© *The Journal on Information Technology in Healthcare* 2005; **3**(5): 295–300

Communication Support for Managed Care

Ulrike Müller[*], *Gert Funkat*[*], *Dirk Jaeckel*[†], *André Kaeding*[‡], *Alfred Winter*[*]

[*] Institute for Medical Informatics, Statistics and Epidemiology, [†] Clinical Center, University of Leipzig and [‡] GMC Systems, Leipzig, Germany.

ABSTRACT

The focus in healthcare is gradually shifting from isolated procedures in single healthcare institutions (e.g. a hospital) to patient-oriented care extending across institutional boundaries. A main objective of this approach is to reduce healthcare costs by decreasing hospital stays and increasing community care. To achieve this objective in practice, all relevant treatment facts must be made available to different care providers at the point of care. This paper describes an approach by which information technology can support managed care by providing a communication solution that meets user requirements.

INTRODUCTION

Managed care requires close cooperation and co-ordination of services provided by different health-care professionals across both primary and secondary care (trans-sectoral)[1]. Its main objectives are to:

- Standardise treatment
- Avoid repetition of documentation, examinations and investigations
- Decrease hospital stays
- Improve the quality of care
- Reduce healthcare costs

Managed care structures exist in several countries including the USA[2], Switzerland[3], the United Kingdom[4] and Germany. A prerequisite for successful trans-sectoral managed care is that all relevant treatment facts are easily and readily available to different care providers at the point of care. In practice, this is best achieved through the use of electronic patient records. However, the electronic exchange of patient information requires a communication infrastructure that satisfies both technical and legal requirements.

Correspondence and reprint requests: Ulrike Müller, Institute for Medical Informatics, Statistics and Epidemiology; University of Leipzig, Härtelstr. 16/18, 04107 Leipzig, Germany. E-mail: ulrike.mueller@imise.uni-leipzig.de.

In this paper we describe one approach to finding a suitable communication solution for the exchange of patient data between different healthcare institutions. We detail both potential obstacles as well as possible solutions to demonstrate that the approach can be used in countries that do not have a sophisticated telematic infrastructure.

METHODS

Analysis of Requirements

The first step in creating a communication infrastructure is to identify the requirements of the potential users. For the purpose of this study these were the physicians of the Clinical Center of Leipzig University and physicians working in private medical practices in Leipzig.

To analyse their needs, an initial workshop, was set up between physicians from the Clinical Center and information technology (IT) experts. The physicians described their needs and their expectations of how IT could help their practices. In return the IT experts identified potential solutions as well as limitations due to IT-infrastructure and legal requirements. A second workshop was also conducted to explore the requirements of the physicians in private practices.

From the workshops the following requirements were identified:

Clinical Center of Leipzig University. Patient data in the Clinical Center of Leipzig University is already documented in electronic format using the Center's administration and clinical documentation system (IS-H/IS-H*MED). Implementing a duplicate documentation system is therefore not a sensible option. To maintain the usual practice workflow, it is necessary for data generated by physicians in private medical practice and sent to the Clinical Center of Leipzig University to be integrated in IS-H/IS-H*MED. Ideally, the data should be presented as it is generated in the Clinical Center of Leipzig University. This means that a communication solution has to offer standardised exchange formats, such as XML (extensible markup language)[5] or HL7 (Health Level 7)[6], that could be integrated in IS-H/IS-H*MED by the communication server of the Clinical Center of Leipzig University.

Physicians in private practices. The introduction of new or additional application systems is likely to be met with strong resistance in the private sector. This is mainly due to the costs and time associated with implementing the systems and training staff to use them. Inevitably, the private sector would like systems that can be integrated in their workflow with the minimum amount of changes in their daily processes.

Data security. German data security legislation requires personal data to be protected by technical and organisational sanctions. Data must have the following parameters guaranteed:

- *Confidentiality* – only beneficiaries have access to the data

- *Integrity* – data cannot be read, changed, copied or deleted during the communication and storage process by unauthorised persons
- *Authenticity* – the author of the data is identifiable
- *Availability* – the data is protected from loss

POINT OF DEPARTURE

Presently there are more than 200 different software products installed in German medical practices, ranging from single installations to over 14,000 (approximately 14% of market share)[7]. In hospitals, application systems frequently exchange data using HL7 communication standards or the standards for Digital Imaging and Communications in Medicine[8], whereas in the private sector data is often exchanged using xDT-Data (xDT is an ASCII [American Standard Code for Information Interchange] file standard based around numeric tags and field content. xDT standards define more than 500 items including medical, laboratory and billing data. Examples are: ADT = billing/claims information, BDT = medical data, indication-based disease data, GDT = medical device data, LDT = laboratory data and laboratory orders)[9]. Efforts are being made to develop and establish a uniform communication standard (e.g. Standardized Communication of Information Systems in Physician's Offices and Hospitals using XML [SCIPHOX][10]), but this is still

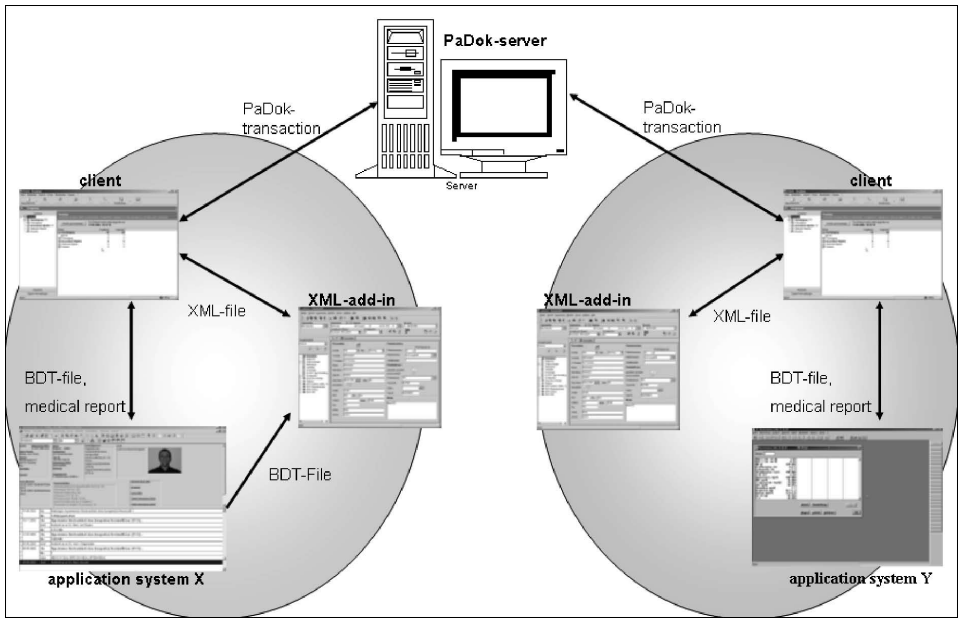

Figure 1: *The PaDok® system*

BDT = Medical Data File; XML = Extensible Markup Language.
(Source: Kaeding and Jäger-Glogauer, 2003[13] – adapted)

in progress. Two potential existing solutions to enable secure electronic exchange of patient data are PaDok® and VCS interface.

PaDok®. PaDok® (Patient Accompanying Documentation) is a system developed by the Fraunhofer Institute to enable secure, platform-independent, system-wide exchange of patient data between medical care providers[11]. Transmission of data requires the sender and recipient to be identified. However, for many routine care processes, e.g. electronic prescriptions or electronic radiology requests, a precise recipient cannot be identified at the time that the message is generated and sent. PaDok® therefore has the facility to make a message available to an authorised group e.g. pharmacists or radiologists. The data is stored on a server (Figure 1) in encrypted format with encryption taking place prior to the message being sent. Access to the data is controlled by the patient who provides healthcare professionals of his or her choice with a key to access the data and decrypt it.

VCS. VCS is a communication standard that has been developed by the German Association of Vendors of Software for Medical Practices (VDAP)[12]. The VCS standard defines the communication path based on Internet standards and also identifies the content and structure for business transactions. For the communication path, a number of protective measures exist to guarantee a high level of data security at anytime:

- Authentication
- Encryption
- Digital signature
- Acknowledgement service including expiry date

The communication is only possible via VCS-certified network operators[12].

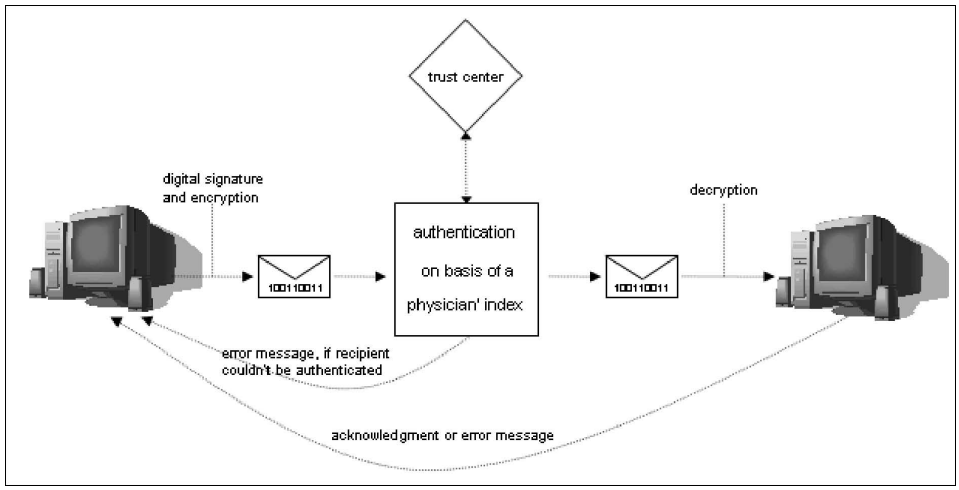

Figure 2. *The VCS System*
(Source: VDAP, 2001[13] – adapted)

Unlike PaDok®, the precise recipient of the message has to be known when the message is sent. Before the encrypted and signed message is delivered, the sender and recipient are authenticated on the basis of a physician's index that is stored in a trust centre. After a successful delivery, the sender receives an acknowledgement. Otherwise, an error message is sent. The operating mode is shown in Figure 2.

INTEGRATION ARCHITECTURE

There are four possible ways of creating a communication infrastructure as shown by the target matrix in Table 1.

The analysis of requirements in this particular project revealed that the communication solution for the Clinical Center of Leipzig University has to enable encryption, authentication, digital signature and the integration of patient data into different application systems. From the matrix shown in Table 1 it is clear that only VCS or PaDok® satisfy these requirements. In view of the fact that PaDok® offers more flexibility with respect to selecting medical practitioners to send communications to, this system seems preferable to VCS.

DISCUSSION

In choosing an appropriate communication infrastructure solution to allow electronic data exchange of patient data between different care providers, user requirements and legislation must be taken into account. Users require a system that will easily integrate with their existing medical records but at the same time provide a high degree of data security. The system should also be flexible enough to accommodate normal working practices, for example referring a patient to a department (e.g. Accident and Emergency) rather than a specific person.

From the available solutions to meet these requirements, PaDok® is currently the most suitable. It should, however, be appreciated that it does not enable

Table 1. *Target matrix*

	No integration of data into application systems	Integration of data into application systems
Encrypted communication	Encrypted e-mail communication	VPN*-tunneling
Encrypted communication including authentication and digital signature	Online health records	e.g. VCS or PaDok®

VPN = Virtual private network and represents a network constructed by using public wires to connect nodes. For example a network can be created by using the Internet as the medium for transporting data. Encryption and other security mechanisms are used to ensure that only authorised users can access the network and that the data cannot be intercepted.

complete integration of all IT systems in medical practices. It does, however, provide a major step forward in communication and integration of medical data by enabling the secure exchange of digital or digitised documents. It should also be appreciated that successful use of such systems is ultimately dependent on user engagement. At present many physicians are not particularly interested in the use of such systems and are happy continuing with their existing systems and practice. To successfully engage them, benefits will need to be demonstrated and incentives may need to be offered.

REFERENCES

1 Riedel R, Schmidt J, Hefner H. *Leitfaden zur Integrierten Versorgung*. http://www.bkk-nrw.de/projekte/leitfaden_integrierte_versorgung/; 2004.
2 Lagoe R, Aspling DL, Westert GP. Current and future developments in managed care in the United States and implications for Europe. *Health Research Policy and Systems* 2005; **3**: 4.
3 Fisher MA. Managed care und Ärztenetzwerke in der Schweiz. *Primary Care* 2003; **46**: 940–94.
4 Stevens S. Reform strategies for the English NHS. *Health Affairs* 2004; **23**: 37–44.
5 Bray T, Paoli J, Sperberg-McQueen C, Maler E, Yergeau F, Cowan J. *Extensible Markup Language (XML) 1.1*. www.w3.org/TR/1998; 2004.
6 Health Level 7. http://www.hl7.org.
7 KBV. *Installationsbestand zu ADT-Abrechnungssystemen pro Anbieter/System*. http://daris.kbv.de/daris/link.asp?ID=1003737294; 2004.
8 DICOM Standards Committee. http://medical.nema.org/.
9 KBV. *xDT – Synonym für elektronischen Datenaustausch in der Arztpraxis*. http://www.kbv.de/it/xdtinfo.htm; 2004.
10 Heitmann K. Elektronische Kommunikation im Gesundheitswesen. In: Eissing U, Noelle G, Kuhr N (eds.), *MEDNET Arbeitsbuch für die integrierte Gesundheitsversorgung 2002/3*, Bremen: Edition Temmen, 2003, pp. 176–183.
11 Fraunhofer Institut für Biomedizinische Technik. *PaDok®-Patientenbegleitende Dokumentation – Ein Konzept zum sicheren Austausch vertraulicher medizinischer Daten*. http://www.ibmt.fraunhofer.de/Produktblaetter/MT_padokdoku_de.pdf; 2002.
12 VDAP Verband Deutscher Arztpraxis-Softwarehersteller e.V. *VCS – der neue Standard für die elektronische Arzt-Arzt-Kommunikation*. http://www.vdap.de/html/vcs/vcs.html; 2001.
13 Kaeding A, Jäger-Glogauer B. *"Tele-DMP" – Unterstützung des DMP Diabetes durch mobile Datenerfassung. Hauptstadtkongress Medizin und Gesundheit*, Berlin 24. http://www.hauptstadtkongress.de/2003/tagungsbeitraege/kaeding.pdf; 2003.