HIPAA's *Privacy Rule* covers the transmission and maintenance of identifiable health information, regardless of the medium on which it is stored. This especially includes non-electronic data. MAGDA-LENA's section on *privacy and security* is primarily concerned with the exchange of healthcare information, and also addresses internal privacy and security issues of MAGDA-LENA participants. Although MAGDA-LENA does not explicitly exclude non-electronic data from its scope, its current provisions only relate to electronic data.
- MAGDA-LENA requires health information to be de-identified (allowing later re-identification) for its processing or exchange, wherever possible. HIPAA only encourages covered entities to use de-identified information wherever possible but does not demand it. Instead, §164.502(b)(2) and §164.514(d) require covered entities to make reasonable efforts to limit data to the "minimum necessary" to accomplish the intended purpose (which may be de-identified information).
- De-identified information is not subject to the requirements of HIPAA's *Privacy Rule*. MAGDA-LENA, however, covers the exchange of all identifiable and de-identified health information. Only anonymous health information which may not be re-identified is not covered by MAGDA-LENA.

- HIPAA's *Privacy Rule* provides two alternative methods to de-identify health information (see §164.514). First, a person with appropriate knowledge applying generally acceptable statistical and scientific methods for de-identification declares that there is a very small risk that the information could be used for identification. Alternatively, the *Privacy Rule*'s *safe harbor method for de-identification* (not to be confused with the *Safe Harbor Privacy Principles*) may be used, which enumerates a list of 18 identifiers (e.g., name, street address, social security number) to be removed. Further, no indication must exist that the remaining information could be used, alone or in combination, for identification. When used for research purposes only, data may (in mitigation of the *safe harbor method*) also include admission, discharge, and service dates, date of death, age (including age 90 or over), and five-digit zip codes. For this so-called "limited data set" option, a data use agreement has to be obtained from the data recipients, in which they agree to limit the use of the data to the purposes specified in the *Privacy Rule*, to limit who may use or receive the data, and agree not to re-identify the data or contact the individuals. MAGDA-LENA describes a method for de-identification (26), which is based on achieving so-called "k-anonymity" for secondary identifiers (attributes whose values, in combination, enable identification; e.g., zip code of a small town and a rare profession) after removal of primary identifiers (e.g., social security number). A record is considered *k-anonymous* (and thus de-identified) if it can be shown that at least *k* other records with identical values for secondary identifiers exist.

Summing up, MAGDA-LENA's section on *privacy and security* is more implementation-oriented than HIPAA's *Security Rule*. In contrast to the *message standards* domain, this makes the application of the corresponding MAGDA-LENA directives more "straight-forward", whereas HIPAA remains more flexible to technological progress.

5.5 Network providers and nodes

HIPAA does not contain a chapter comparable to MAGDA-LENA's section on *network providers and nodes*. However, HIPAA's *Security* and *Privacy Rules* require business associate contracts in cases where a covered entity uses a third party to transmit health information. Hereby, the covered entity may oblige network providers to safeguard the information from misuse.

6 Conclusion

Keeping abreast of current developments in applied medical informatics, substantial progress has been made over the past few years toward establishing a nationwide healthcare information network in Austria. In this paper we have presented the underlying strategic iterative approach which was shown to yield good results:

- In the first step, a general framework named MAGDA-LENA was set up, which provides a set of guidelines to direct electronic medical data exchange. A first version of the MAGDA-LENA directive was published in 1998 and received wide public attention.
- In the second step, detailed message standards for various healthcare communication scenarios are being developed, based on the guidelines. Existing national or international standards have been used wherever possible. In cases where no suitable standards are available, the MAGDA-LENA framework provides a procedural model for uniform development of new messages.
- The third step consists of implementing these standards by organizing corresponding pilot projects. The results of the third step are being used to further develop the general guidelines.

Based on the first version of MAGDA-LENA, a number of pilot projects have been started. In coordination with the STRING commission, Austrian health service institutes have implemented the guidelines. The experience gained during the first practical implementation period clearly revealed the necessity to stipulate the regulations more explicitly and precisely. This led to the development of a more detailed second version of MAGDA-LENA, which is, for example, much more explicit in the specification of identifiers and catalogs. As was done with its first version, MAGDA-LENA's version two was tested in practical pilot projects. This second implementation period brought the insight that the conversion of existing applications to the new and highly extended specifications entail an enormous workload. On account of the high costs involved, some of the conversion work has thus been delayed or not carried out at all.

The HIPAA framework represents an approach for guiding healthcare data exchange in the US that is comparable with MAGDA-LENA. So far the compliance deadlines of two of its rules (*Transaction* and *Privacy Rules*) have passed, which means that adherence to their provisions is obligatory. In its effort of further advancing the rules, which incorporates public reactions to existing provisions, the HHS has adapted the Transaction and Privacy Rules since their first publication. Within the Transaction Rule, modifications can be grouped into i) changing the usage of particular data elements from required to situational, ii) removal of certain data elements, iii) allowing certain information to be reported via external code sets, and iv) adding additional functionality to some transactions. Modifications to the Privacy Rule include certain alleviations in the use and disclosure of protected health information (PHI) for the purpose of treatment (e.g., consent is now optional), payment, healthcare operations, and research (e.g., "limited data set option"), and on business associate requirements. Use and disclosure of PHI for marketing purposes is now, however, limited in comparison to the original rule. An Electronic Signature Standard, which should originally be included in the Security Rule was postponed to allow ongoing work of the industry to be incorporated. Work on a unique identifier for individuals was halted due to privacy concerns.

MAGDA-LENA and HIPAA are very similar in respect of their general goals and content. Individual differences within the domains of *message standards*, *identifiers*, *privacy* and *security* have been discussed in section 5. An obvious difference between the two frameworks is the fact that HIPAA is legally binding, whereas MAGDA-LENA currently only has recommendatory status.

The feedback from the detailed version two of MAGDA-LENA has shown that the extended regulations cannot be thoroughly fulfilled on a voluntary basis but have to be sustained by law. For this purpose, the MAGDA-LENA framework has been integrated into a new Austrian law for health telematics. A first draft bill of this law was circulated for opinion in 2002; its revision is still in progress.

Acknowledgments

The authors wish to thank Ernst Leitgeb and Verena Spiteller for their valuable suggestions.

References

1. Health Insurance Portability and Accountability Act (HIPAA). http://www.hhs.gov/ocr/hipaa/.
2. European Commission, Directorate General Information Society. The eEurope initiative. http://europa.eu.int/information_society/eeurope/index_en.htm.
3. European Commission, Directorate General Information Society. The E-Health initiative. http://europa.eu.int/comm/health/ph_information/e_health/e_health_en.htm.
4. European Commission. Health and Telemedicine Projects co-funded by the European Commission. http://www.ehto.org/ht_projects/index.html.
5. CEN/TC 251. European Standards in Health Informatics. http://www.centc251.org/FinWork/greensheetpwd.htm.
6. CEN /TC 251. Revised proposal for a new work item entitled: Health informatics – Guidance on good practice for patient identification in the process of care; 2003. Report No.: CEN/TC 251/N03-009rev. http://www.centc251.org/TCMeet/doclist/TCdoc03/N03-009rev-PatientIdentification-NWP.pdf.
7. MedCom. http://www.medcom.dk/.
8. HYGEIAnet. http://www.hygeianet.gr/.
9. Tsiknakis M, Katehakis DG, Orphanoudakis SC. An open, component-based information infrastructure for integrated health information networks. Int J Med Inf 2002;68(1-3):3-26.
10. International Standards Organization Technical Commitee 215 (ISO/TC 215). http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720.
11. European Committee for Standardization Technical Committee 251 (CEN/TC 251). http://www.centc251.org/.
12. Austrian Standards Institute. http://www.on-norm.at/index_e.html.
13. Beeler GW. HL7 version 3--an object-oriented methodology for collaborative standards development. Int J Med Inf 1998;48(1-3):151-161.
14. Beeler GW, Huff S, Rishel W, Shakir AM, Walker M, Mead C, et al. HL7 V3 Message Development Framework; 1999. http://www.hl7.org/library/mdf99/mdf99.pdf.
15. The openEHR foundation. http://www.openehr.org/.
16. Ingram D. The Good European Health Record Project. In: Ladeira MJ, Laires MF, Christensen JP, editors. Health in the New Communications Age. Amsterdam: IOS Press; 1995. p. 66-74.
17. Burggasser H, Dorda W, Gambal J, Gell G, Ingruber H, Kotschy W, et al. Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz (MAGDA-LENA V2.0); 2000. http://www.akh-wien.ac.at/STRING/.

18. CEN/TC 251. Health informatics - Electronic healthcare record communication. European Prestandard: European Committee For Standardization; 2000. Report No.: ENV 13606. http://www.centc251.org/FinWork/greensheetpwd.htm.

19. CEN/TC 251. Medical Informatics - Methodology for the development of healthcare messages; 1996. Report No.: CR 12587. http://www.centc251.org/FinWork/greensheetpwd.htm.

20. UN/CEFACT. Unified Modelling Methodology (UMM); 1999. Report No.: CEFACT/TMWG/N090. http://www.unece.org/cefact/.

21. Austrian National Counsil. The Austrian Signature Act; 1999. Report No.: BGBl. I Nr. 190/1999. http://www.signatur.rtr.at/en/legal/index.html.

22. Austrian National Counsil. The Austrian Signature Ordinance; 2000. Report No.: BGBl. II Nr. 30/2000. http://www.signatur.rtr.at/en/legal/index.html.

23. Electronic Business using eXtensible Markup Language (ebXML). http://www.ebxml.org/.

24. European Commission. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995. http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

25. US Department of Commerce. Safe Harbor Privacy Principles; 2000. http://export.gov/safeharbor/.

26. Simonic K, Gell G. MAGDA-LENA Datenschutz-Policy für die Kommunikation in Forschung und Lehre; 2001. http://www.uni-graz.at/imi/datenschutz/index.html.