Identity Management for Health Professionals

A Method for the Integration of Responsibility, Organization, and IT

In many hospitals, it is not possible to ensure that the medical staff responsible for a patient or case have access to the necessary information on diagnoses, treatments and therapies as and when required and in accordance with compliance regulations. The information is available in applications which are structured according to professional groups (doctors, care staff, therapists), and access to that information is not oriented towards processes. A hospital-wide system for managing identities (user accounts, permissions) is missing. While the technical means can be obtained, responsibility is not clearly defined and consequently neglected. The present article provides a maturity model for assessing the as-is situation and formulating objectives, a procedure for applying the maturity model and reports from practice on its successful use in two large Swiss hospitals.

DOI 10.1007/s12599-012-0244-2

The Author

Prof. Dr. Peter Rohner,
Assistant Professor (✉)
Institute of Information Management (IWI)
University of St. Gallen
Mueller-Friedberg-Str. 8
9000 St. Gallen
Switzerland
peter.rohner@unisg.ch

Received: 2011-12-04
Accepted: 2012-10-04
Accepted after three revisions by Prof. Dr. Buhl.
Published online: 2013-01-23

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Rohner P (2012) Identitätsmanagement für Behandelnde in Krankenhäusern. Reifegradmodell und Methode zur Integration von Verantwortungs-, Organisations- und IT-Aspekten. WIRTSCHAFTSINFORMATIK. doi: 10.1007/s11576-012-0346-y.

1 Introduction

1.1 Integration Tasks in Hospitals

Among doctors, care staff and therapists in hospitals there is a high level of specialization between and within the professional groups as a result of a strong disciplinary tradition (Glouberman and Mintzberg 2001). The hospital organization combines these specialized services rendered by the professional groups into one service for the patient. The services are provided jointly by specialist doctors, care staff and therapists in departments such as those for internal medicine, surgery, or gynecology (Anderson and McDaniel 2000). The medical services required by various departments and clinics such as intensive-care medicine, or anesthesiology, which also involve direct treatment of the patient, are frequently housed in separate units. The departments and clinics call upon the medical services with an indirect involvement in patient treatment such as radiology, laboratory, or pharmacy on a case-by-case basis. Traditionally, the management of clinics or departments and medical service sis decentralized and based on medical disciplines (Vera and Kuntz 2007). Working practices and the software used to support them have been developed for specific professional groups and are strongly focused on medical discipline (Niemann et al. 2002). The heterogeneity of services, processes and software is far greater than in organizations belonging to other sectors (Haux et al. 2004)and has evidently shown no significant change in over a decade (Bihr and Seelos 1997).

The treatment processes can be set up within an organization, e.g., between various professional groups within a hospital, or on a collaborative basis with external partners, e.g., between a hospital and a registered medical practice. In both scenarios, the applications have to meet particularly high demands where identification is concerned. An incorrect allocation between patient and e.g., medical prescriptions or a doctor's lack of access permissions to an application in an acute situation can have fatal consequences (Looser 2010). In view of the growing number of treatment sat interdisciplinary centers (Braun von Reinersdorff 2007), increasing quality and patient safety requirements, and the simultaneous rise in pressure for treatments to be economically efficient (Farsi and Filippini 2006; Bohmer 2009), the need for process-orientation in hospitals is becoming ever more important (Bartz 2006; Mentges 2006; Rotter et al. 2010). Against this background, it becomes essential for the collaboration between medical staff who are directly involved with the patient to be coordinated on a process-oriented basis (Dykes and Wheeler 2002). Interdisciplinary pathways enable the coordination of patient processes from admission

through to discharge and the planning of further patient treatment (Palm 2009). With pathways of this kind, treatments also become controllable in terms of effectiveness (success of treatment) and efficiency (length of stay in the hospital and use of resources) (Haraden and Resar 2005). When the patient is transferred from one professional group to the next on the pathway of diagnosis, treatment and therapy, the information relating to the patient's case must be correct, appropriate to the user and available at the right time (Van Bemmel and Musen 2000). Information on patients and cases must therefore be available in the departments and clinics involved over the entire patient pathway (Cinquini et al. 2009). As an example, a medium-sized Swiss hospital will need to access the following software over the course of a treatment in different departments: clinical documentation, scheduling and operation planning, bed management, personnel deployment planning, activity recording, laboratory order processing, radiology image management, materials management, medication, patient administration and finally billing. This requires on the one hand integration mechanisms for exchanging the information (Münz et al. 2008) and, on the other, control (assign, edit, withdraw) of the permissions that enable medical staff to access the information across all software (Apitzsch 2008). Statutory documentation requirements mean that it must be possible to establish at any point in time "who did what when and why with what outcome with and for whom" (Haas 2005, p. 153). In view of the personal significance that the clinical information can have for the individual patient and the fact that the patient records belong to the patient, high data protection requirements have to be met. These have to be applied over the entire pathway and therefore consistently for all software components used (De Clercq 2008). However, this requirement gives rise to a conflict with daily practice since "doctors and care staff … want data access to be as comprehensive as possible so that they can react quickly in emergency cases or when required to deputies at short notice" (Hoffmann 2010, p. 115). Moreover, group logins are used in many hospitals due to the frequent changes in personnel and the use of temporary and relief staff (Hoffmann 2010, p. 115).

In addition to the increase in process orientation, there is another factor driving the integration of processes and software (Aier and Winter 2009). Hospitals are increasingly striving for external cooperation, i.e. for a division of labor and networking with other service providers. This manifests itself, for example, in care networks (Albrecht and Töpfer 2006). Care processes (patient pathways as well as material and value flows) then have to be set up which span several healthcare organizations, e.g., general practitioners, hospitals offering basic care, specialist clinics and rehabilitation centers. The applications, however, are currently designed for the respective institution and not for inter-organizational cooperation (Connel and Young 2007). In the absence of national or regional solutions for exchanging information (Healthnet British Columbia 2003), cooperation partners in care networks have to make their own arrangements, e.g., with mutual access via web interfaces and/or bilateral information exchange.

In summary, it can be said that identity management in hospitals has already attained or is set to attain considerable importance as a result of growing process orientation and cooperation (Fitterer and Rohner 2010). When considering the required identification tasks, it is possible to differentiate between the following:

- The exchange of information on cases and patients between applications (Mettler et al. 2007) for the purpose of assisting diagnoses, planning and managing treatments, documenting processes, enabling transfers between areas of responsibility or carrying out administrative activities (Haux et al. 2004).
- The regulation of staff access permissions to enable the management and documentation of access to applications (information on cases and patients) and resources (e.g., access to rooms, workplaces, equipment) (Ingenerf and Stausberg 2005).

To this end, the identities of medical staff and details of their assigned access permissions (Links 2008) for all required applications along the pathway have to be appropriate (e.g., restricted for support staff), timely (e.g., made available at the latest when the attending doctor begins the diagnosis or treatment activity supported by an application), consistent (e.g., always the same for each diagnosis or treatment and for medical staff exercising the same role) and traceable (e.g., in respect of authority in the treatment process).

At the same time, the required identity management in hospitals must be suitable for

- large quantities of identities (patients and medical staff),
- high turnover (e.g., high number of cases and many changes of doctors in training rotation),
- high complexity (e.g., due to the high number of different applications and dynamic transformations of organization units as well as the accumulation of data protection regulations that occurs along the patient pathway),
- eHealth scenarios, i.e. loosely coupled applications (processes and software) of several cooperation partners.

1.2 Gaps in Identity Management in the Real World of the Hospital

Against this background, the coordination of technical, organizational and leadership aspects of managing the identities of patients and medical staff becomes particularly important. To obtain a picture of the status of identity management in hospitals, interviews are conducted with a total of 22 representatives from Swiss hospitals. Of these institutions, 17 can be categorized as medium-sized hospitals with 200 to 400 beds and five as large hospitals with more than 400 beds (for categorization cf. BFS 2006). The selected interviewees meet the job profile of the hospital IT manager (Köbler et al. 2010). The interviews begin with questions relating to hospital services (clinical service offering and quantity), hospital organization (clinical and administrative processes), applications used (software and platforms), IT organization (positioning in the hospital organization, available resources, and established service processes) as well as IT context (strategy, leadership, and governance). The current individual situation is then discussed in the interviews with regard to:

(i) identification of cases and patients,
(ii) identification of staff, with an emphasis on medical staff.

Here, reference is made to the two integration scenarios

(a) integration of the hospital's own software for internal cooperation,
(b) integration of the hospital's own software and the software of external cooperation partners.

Figure 1 shows the dimensions of integration and identification, supplemented by the differentiation according to purpose (administrative and clinical) for which the information is used in the applications.

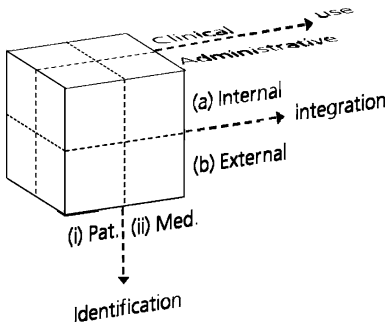

Fig. 1 Identification dimensions

The statements made in the interviews lead to the following findings with regard to *(i) the identification of cases and patients*. When integrating the hospital's own applications (integration scenario a), bilateral interfaces or platforms for Enterprise Application Management (EAI; cf. Niemann et al. 2002; Khoumbati and Themistocleous 2006) are used to transfer case and patient data. Mapping tables are maintained between applications to synchronize the identifiers (key attributes) of cases and patients. Individual hospitals use a Master Patient Index (MPI; cf. Lenson 1998) which enables identifiers to be mapped across multiple applications. Bilateral interfaces or EAI tools for transferring case and patient data are also used between the applications of different hospitals (integration scenario b). For case and patient identification (identification type i), regional MPIs are being set up which ensure the unique assignment of information to cases and patients when exchanging data. For both integration scenarios (internal cooperation in integration scenario a and external cooperation in integration scenario b), the hospitals interviewed have stable technical tools and experience for their planning, implementation and operation. As a result, the identification of cases and patients is well established for the exchange of clinical and administrative information between different applications.

With regard to the *identification of medical staff and other employees* (*identification type ii*), the interviews show the following picture. In 18 of the 22 hospitals, authentication (login to an application by entering user name and password) is separately controlled by each application, in other words without preceding access management. Six hospitals use strong authentication for specific applications, e.g., with chip cards. In three of these hospitals, the chip cards are used for other purposes such as meals accounting. The medical staff identities required for authentication and authorization are separately managed in the various application sat all the hospital staking part in the interviews, in most cases by the respective application managers within IT. They receive the change notices (start, change, departure) from the HR department, directly from the departments or clinics on forms, or as unstructured messages (e.g., "… has the same activities as" or "… same programs as for…, please"), open or modify accounts and also take care of assigning permissions (authorizations) to users. In this context, problems were mentioned throughout with setting up or closing accounts on time (or failure on the part of the line manager or HR to notify in good time) as well as with the coordination with other activities such as purchasing IT equipment, providing rooms, or entries in access systems. These problems negatively affect job starts, employee satisfaction with the IT infrastructure and the first impressions of new employees. Around one third of the hospitals interviewed use tools (e.g., commercial software for provisioning or programs written in-house). These are used for the initial distribution of identity attributes (new employees) from a source application (typically an HR application) to one or more target applications so that they can be imported as user attributes. In the other hospitals, the attributes are also entered manually for new employees. In view of the effort observed for updating user information in the individual applications and the error rates involved, the hospitals expect to see short-term benefits from projects aimed at process improvement and at the automation of user data distribution, such as time savings and better services. Nonetheless, tools fur Role-Based Access Control (RBAC; cf. Fuchs and Pernul 2008), which would help to translate medical responsibility into the authorization components of the various software by means of role definition and consequently enable the uniform adoption of data protection and compliance requirements (cf. Wortmann and Winter 2007), are only used across applications in two of the 22 hospitals interviewed. For this reason, the differentiation and assignment of user permissions for software for clinical or administrative purposes (cf. **Fig. 2**) have to be taken care of separately in all applications. The possible synergies between support services, e.g., HR, Facility Management, and IT Management, when processing employee starts and departures are expected to mean that projects for coordinating support services would pay off in the short term, e.g., by freeing up working time for other activities, which would be of direct benefit for staff. However, projects of this kind are not considered feasible as long as support service managers fail to take a common view on identity management.

A key finding which can be concluded from the 22 interviews is that the use of technical solutions (tools) only resolves problems relating to technical aspects of exchanging user data between different applications. Organization and leadership tasks, on the other hand, which arise in hospitals in conjunction with the use of technical solutions for managing the identities of medical staff, remain largely unresolved. The interviews revealed significant gaps relating to the management of HR processes (start, change, or departure of employees) and the coordination between line, HR and IT with regard to responsibility for user accounts as well as requesting, specification (e.g., permissions) and provision.

Another finding to emerge from the interviews concerns the lack of initiative and clear responsibility for identity management at the level of the individual departments or clinics and consequently the necessity to address the topic at the level of the hospital as a whole. There is little willingness on the part of the individual departments, clinics, and support organizations to invest time in closing the gaps (i.e. leveraging potentials) in the management of medical staff identities. Department and clinic heads concentrate their sights on their own units and therefore fail to see any immediate benefit for their own "business". The organization units medically and financially responsible for the applications, e.g., radiology for image management (RIS/PACS; cf. Huang 1999), the clinical departments for clinical information systems (CIS; cf. Haux et al. 2004), the administration for planning and billing systems (ERP), are either not willing or not able to (jointly) finance an integrated solution for identity management within their budgets for projects and operation of their applications. Their focus is instead limited to creating and operating the infrastructures required for their particular applications. The relationship between their contribution to a solution for the hospital as a whole and any immediate benefit for their own units is unclear. While

the value of an integrated solution in terms of the information obtained for their own field of work rapidly becomes visible for everyone involved in it, there are strong variances in willingness when it comes to preparing information for the purpose of passing it on to downstream departments. The potentials for the organization as a whole are therefore not utilized, e.g., the effects of defining and documenting the organization structure for the entire hospital, management of the process structure across departmental boundaries and the harmonized regulation of compliance across applications. Even if a general consensus existed and there was a willingness to invest in a "solution" for medical staff identity management for the entire hospital, in the wake of which many follow-on projects would stand to profit, the appropriate approach for introducing and operating a hospital-wide system of identity management addressing the key aspects of responsibility, organization, and technology would be missing.

2 Challenge

2.1 Consistency of Responsibility, Organization, and IT

The interviews showed the absence of an approach which can bring forward responsibility aspects (e.g., clear assignment of roles), organization aspects (e.g., process design), and technical aspects (e.g., tools for distributing account data to different applications) of managing the identities of medical staff throughout the entire hospital[1] in a coordinated fashion in terms of both content and timescale. This raises the question of what particular conditions an approach of this kind should take into account. It also became clear from the interviews that above and beyond the technical aspects, the design of identity management systems can mean significant changes for medical staff with regard to the division of labor as well as responsibility and authority within and between departments and support services. For example, the assignment of authority in clinical and administrative cases is considerably altered by processes for defining roles and by the assignment of these roles to people which control the respective processes (amongst others for the purpose of allocating permissions). The same applies to the granting of access permissions to documentation. The apparently "technical" topic of identity management can change responsibilities, obligations, and positions of power.

In hospitals, substantial changes in responsibility and organization are difficult due to a priori resistance to reforms (Vogd 2006). In the majority of cases, such substantial changes fail (Walston and Chadwick 2003). Obvious approaches such as Business Process Redesign (Davenport and Short 1990; Al-Mashari and Zairi 1999), which can provide a framework for the method to be developed in this paper, are nonetheless aimed precisely at dealing with radical changes to processes, structures, and behaviors of this kind. For this reason, they can meet with resistance from hospital staff, jeopardizing IT-related projects in particular (Fernando et al. 2010). In view of the fact that, in comparison with other sectors, process orientation in hospitals remains in its infancy (Helfert 2009), the reservoir of best practice in dealing with changes and resistance to their introduction remains limited, or aimed at individual aspects such as specific disciplines or situations. The use of maturity models (Gibson and Nolan 1974) as a tool for taking stock of the current situation and planning for change nonetheless enables different perspectives and stakeholders to be taken into account when tackling changes (Bessant and Caffin 1997; Lindberg and Berger 1997). Maturity models are also a highly suitable approach for (further) developing very different aspects (e.g., capabilities, tasks, technology) in a coordinated fashion. For this reason, a maturity model should be used for the integrative design of technology, organization, and responsibility for medical staff identity management (cf. Sect. 3.2 for the fundamental principles of maturity models). Literature research shows that a model of this nature does not exist. Based on an analysis of the interviews (cf. Sect. 1.2), the following requirements have been formulated for the design of the maturity model:

A. Coordinate development of the aspects technology, organization, and responsibility for identity management in the hospital (the maturity model should depict the maturity levels of these aspects),
B. Analyze and visualize the current status of these aspects (hospital-wide or specifically for individual departments or support areas; the maturity model should allow the depiction of the as-is situation regarding these aspects),
C. Show potentials for optimization (the maturity model should offer maximum positions for each aspect),
D. Define and visualize target statuses (the maturity model should offer positions which can be defined as target positions or stages and along which it is possible to develop maturity level),
E. Define the steps to achieve those statuses and in so doing create the foundation for defining projects (by describing the positions, the maturity model should also implicitly show the change required in the hospital to achieve the respective gain in maturity),
F. Create a common goal on the part of hospital management, senior clinical staff (e.g., senior consultants, care staff managers) as well as heads of the support areas HR and IT (the maturity model should provide an overview of the as-is situation, the target situation and the stages towards its achievement); make that common goal communicable, and provide the appropriate documentation and communication to those affected (primarily doctors, care staff and other patient-facing hospital employees as well as affected employees in support areas) for each stage.

On the basis of these requirements to be met by a maturity model, the research questions are as follows:

– Question 1: Which aspects of technology, organization, and management have to be considered in the maturity model for identity management in hospitals?

[1] For the integration between the applications of different institutions (external cooperation, integration scenario b), technical concepts for distinguishing between centralized authentication and decentralized authorization are known under the heading of "Identity Federation" in the hospitals surveyed (cf. Böhm and Caumanns 2007). As yet, however, no solutions have been implemented or any concrete planning steps taken. In none of the hospitals surveyed is it clear how the various organizational structures and processes as well as the different compliance and security policies of the institutions involved are to be taken into account. What is clear throughout, however, is that "order" first has to be established in internal identity management before link-ups with external partnerscan be initiated.

– Question 2: What development stages have to be defined for these (partial) aspects in order to be able to analyze and visualize the as-is situation for a hospital, show the potentials, define a target situation and the steps towards achieving it as well as deriving the appropriate projects?
– Question 3: How does one proceed with the maturity model in order to create a common goal on the part of line management, HR, and IT in the hospital, to ensure documentation of the common goal along with the logical planning derived from it, and to support communication to management and parties affected?

The research process follows the Design Science Research Methodology (Hevner and Chatterjee 2010, based on Peffers et al. 2007):

1. Problem identification and motivation (cf. Sects. 1.2 and 2.1)
2. Define the objectives for a solution (cf. Sect. 2.1)
3. Design and development (cf. Sect. 3 for creation of the foundations and Sect. 4 for design of the maturity model for identity management)
4. Demonstration (cf. Sect. 5.1 Testing)
5. Evaluation (cf. Sect. 5)

For design, tests, and evaluation, different focus groups (Gibson and Arnott 2007) of hospital representatives are involved within the framework of this method. With regard to the characteristics and number of members, the composition of these groups follows the recommendations for healthcare focus groups (WHO 2008) on the one hand, and for focus groups in the area of design-oriented information management on the other (Hevner and Chatterjee 2010).

2.2 Sequence of Research Work and Structure of This Article

Section 3 begins with a description of the fundamental principles of identity management. This includes the state of the art in the literature along with a look at other sectors and the current status in hospitals. An outline of current findings regarding the construction and use of maturity models follows. Sect. 4 starts off with the construction of the maturity model on the basis of the requirements. The model is then embedded in a method so that it can be applied in practice. The artifact (maturity model and application method) is then complete. The evaluation of the artifact is documented in Sect. 5. The artifact is first put to the test within the framework of a project at a university hospital. Following the results of the test, adjustments are made and another application takes place in a project at a central hospital. The impact of the artifact and findings obtained from the perspectives of research and practice are discussed in Sect. 6. The article concludes with an outlook for further research. **Table 1** provides an overview of how the article is structured in the context of DSRM.

3 Solution Building Blocks

3.1 State of the Art in Identity Management

Sectors outside the healthcare system such as banking, insurance, or telecommunications are a step further than hospitals when it comes to the use of tools for employee identity management (Hoffmann 2010, p. 113). This experience gained outside the hospital sector can serve as the foundation for designing the maturity model for identity management in hospitals. In the extensive literature on identity management in other sectors or from a sector-neutral perspective, the approach to the topic varies depending on viewpoint (cf. **Table 2**). Todorov (2007, p. 39) emphasizes and deals with the technical aspects of data protection in conjunction with identity management by focusing on the "authentication challenges". Mackinnon (2007, p. 105) emphasizes the user perspective and defines identity management as "… providing the right people with the right access at the right time…". Lux (2007, p. 34) understands identity management "fundamentally as the controlled use of digital identities and the associated permissions" and derives the necessity for appropriate methods (creation, distribution, use, termination/archiving). Mezler (2008, p. 10) considers identity management as "the sum of all measures which are necessary for the unique identification of persons and users in IT systems and to provide them with the precise access permissions currently required in the exercise of their duties. All the associated measures are to be performed within the framework of standardized and transparent processes". He therefore makes it clear that mastery of the processes for administration of the digital identities is an important part of identity management. To summaries these sources, the challenge in identity management lies in mastering the two dimensions

– Coping with the quantities (through process automation),
– Coping with the requirements for correctness at all times (through process control).

The requirements to be met by process automation rise with the number of applications and users as well as with the rate of personnel turnover. The requirements to be met by process control increase with the continuing specialization of the organization and applications as well as with the growing importance of data protection (Satchell et al. 2006) and compliance (cf. Herwig and Schlawitz 2004). As observed further above, this leads to high demands in respect of both dimensions in the case of hospitals. For process automation, i.e. for handling (high) quantities, Lux (2007) proposes the definition and management of processes for start, change, and departure of users as well as processes for role administration (combined allocation of permissions to resources) and assignment. He introduces the following perspectives: data provision service (management of a user directory), transaction service (shared login functions for the associated applications), and administration service (synchronization of user data between the associated applications). Mezler (2008) proposes four layers: personal data, resources (users, account), authorization (roles, permissions), and authentication (access).

For process control, i.e. ensuring the correctness of all allocations at all times, Richter (2007) proposes User Account Lifecycle Management (create, modify, delete). Herwig and Schlawitz (2004), Fuchs and Pernul (2008), and Tsolkas and Schmidt (2010) emphasize the importance of role management. Benantar (2006) considers this to be the fundamental prerequisite for effective data protection. Windley (2005) looks at both dimensions and, with a technical focus, proposes an architecture for taking both into account. Like other authors, he also highlights the fact that, on the one hand, the IT infrastructure has to meet specific requirements before identity management can be implemented and, on the other, that clarifying and defining aspects of organization, and responsibility are a sine qua non for the implementation of technical models.

Table 1 Phases and the respective epistemological and design methods applied

Step in accordance with Design Science Research Methodology	Section	Epistemological and design activities in accordance with Design Science Research Methodology	Results
Problem identification and motivation	1.2 Gaps in identity management n the real world of the hospital	• Evaluation of open, guided interviews with experts (22 IT managers from hospitals)	• State of the art, unresolved leadership, and organization tasks
	2.1 Consistency of responsibility, organization, and IT	• Ditto	• Requirements to be met by the maturity model
Define the objectives for a solution	3.1 State of the art in identity management	• Literature analysis	• Aspects of identity management addressed in the literature
		• Focus group workshop with five identity management experts	• Tools currently available (software solutions)
	3.2 Construction and application of maturity model	• Literature analysis	• Design principles
Design and development	4.2 Definition of design objects [parts of the maturity model]	• Focus group workshop with seven members of a Swiss eHealth working group	• Design objects of the maturity model
	4.3 Definition of development stages [for the parts of the maturity model]	• Focus group workshop with seven members of a Swiss eHealth working group	• Development stages for the design objects
		• 12 members of senior hospital management	• Review of the maturity model
	4.4 Embedding in a method [for application of the maturity model]	• 12 members of senior hospital management	• Embedding in a method
Demonstration	5.1 Testing	• Use of maturity model and method in a hospital within the framework of a project	• Testing; adjustment requirements
Evaluation	5.2 Application	• Use of maturity model and method in a hospital within the framework of a project	• Testing of adjustments

Table 2 provides a summary of the aspects emphasized in the discussed literature. The rows of the table show the topics and range from responsibility (top row) to organization (rows two and three) and technology (rows four to seven). The black and white portions of the Harvey Balls indicate the importance accorded to the respective topic by the source authors (named in the columns). A white Harvey Ball indicates that a given topic is not addressed. A black quarter means that a topic is only mentioned but not addressed. A half black, half white Harvey Ball means that reference is given to models, methods, and examples for the topic in question. Three-quarters black denotes that the authors accord a high level of importance to the topic in the overall context (e.g., in concrete terms through the explicit presentation of models and methods along with instructions). A completely black Harvey Ball shows that the authors devote substantive content to the topic, along with concrete proposals for use in specific situations.

In addition to the analysis of the concepts available in the literature, the current offering of technical integration solutions and process automation tools is investigated in a focus group composed of five identity management experts. There are a large number of tools (software) available on the market, which cover the aspects shown above in various combinations. Tools are offered under the heading of "identity management and provisioning services" which support the process of identity management by means of workflow engines (e.g., when a new employee starts work) and can synchronize the attributes of user accounts (e.g., personnel ID, name, roles) collected via the workflows between different applications. This hugely increases the efficiency of the application owners in IT when dealing with large quantities of identities to be managed and high turnover rates. With the identity management software, the user attributes only need to be created once. This software transforms attribute values as required by the target software (e.g., for the attribute name, from John Smith to jsmith) and sends them via connectors for transfer (the actual provisioning) to the target software (in the hospital e.g., to the software for the clinical documentation of cases, the software for personnel deployment planning or the software for encoding diagnoses and activity recording during treatments). Under the heading of "access management" there are tools available on the market, which simplify access to different software for the users. At best, users only need to log in once with the access management system (single sign-on). Authentication with the individual software takes place during

Table 2 Aspects considered in the literature on identity management

Topics \ Source	Benantar (2006)	Fuchs and Pernul (2008)	Herwig and Schlawitz (2004)	Lux (2007)	Mackinnon (2007)	Mezler (2008)	Richter (2007)	Todorov (2007)	Tsolkas and Schmidt (2011)	Windley (2005)
Responsibility for identity management	○	●	○	◔	●	●	○	○	◑	◑
Identity life cycle processes	●	◑	○	◑	●	●	◑	○	●	●
Role definition and assignment	●	●	●	○	○	●	◑	○	●	●
Provisioning platform (workflows, ID distribution)	●	○	◑	●	○	●	●	●	●	●
Tools for role definition and assignment	●	●	●	○	○	◑	○	○	●	●
Tools for user login	◔	◔	◑	◔	○	◔	◑	◔	◕	○
Infrastructure requirements	●	○	◑	●	○	●	●	●	◑	●

run time via access management mechanisms. This leads to a high level of user comfort by reducing the number of login operations required for different software. In hospitals, this accommodates the way doctors and nurses work in the clinical field, which involves frequent changes of location (e.g., moving between examination rooms, treatment rooms, and wards) and often having to login again to a PC or software.

Plans to introduce card solutions for the identification of patients (e.g., in Switzerland the electronic insurance card (VK) or in Germany the electronic health card (eGK)) and medical staff (e.g., the health professional card (HPC in Switzerland; HBA in Germany)) have been defined at national level and are being implemented. In the context of medical staff identity management, the way in which solutions for the administration of health professional cards are handled is relevant (e.g., HBA, HPC). Mauro et al. (2008) have formulated requirements on the basis of a broad survey among IT managers in hospitals and presented solution concepts. The authors point out that in hospitals, the integration of CIS and card solution is necessary and in view of the large number of different CIS and the different card solutions, a ready-made integration solution cannot be expected in each case. This finding is confirmed in the focus group workshop. From the perspective of identity management in hospitals, the national card solutions offer the facility to store identities. In order to be able to use card solutions, however, authentication and authorization by means of the card must be possible for every application in hospitals – and it is possible for a number of applications apart from the CIS to exist. This calls for integration solutions which have to be planned, implemented, and operated. In the focus group workshop, it was reported by all participants that the medical side (departments and clinics) and the management of Swiss hospitals expect the card initiatives (VK, HPC) per se to contribute towards resolving identity management problems in hospitals. This idea needs correcting.

In conclusion from the literature analysis and the session with experts, the following perspectives and aspirations in conjunction with identity management for hospitals are distinguished:

- Responsibility perspective: Defined procedure and clear legal basis for the granting of permissions to users as well as regulations to protect against abuse and manipulation of data relating to both patients and cases and to the identities of medical staff.
- Organization perspective (enterprise level): Definitions, processes, and requirements to be met by IT tools which ensure that the right resources (IT applications, permissions, and personal work equipment, etc.) are uniquely assigned to the right people over the period of use and provided at the right time.

Table 3 Requirements to be met by the artifact based on the gap analysis (cf. Sect. 2)

A	Coordinate development of the aspects technology, organization, responsibility for identity management in the hospital (the maturity model should depict the maturity levels of these aspects).
B	Analyze and visualize the current status of these aspects (hospital-wide or specifically for individual departments or support areas; the maturity model should allow the depiction of the as-is situation regarding these aspects).
C	Show potentials for optimization (the maturity model should offer maximum positions for each aspect).
D	Define and visualize target statuses (the maturity model should offer positions which can be defined as target positions or stages and along which it is possible to develop maturity level).
E	Define the steps to achieve those statuses and in so doing create the foundation for defining projects (by describing the positions, the maturity model should also implicitly show the change required in the hospital to achieve the respective gain in maturity).
F	Create a common goal on the part of hospital management, senior clinical staff (e.g., senior consultants, care staff managers) as well as heads of the support areas HR and IT (the maturity model should provide an overview of the as-is situation, the target situation and the stages towards its achievement); make that common goal communicable, and provide the appropriate documentation and communication to those affected (primarily doctors, care staff, and other patient-facing hospital employees as well as affected employees in support areas) for each stage

– Organization perspective (user level): Definitions, processes, and requirements to be met by IT tools which ensure that users' own permissions enable them to fulfill their tasks, that their identity cannot be abused (relief from the burden of proof) and that they can rely on the identity of other users.
– Technical perspective: Tools (software) with pre-authentication procedures (resulting in the creation of digital identities as objects for the identification of subjects), mechanisms for identification (e.g., reading of object) in all applications as well as for the administration of all digital identities of all users for all applications, including cards, e.g., of health professional associations.

3.2 Construction and Application of Maturity Models

The maturity of processes, organizations, or information systems, understood to mean their completeness and perfection, can be measured on the basis of their capabilities or impacts. Gibson and Nolan (1974) were the first to develop the maturity approach. This enables the analysis of characteristics and capabilities through comparison with predefined development stages which can range from a rudimentary level through to perfection. A large number of maturity models have been developed in science and practice since then and have proved very popular in areas such as process management and quality management (de Bruin et al. 2005). In the field of software development, the Capability Maturity Model (CMM) became established at the end of the 1980s and the Capability Maturity Model Integrated (CMMI), a further development of the former, from the late 1990s onwards, both of which address the evaluation and development of processes, and structures for the organization of software companies (Ahern et al. 2004). Fraser et al. (2002) attribute the following characteristics to maturity models:

– A specific number of development stages (e.g., 1 to 5), one generic characteristic per development stage (e.g., "ad hoc", "reproducible", "defined", "controllable", and "optimized"),
– Dimensions (parts, design objects) which constitute the entire model and contribute different views,
– A description of the status at each development stage of each part of the maturity model.

Maturity model scan be used as assessment models to examine a specific field for quality attributes, to benchmark with comparable organizations and to obtain ideas for improvements. As optimization models (maturity/capability models), they are used to assess improvement potentials and to control continuous improvement. On the basis of best practice, they indicate an improvement path for a specific field (Paulk et al. 1993). The route to be taken in a specific situation (e.g., sector, size, and positioning of an enterprise where a field is being considered) to achieve improvement (development path) is not usually suggested by maturity models (e.g., Ahern et al. 2004; Fraser et al. 2002). The use of maturity models (de Bruin et al. 2005) for assessment purposes can take the form of self-assessment, supported assessment (e.g., with assistance from external consultants or industry associations) or by third parties (e.g., by a certifying body).

The scientific value of maturity models is continually being questioned, amongst others because the construction (selection of the design objects to model a field as well as definition of the number and content of development stages for the design objects) is based on literature reviews, Delphi methods, or focus groups and is therefore strongly influenced by the designers involved (e.g., Lahrmann et al. 2011).

In the healthcare sector, maturity models have established themselves in the field of quality assurance, e.g., the EFQM model of the European Foundation for Quality Management (EFQM 1999). Gericke et al. (2006) propose the use of maturity models in the health care sector for further strategic, organizational, and technical fields, and for coordinating their optimization.

4 Design of the Maturity Model for Identity Management

4.1 Requirements to Be Met by the Artifact and Its Development

The requirements which practice expects a model or a method for the assessment and systematic development of identity management in hospitals to meet (cf. Sect. 2.1) are repeated in **Table 3**.

The maturity model to be developed has to satisfy these requirements and should be used in hospitals for supported identity management assessments as well as enabling the planned development of this field.

Becker et al. (2009) put forward eight requirements to be met by the development of maturity models in the context of

Table 4 Requirements to be met by the development process for maturity models according to Becker et al. (2009) and how they are addressed in this project

Requirements of Becker et al. (2009)	How the requirements of Becker et al. (2009) are addressed in this project
Comparison with existing maturity models (A1)	Based on CMMI stages, study of maturity models for business/IT alignment (amongst others, Luftman 2000; Santana Tapia et al. 2008), study of accepted maturity models in hospitals (EFQM)
Iterative procedure (A2)	Development of design objects based on literature research and expert interviews, definition of development stages and tests jointly with experts from hospital practice
Evaluation (A3)	Application in multiple tests with focus groups consisting of hospital representatives and in two case studies in hospitals
Multimethodological procedure (A4)	Literature research, analysis of other maturity models from practice, involvement of experts from the healthcare sector as well as identity management project managers
Demonstration of problem relevance (A5)	Interviews in hospitals
Problem definition (A6)	Identification of gaps in identity management in hospitals
Presentation of results in a form appropriate to the addressees (A7)	Conference papers, book chapter, this article
Scientific documentation (A8)	All interactions within the research project are stored in a database along with all documents created and all findings obtained

IT management, which are embedded in a design-oriented research approach. **Table 4** shows how these requirements are taken into account in this article in the construction of the maturity model.

The design process for the model consists of two steps: first, the design objects are defined (cf. Sect. 4.2), then their development stages (cf. Sect. 4.3). For acceptance in practice, two potentially conflicting characteristics must be combined in the model in both steps.

On the one hand, the model must be able to depict the organization, which in the case of hospitals is highly specialized from both a medical and institutional perspective, as well as having varying levels of maturity. To this end, the model must be understood in different environments and therefore be applicable. This means covering a broad range in view of the wide variances in the clarity and rigidity of regulations in the individual medical disciplines and the heterogeneity of the development stages to be depicted. There are considerable differences, for example, between emergency admission, accident clinic, and surgery, elective care areas such as orthopedics, ophthalmology or ENT as well as the laboratory or physiotherapy. On the other hand, the model must be simple in order to encourage its use. Apart from the hospital management, senior clinical staff (e.g., senior consultants, care staff managers) and the heads of support areas, in particular HR and IT, all those affected by or involved in identity management – primarily doctors, care staff, and other patient-facing hospital employees as well as affected employees in support areas – must be able to identify themselves with the model and feel at home with it.

To ensure that sufficient weight is accorded to both of these characteristics, the two development steps are supported by focus groups comprised of hospital practitioners. The experts involved bring knowledge and experience with them, partly in the management and organization of clinics, departments, hospitals, and partly with hospital IT and the technical aspects of identity management (some also from other sectors). The focus groups are prepared for their work by discussing current developments in hospitals such as the process orientation of service provision, the establishment of medical care centers or the professionalization of the various occupational groups as the drivers of changes in hospital information systems, and by reaching a consensus.

4.2 Definition of Design Objects

When defining the design objects of maturity models, the foundations shown in Sect. 3.1, the derived dimensions which identity management is aimed at mastering (quality and quantity) and the identified perspectives (responsibility, organization, technology) are combined to form a model of identity management for hospitals, taking into account practice models for identity management (e.g., Flynn 2007), and assessed in focus group workshops. The focus group is comprised of seven members of a Swiss eHealth working group with a focus on the field of identification (patients and medical staff). **Figure 2** shows the model encompassing responsibility, organization, and technology:

"Responsibility" is located at the top layer of the model. The identity management design object "leadership" is understood to mean the awareness on the part of senior hospital managers and department heads that responsibilities for all aspects of governance and compliance must be clear and that leadership activities are necessary. The middle layer of the model – "organization" – encompasses the organizational perspectives and primarily covers the process control dimension of identity management. For this purpose it contains the two design objects "processes" and "roles". The "technology" layer of the model is aimed at the process automation dimension and consists of multiple design objects. The Meta Directory holds the digital identities (consisting e.g., of surname, name,

[2]The Data Hub can also be connected to applications which administer patient data. If, for example, web-based eHealth services are to be offered to patients and authentication and authorization are necessary for the respective applications, patient data can be extracted and user data created via the DDS.

user name, password) of the people who act as users in at least one of the applications which can use the technical platform of the identity management system. The Data Hub[2] ensures the platform- and application-specific transformation and distribution of user data on the basis of definable rules. A Workflow Management System (WFL) instantiates the processes for the user starts, departures, changes, etc. This enables, for example, the four eyes principle to be implemented in processes, as workflows are able to request the authority for specific permissions from the people responsible. The Self-Service (SES) allows users to edit selected attributes of their own user information (e.g., own mobile phone number) and to request permissions. The Look-Up Service (LUP) can be used to search from within applications according to user attributes in the Meta Directory (e.g., a telephone directory application). The administration components (Admin) are for configuration and administration purposes. The design object Role-Based Access Control (RBAC) is used to depict roles, to combine permissions and resources for those roles, and in order to be able to assign users the appropriate permissions for resources on the basis of roles. As a result, the large number of assignments between users and permissions for specific resources are structured, reduced in number and become better manageable. From the focus group discussions on the RBAC component it became clear that gaps in role management have to be expected in practice because most hospital applications – with the exception of the more modern CIS – do not possess role concepts, which means that the definitions for these applications in the RBAC cannot be instantiated.

With the Audit component, all configurations, and transactions are recorded in order to meet the need for transparency, e.g., due to compliance requirements. Sign-On enables and secures access during run time and permits access to multiple applications with just one login operation (further logins are completed without user interaction). In the focus group workshops, further design objects are identified (by the IT representatives) as essential elements of the technical layer of identity management, for example, the Public Key Infrastructure (PKI) for generating, testing, and administering keys for strong

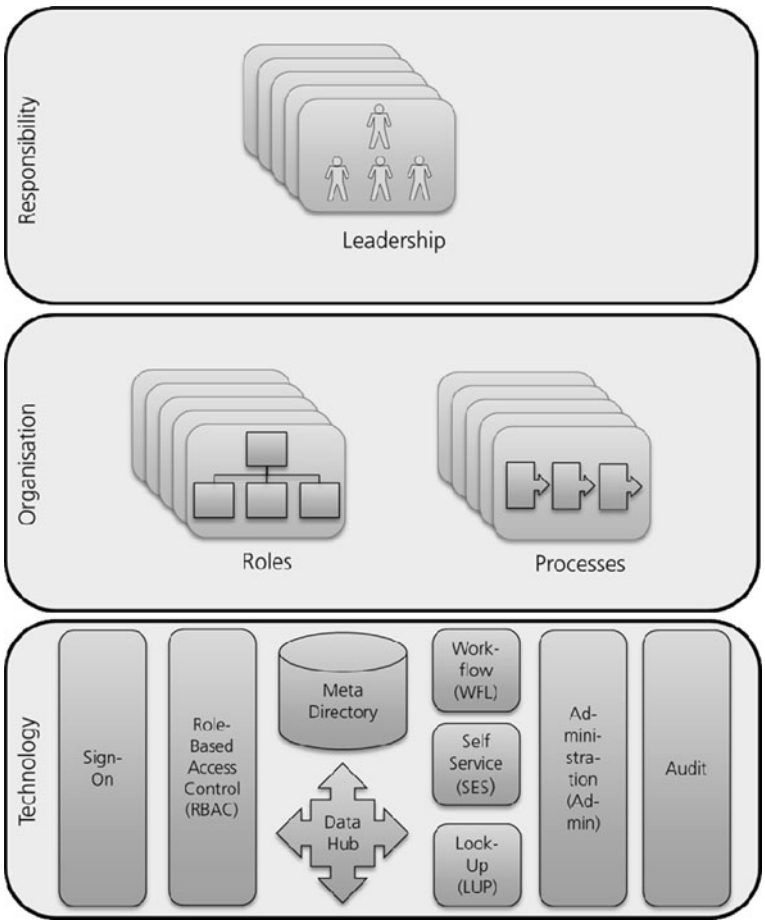

Fig. 2 Design objects (parts) of identity management in hospitals

authentication. This and other technical components have not been included in the following as these are infrastructure requirements rather than identity management design objects. Explicit design objects for identity federation (Böhm and Caumanns 2007), which enables access to applications across institutions with different integration platforms, have also been dispensed with. Identity federation is instead dealt with as a development stage on the technology layer.

CIS are the most important applications in the daily clinical routine (Haas 2005). Following several iterations of adjustments to the model, it is therefore clarified in focus group discussions whether the developed model for identity management in hospitals is compatible with the concepts and models of the CIS which support clinical work and are commonly found on the market. Common CIS contain components which serve the purpose of user and role administration. The approach pursued from the viewpoint of identity management (e.g., data and/or process orientation) and the respective scope of functions (e.g., possibilities for exchanging user data with other applications) vary considerably from one product to another. There are no corroborated findings (e.g., a scientifically founded investigation and analysis) on the extent to which CIS available on the market can directly satisfy the requirements to be met by an identity management solution. In the focus group discussion, however, it becomes clear on the one hand that the built-in utilities of CIS are inadequate for handling the role definitions, role assignments, the HR start, change, departure processes, and the distribution of account data (identity feed, e.g., from the HR application) for the purposes of the developed model. An additional integration platform (e.g., EAI with HR connector or specialized identity management tools) will always be required. On the other hand, it also emerges from the discussion that the concepts and models of commercially available. CIS are compatible with the developed model for identity management

in hospitals (cf. the components Sign-On, RBAC, Meta Directory, Data Hub, WFL, SES, LUP and Audit in **Fig. 2**). Following this test of "connectivity" to the most important category of applications for supporting clinical work, the model is approved by the focus group.

4.3 Definition of Development Stages

Based on the top-down procedure model for the construction of maturity models proposed by de Bruin et al. (2005) and the criteria contained in their model, a maturity model for identity management in the networked hospital is developed in further focus group workshops, taking into account the requirements drawn up further above. The maturity models of Luftman (2000) and Santana Tapia et al. (2008) – both of which focus on IT/business alignment – are used as references for comprehensibility in terms of the various perspectives and professional groups. The structure used above encompassing the three layers of responsibility, organization and technology can be retained. However, the differing number of design objects in the reference model is evened out in the maturity model in order to prevent an overemphasis on technical aspects due to the larger number of technical design objects. To this end, technical design objects which in the view of future users of the maturity models belong together are consolidated. Several design objects on the technical layer are consolidated for the identity management platform. The evolving maturity model is repeatedly checked for maximum simplicity in interim reviews by testing all design objects and all development stages for interdisciplinary comprehensibility. During the course of these applicability and comprehensibility checks, design objects are reorganized in some cases, e.g., "Sign-On" is split into the purposes of protection (on the responsibility layer) and comfort (on the technology layer).

To aid comprehensibility, all terms used for the design objects and their development stages are defined in a glossary belonging to the maturity model. Individual design objects with tool-like characteristics, e.g., RBAC, are incorporated in the development stages of organizational design objects, e.g., roles. When a concrete development stage of a design object explicitly builds on the preceding development stage, this is indicated by "…".

The first iteration gives rise to a different number of development stages for the various design objects (between 3 and 6). A feedback round in the focus group of practitioners shows that a maturity model that has a different number of development stages for the individual design objects is likely to encounter acceptance problems. Maturity models which are commonly found in practice, e.g., EFQM in hospital quality management or CMMI in IT, possess a uniform number of development stages for all elements considered. Despite the fact that this leads to different intervals between the development stages of the individual design objects, development stages based on Fraser et al. (2002) and Ahern et al. (2004) are therefore selected in a second iteration in response to feedback from the practitioners. The concrete development stages are redefined for each design object and checked for measurability. The lower most development stages are chosen to correspond to the status "non-existent/not possible", the following stages must each contain the conditions of the previous stages, and the upper most development stages have to be achievable in practice and also measurable. The development steps between the development stages are checked to ensure they can be formulated as a project. The first representation of the maturity model takes the form of a simple text table.

Tests in hospital practice ensure the required applicability mentioned above (cf. Sect. 4.1) in the environment of hospital organization structures which are highly specialized in terms of medical disciplines and institutions as well as possessing different levels of maturity. Firstly, the tests look at the specific conditions of the respective specialist area (e.g., emergency admissions, accident clinic, surgery, orthopedics, ophthalmology, ENT as well as laboratory or physiotherapy). The next step is to check whether interdisciplinary and integrative planning of identity management design is made possible from the viewpoint of the hospital as a whole. This ensures that the stakeholders (from the specialist areas) can jointly depict and develop the specific as-is status and the specific target status in hospitals with the maturity model. A graphic presentation is prepared (improvement from left to right, development stages in the form of arrows), giving the maturity model in **Fig. 3**.

To test the applicability in practice, the maturity model is presented to 12 members of senior management from 7 medium-sized hospitals (who were not represented in the design phase focus groups) at a workshop on topics relating to business/IT alignment in hospitals. The model is assessed in respect of the functional requirements defined in Sect. 4.1 as well as completeness, consistency, comprehensibility, correctness for hospitals and applicability in different situations. To this end, the workshop participants specify the as-is status of their hospitals in the maturity model along with possible future optima with regard to managing the identities of medical staff. It becomes clear that when using the maturity model, the optimum for the situation of a given hospital is to be identified, rather than aiming for the highest development stage as a matter of principle. The suitability of the maturity models is confirmed throughout.

As another test for the applicability of the maturity model, the depiction of data protection policies is checked. One of the hospitals in which the maturity model is tested has a data protection policy which is based on the relevant laws (national level), ordinances (canton level), and association regulations (for specific professional groups or specific types of department and clinic). This policy stipulates that it must be possible to evaluate all documentation operations at all times for each case, amongst others according to medical staff. The maturity model (cf. **Fig. 3**) can be used in the test to define the target stages resulting from the data protection policy. Comparison with the as-is status makes it possible to identify where further development is needed with regard to responsibility, organization and technology. It becomes clear that methodological support must be provided for dealing with data protection issues when using the maturity model. Requirements arising from the data protection policy of the respective hospital can then be included in assessment and planning in a coordinated fashion while taking all the aspects into account (cf. Workshops 3 and 4 in **Table 5** further below).

4.4 Embedding in a Method

Comments from the participants in this initial explorative testing make it clear

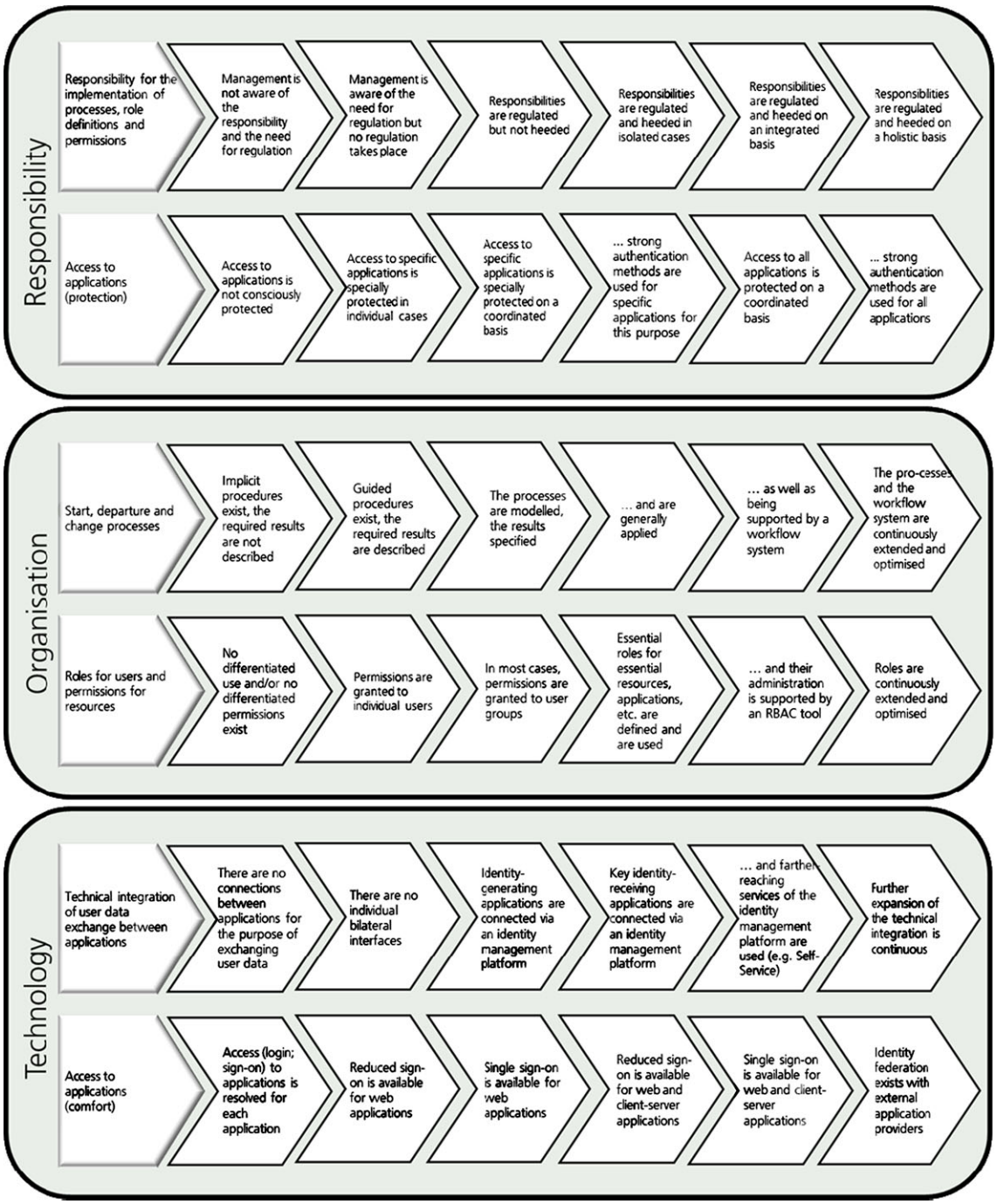

Fig. 3 Maturity model for medical staff identity management in hospitals

that they consider it decisive for the maturity model to be embedded in a project procedure which is accepted in practice and within a project organization (addressing the appropriate levels: steering, management, teams) if the model is to serve its intended purpose (triggering change projects). For better acceptance, the additional involvement of the finance and controlling departments is recommended so that the correlations with the financial structure and reporting (e.g., for profit centers and cost centers) can be taken into account in the identity management solution from the outset. Following these remarks, a method "Preliminary Study for Identity Management" is proposed, based on the procedure for preliminary studies commonly used for feasibility studies in pilot hospitals, which is in turn based on the "Hermes" method (Swiss Federal IT Strategy Board, Informatikstrategieorgan Bund (2012)). **Table 5** shows the method. The columns for describing the activities follow Winter (2003).

In the main study following the preliminary study outlined here, there are again fundamental questions to be asked such as: "What problems (are expected to) arise for implementation of the planned identity management on the IT side?" "Can the coordination within and be-

Table 5 Method for "Preliminary study for identity management"

Activity	Expected results	Involved roles	Techniques used	Templates, sources and tools used
Kick-off:	Common understanding of starting position, necessity for and value of identity management, project purpose and process, objectives of preliminary study, project organization; formation of 3 groups: "Departments and clinics" (working directly or indirectly with the patient), "Support" (HR, Finance, Facility Management, IT infrastructure), "Applications" (IT applications, medical technology)	"Departments and clinics", "Support", "Applications"; jointly	Workshop	Documents prepared individually for the respective hospital based on Sect. 2; software for project management (administration of contact details of group members, activities, documentation, completed models, reports, etc.), referred to below as "project tool"
Workshop 1	Definition of the terms used in the project, common understanding of identity management design objects, identification of key applications for clinical and administrative operations	"Departments and clinics", "Support", "Applications"; jointly	Workshop	Glossary, model with the identity management design objects from **Fig. 2**, project tool
Workshop 2	Objectives and value of systematic approach to the topic of identity management from the viewpoint of the three groups	"Departments and clinics", "Support", "Applications"; individually	Workshops	Model for identifying and assessing benefits (e.g., Royer and Meints 2009; Sward 2006), project tool
Workshop 3	Assessment of as-is status in groups; comparison and analysis of variances	"Departments and clinics", "Support", "Applications"; individually	Workshops; evaluation	Maturity model (**Fig. 3**), project tool
Workshop 4	Scenarios (maturity level to be reached within 12, 24 and 48 months) and benefits per group	"Departments and clinics", "Support", "Applications"; individually	Workshops	Maturity model, project tool
Workshop 5	Agreement on scenarios "12", "24", and "48"; development of the prerequisites to be met in order to achieve them	"Departments and clinics", "Support", "Applications"; jointly	Workshop	Maturity model, project tool
Workshop 6	Request to steering committee to proceed (main study)	"Departments and clinics", "Support", "Applications"; jointly	Workshop	Project tool

tween departments and clinics be put in place as the prerequisite for implementing identity management for medical staff?"

5 Evaluation

5.1 Testing

The maturity model and the method "Preliminary Study for Identity Management" are used on a test basis at a university hospital for acute somatic disorders (6,000 employees, 30,000 in-patient and 160,000 out-patient cases p.a.) with a project team of 19 people. The case (400 applications in total, of which 50 are to be covered by an identity management solution) is published in Mettler and Rohner (2009). In the assessment performed by the project management team, the requirements (cf. Sect. 2) are met by the maturity model and the method in the case as follows (see **Table 6**).

Up to this point (up to and including Workshop 6), the preliminary study has taken around 150 person-days, distributed among some 20 hospital staff (situation analysis, preparing, and holding workshops as well as workshop follow-up, bilateral discussions, visits to other hospitals, drafting the request to the steering committee, presentation to the steering committee, documentation of preliminary study).

The artifact (maturity model and method) served its purpose in its first practical application. As a result of the intensive interdisciplinary work on the topic, it was possible to clearly identify the benefits of coordinated development of identity management, taking into account the aspects responsibility, organization, and technology. In the request to the steering committee it is stated that "… the benefits lie in

- enhanced security through the reduction in access permissions in line with current circumstances and requirements,
- high transparency through clear overview of access permissions,
- reduction in support queries,
- gain in resources, making more resources available for line support,
- faster operational readiness after employee starts or changes,
- gain in flexibility (deputizing arrangements for limited time periods, e.g., for doctors),
- reduction in errors [in user data management],
- delegation of authorization and release of resources by IT employees to clinical managers in the departments and clinics,
- transparency regarding permissions and any subsequent changes to license concepts,
- accuracy, quality, and consistency of data."

The common conception of the benefits became the main driver for further activities. Following the Workshops 1 to 6 using the maturity models, a program

Table 6 Fulfillment of the requirements to be met by the maturity model and the method during testing

A	Bring together the views of technology, organization, and responsibility in one model	Through the joint work of the various stakeholders from departments and clinics, management, and support with the maturity model (at the kick-off meeting, in Workshops 1 and 2 as well as in various bilateral or multilateral meetings in between and subsequently), a common understanding of the identity management design objects (responsibility, organization, and technology) has been arrived at. It was also agreed that only a systematic and joint procedure would serve the purpose.
B	Analyze and visualize as-is status	Workshop 3, which was conducted for each stakeholder group, revealed different perceptions on the status of identity management in terms of responsibility (e.g., "who is responsible for clarifying the roles for doctors at the Department of Otorhinolaryngology from the information viewpoint?", "is that responsibility heeded?"); organization (e.g., "how does preparation for the job start of a registrar at the Department of Otorhinolaryngology work? – who takes care of what?", "who decides which IT equipment is provided for what role?", "how are access permissions that deviate from the role definition requested, approved, and documented in individual cases?", "who takes care of entering personnel data in SAP HR and how far in advance?", "what provisions are made to ensure continuous updating of cost center allocations?"); and technology (e.g., "for access to which applications is strong authentication mandatory?", "who decides whether we should wait for the HPC system as card solution?"). The maturity model proved to be an essential tool for triggering and steering discussions.
C	Make gaps and potentials for optimization visible	Agreement in respect of the different perceptions and unresolved questions was reached at a "consensus workshop".
D	Present target statuses (statuses to be aimed for)	At Workshop 4, scenarios for the coming 12, 24, and 48 months were first depicted jointly in the identity management maturity model by all stakeholders. Following intensive discussions, the scenarios were consolidated into: "rapidly achievable intermediate step" (within two years) and "wall-to-wall optimization as target status" (in another two years).
E	Define steps towards achieving target scenarios (as foundation for defining projects)	Both scenarios were represented as statuses in the maturity model and supplemented with measures to achieve them (Workshop 5). Both provided the grounds for the hospital management to implement the measures (Workshop 6). As the structures and content for planning how to proceed are not stipulated, their description remained at an aggregate level which does not permit any estimates of the investment for the complete project. This actually corresponded to the implicit expectations of the project team for Workshop 5.
F	Create a common conception on the part of line management, HR, IT, and hospital management, and ensure the appropriate documentation and communication to management and affected parties at each stage	A common conception of facts is arrived at in Workshop 3 and documented in the maturity model. The maturity model does not help in arriving at a common conception of the consequences (measures) of the two scenarios and the appropriate conditions to be created because it allows the statuses to be depicted but not the pathway between them.

consisting of three projects was launched in the hospital:
- "Organization structure" project (structures and views),
- "Process structure" project (processes and roles),
- "Technology" project (data hub).

The case evaluation conducted jointly with the project management team results in the possibilities for improvement listed in **Table 7** in addition to the comments on the requirements E and F (divided into findings from the case and consequences for the next case).

In summary, the change aspect is to be given stronger emphasis in the method for the preliminary study as a result of the consequences given above, while the maturity model can be left unchanged.

5.2 Application

The maturity model and the adapted method "Preliminary Study for Identity Management" are applied in a central hospital for acute somatic disorders (2,400 employees, 24,000 in-patient and 140,000 out-patient cases p.a.) with a12-member project team. The case (26 applications to be covered by identity management) shows that, following the adjustments to the method involving the additional results logical planning, report on the preliminary study and foundations for the invitation to tender, the requirements E and F are now also met (the plan is currently being implemented in the hospital).

The maturity model, the procedure model, the glossary, a template (results template for the preliminary study), a generic logical planning approach, and other materials are available via the website ehealth.iwi.unisg.ch/identity_management.

6 Conclusion

Managing the identities of medical staff is an essential infrastructure for process-oriented clinical and administrative work. Identity management includes the technical means (e.g., for user data exchange between applications), organizational definitions (e.g., HR processes for start, change, and departure of medical staff in the hospital as well as role definitions) and regulated responsibilities (e.g., for data protection). In practice, there are shown to be gaps, particularly

Table 7 Findings from initial testing and consequences for adaptation of the artifact

Finding	Consequence
The intention to follow the preliminary study for identity management with a main study creates the impression of a "paper exercise"; implementation is not foreseeable for the members of the project groups; a sense of the urgency is missing	Instead of planning a main study in Workshop 6, projects for each design object are already suggested in Workshop 5 in order to initialize changes more rapidly. A coordinated process is to be ensured with logical planning across all projects.
The method lacks a checklist of all the aspects to be taken into account during the continuing process of improving identity management	A document template containing all aspects in generic form (headings and points to consider) is added to the method. The document template is presented in Workshop 1 as results template for the preliminary study.
One workshop (No. 6) is not sufficient for defining and formulating further procedure for improving identity management	Workshop No. 6 is conducted in two parts; a generic logical planning approach, enabling the work in this workshop to proceed at a faster pace, is added to the method.
The anticipated tasks for the project groups exceed what can be achieved alongside the daily work routine	Not specifically taken into account in the method; assessing the necessary capacity requirements is the task of project management.
Foreseeable obstacles to implementing the logical planning approach are not recorded and taken into consideration as early as possible by the method	Taken into account in Workshop 5.
The information obtained in the preliminary study is only suitable in part for contracting an external provider to perform the implementation (which can be desirable to bring best practice and external drive into the project)	Bring the points to be considered in the document template in line with the orientation of parties not involved in the preliminary study; compile the foundations for putting a complete project out to tender.

with regard to the control of HR processes and the coordination between line (department and clinic management), HR and IT with regard to responsibility for role definitions (permissions) and the request, specification, and provision of user accounts and equipment (IT and medical technology). The following appear to be essential basic conditions for closing these gaps between responsibility, organization, and technology in practice:

- Projects for creating and improving infrastructures for identity management must be coordinated on a hospital-wide basis (not conducted in individual departments and clinics or for individual professional groups).
- Hospital-wide identity management means significant changes, amongst others with respect to powers of authority (e.g., who allows whom to view which parts of which case/patient records?) or transparency (e.g., who has more permissions than others at the same level in the hierarchy?) and consequently a risk of rejection by, e.g., individual professional groups or specific hierarchical levels. In projects creating and improving infrastructures for identity management, the different perspectives of the parties involved and affected professional groups must therefore be properly addressed.

Maturity models enable an objective assessment of the initial situation from different perspectives and the planning of non-radical, manageable steps towards change. A maturity model was constructed to enable a contribution in the form of an artifact towards the creation and improvement of infrastructures for managing the identities of medical staff in the specific context of hospitals. Embedded in a method termed "Preliminary Study", the maturity model leads to the initiation of projects in hospitals in two cases and therefore brings about the desired effect of change.

In conjunction with the cases, an issue repeatedly discussed was whether providing the infrastructure for identity management proactively, based on the assumption of the growing importance of process management, would not in part mean unnecessary time and expense. Up to now, rather than the time-intensive tasks of overcoming resistance and working in projects, the approach had been to wait until the need became acute and triggered the necessary projects and investment budgets. In this respect, the present article leaves it open to question whether better results can be achieved in the individual hospital through "enabling" or "necessitation".

The findings and results should be assessed from the perspective of several limitations. The focus groups and cases are situated in Swiss hospitals for acute somatic disorders which in terms of size are medium and large based on the numbers of in-patient cases. In view of the basic characteristics of hospitals, it is to be assumed that institutions which are smaller (with less than 10,000 in-patient cases p.a.), differ in focus (e.g., rehabilitation) or are located in other countries (e.g., Germany) can also profit from the findings and results. However, this is yet to be put to the test. The use in countries with significant differences regarding regulations such as data protection (e.g., HIPAA in the USA) are likely to require huge adaptations in the weighting of responsibility, organization, and technology (number and differentiation of design objects as well as level of detail in the description of development stages). The maturity model is not directly transferable to other sectors as it was motivated by the specific circumstances in hospitals. The procedure for developing the model and the method for its application could nonetheless be used in other contexts.

From the research viewpoint, the question to be asked is whether newer approaches to designing maturity models (e.g., using the Rasch algorithm, cf. Lahrmann et al. 2011) would achieve a higher degree of differentiation and therefore better (more precise) effectiveness of the artifact, or whether it is precisely the radical simplicity of the model aimed for by the experts involved in its development (only six strongly consolidated design objects to be assessed in terms of their development stages) that determines its value.

To round off the project presented in this article, work is currently in progress

Abstract

Peter Rohner

Identity Management for Health Professionals

A Method for the Integration of Responsibility, Organization, and IT

As a result of growing economic pressures, collaborations and process orientation are rapidly gaining importance for hospitals. With organisation and software landscapes which have grown over time in line with specific professional groups and functions, the paradigm shift places high demands on integration. One of the key challenges in this context is the hospital-wide management of medical staff identities along patient processes. Effective identity management calls for technical means (e.g. for exchanging user data between applications), organisational definitions (e.g. HR processes for starts, departures and changes of hospital medical staff) and regulated responsibilities (e.g. for role definitions). The article shows that while the technical solutions do exist in practice, the necessary prerequisites are frequently missing where organisation and responsibility are concerned. The changes linked with meeting those prerequisites are likely to affect the work of medical staff and can encounter resistance. A very cautious approach is required to the apparently "technical" task of establishing a system of identity management. The article presents a procedure model which has been put to the test in practice. It ensures that responsibility and authority for identity management are successively installed in line with the specific circumstances that prevail in hospitals.

Keywords: Health informatics, Digital identities, Identity Management, Hospital information system, eHealth, Process management, Clinical pathway, Maturity model

to enable use of the maturity model for comparison between hospitals so that participants in the comparison can learn from the best. Integration in an existing IT benchmarking platform of 26 Swiss hospitals is ongoing.

In the medium term, identity management will have to address the need to master the relationships between identifications of patient, medical staff, material, etc. as only an integrated view of this kind can serve a useful purpose such as the interests of patient safety.

References

Ahern DM, Clouse A, Turner R (2004) CMMI distilled: a practical introduction to integrated process improvement. Addison-Wesley, Boston

Aier S, Winter R (2009) Virtual decoupling for IT/business alignment—conceptual foundations, architecture design and implementation example. Bus Inf Syst Eng 1(2):175–191

Albrecht M, Töpfer A (2006) Erfolgreiches Change Management im Krankenhaus – 15 Punkte Sofortprogramm für Kliniken. Springer, Heidelberg

Al-Mashari M, Zairi M (1999) BPR Implementation process: an analysis of key sucess and failure Factors. Business Process Management Journal 5(1):87–112

Anderson R, McDaniel R (2000) Managing health care organizations: where professionalism meets complexity science. Health Care Management Review (Winter) 2000:83–92

Apitzsch F (2008) Digital rights management for electronic health records. In: Proc of the CeHR 2007 international conference, Regensburg

Bartz M (2006) Patientenpfade – Ein Instrument zur Prozessoptimierung im Krankenhaus. VDM, Saarbrücken

Becker J, Knackstedt R, Pöppelbuß J (2009) Entwicklung von Reifegradmodellen für das IT-Management: Vorgehensmodell und praktische Anwendung. Wirtschaftsinformatik 51(3):249–260

Benantar M (2006) Access control sSystems: security, identity management and trust models. Springer, New York

Bessant J, Caffin S (1997) High-involvement Innovation through continuous improvement. International Journal of Technology Management 14(1):14–22

BFS (2006) Statistik der stationären Betriebe des Gesundheitswesens. Krankenhaustypologie. http://www.hplus.ch/fileadmin/user_upload/Spitalinformatik___Statistik/statistik/Krankenhausstatistik/s_krankenhausstat_krankenhaustypologie.pdf. Accessed 2011-09-15

Bihr H, Seelos HJ (1997) Entwicklung eines Referenzdatenmodells für Krankenhäuser. Wirtschaftsinformatik 39(4):367–371

Bohmer RMJ (2009) Designing care: aligning the nature and management of health care. Harvard Business Press, Boston

Böhm O, Caumanns J (2007) Föderatives Identitätsmanagement am Beispiel der elektronischen Fallakte. Informatik-Spektrum 30(4):240–250

Braun von Reinersdorff A (2007) Strategische Krankenhausführung – Vom Lean Management zum Balanced Hospital Managment. Hans Huber, Bern

Cinquini L, Vitali PM, Pitzalis A, Campanale C (2009) Process view and cost management of a new surgery technique in hospital. Business Process Management Journal 15(6):895–919. 6

Connel NAD, Young TP (2007) Evaluating healthcare information systems through an "Enterprise" perspective. Journal of Information & Management 44(4):433–440

de Bruin T, Rosemann M, Freeze R, Kulkarni U (2005) Understanding the main phases of developing a maturity assessment model. In: Proc of the 16th Australasian conference on information systems, Sydney, Australia

Davenport TH, Short JE (1990) The new industrial engineering: information technology and business process redesign. Sloan Management Review 31(4):11–27

De Clercq E (2008) Problem-oriented patient record model as a conceptual foundation for a multi-professional electronic patient record. International Journal of Medical Informatics 77(9):565–575

Dykes PC, Wheeler K (2002) Critical pathways – Interdisziplinäre Versorgungspfade. Hans Huber, Bern

EFQM – European foundation for quality management (1999) The EFQM excellence model. EFQM Representative Office, Brüssel

Farsi M, Filippini M (2006) An analysis of efficiency and productivity in Swiss hospitals. Swiss Journal of Economics and Statistics 142(1):1–37

Fernando S, Choudrie J, Lycett C, de Cesare S (2010) Hidden assumptions and their influence on clinicians' acceptance of new IT systems in the NHS. Information Systems Frontiers

Fitterer R, Rohner P (2010) Patientenidentifikation und Prozessorientierung – Problemstellung und Grundlagen. In: Rohner P, Winter R (eds) Patientenidentifikation und Prozessorientierung. Springer, Berlin, pp 15–32

Fraser P, Moultrie J, Gregory M (2002) The use of maturity models/grids as a tool in assessing product development capability. In: Proc of the IEEE international engineering management conference, Piscataway, NJ

Flynn MJ (2007) Enterprise identity services. http://360tek.blogspot.com/2006/07/enterprise-identity-services.html. Accessed 2011-10-15

Fuchs L, Pernul G (2008) Prorole: a process-oriented lifecycle model for role systems leveraging identity management and guiding role projects. In: Proc of the 16th European conference on information systems, Galway, Ireland

Gericke A, Rohner P, Winter R (2006) Vernetzungsfähigkeit im Gesundheitswesen – Notwendigkeit, Bewertung und systematische Entwicklung als Voraussetzung zur Erhöhung der Wirtschaftlichkeit administrativer Prozesse. HMD - Praxis der Wirtschaftsinformatik 251:20–30

Gibson CF, Nolan RL (1974) Managing the four stages of EDP growth. Harvard Business Review 52(1):76–88

Gibson M, Arnott D (2007) The use of focus groups in design science research. In: Proc of the 18th Australasian conference on information systems, Toowoomba, Australia

Glouberman S, Mintzberg H (2001) Managing the care of health and the cure of dis-

ease – Part I: Differentiation. Health Care Management Review 26(1):56–69
Haas P (2005) Medizinische Informationssysteme und Elektronische Krankenakten. Springer, Berlin
Haraden C, Resar R (2005) Patient flow in hospitals: understanding and controlling it better. Frontiers of Health Services Management 2004 Summer 20(4):3–15
Haux R, Winter A, Ammenwerth E, Brigl B (2004) Strategic information management in hospitals: an introduction to hospital information systems. Springer, New York
Healthnet British Columbia (2003) B.C. healthcare – client identity management strategy report. Verfügbar unter http://healthnet.hnet.bc.ca/hcimsfinalrpt_071803_v1_1.pdf. Accessed 2010-05-10
Helfert M (2009) Challenges of business processes management in healthcare – experience in the Irish healthcare sector. Business Process Management Journal 15(6):937–952
Herwig V, Schlawitz L (2004) Unternehmensweites Berechtigungsmanagement. Wirtschaftsinformatik 46(4):289–294
Hevner AR, Chatterjee S (2010) Design research in information systems: theory and practice. Springer, New York
Hoffmann E (2010) Von der Strategie zur Umsetzung – Unterstützungsprozesse und Identitätsmanagement im Krankenhaus. In: Rohner P, Winter R (eds) Patientenidentifikation und Prozessorientierung. Springer, Berlin, pp 109–136
Huang H (1999) PACS. Basic principles and applications. Wiley, New York
Informatikstrategieorgan Bund (2012) HERMES – Die schweizerische Projektführungsmethode. http://www.hermes.admin.ch/. Accessed 2011-11-21
Ingenerf J, Stausberg J (2005) Klinische Arbeitsplatzsysteme. In: Lehmann M (ed) Handbuch der Medizinischen Informatik. Hanser, München, pp 626–646
Khoumbati K, Themistocleous M (2006) Integrating the IT infrastructures in healthcare organizations: a proposition of influencial factors. The Electronic Journal of e-Government 4(1):27–36
Köbler F, Fähling J, Leimeister JM, Krcmar H (2010) German hospitals—an empirical study among IT decision makers. Bus Inf Syst Eng 2(6):359–370
Lahrmann G, Marx F, Mettler T, Winter R, Wortmann F (2011) Inductive design of maturity models: applying the rasch algorithm for design science research. In: Jain H, Sinha AP, Vitharana P (eds) DESRIST 2011. LNCS, vol 6629, pp 176–191
Lenson CM (1998) Building a successful enterprise master patient index: a case study. Topics in Health Information Management 19(1):66–71
Lindberg P, Berger A (1997) Continuous improvement: design, organization, and management. International Journal of Technology Management 14(1):86–101
Links HC (2008) Identity & access management success tips. Links. Business Group, Issaquah
Looser H (2010) Patientenidentifikation – ein Beitrag zur integrierten und prozessorientierten Versorgung. In: Rohner P, Winter R (eds) Patientenidentifikation und Prozessorientierung. Springer, Berlin, pp 1–14
Luftman J (2000) Assessing business-IT alignment maturity. Comm AIS 4(14):1–10
Lux T (2007) Identity Management. In: Gluchowski P, Chamoni P, Gersch M, Krebs S, Reinersmann S (eds) Schlaglichter der Wirtschaftsinformatik. GUC, Chemnitz, pp 33–46
Mackinnon P (2007) Large-scale identity Management. In: Birch D (ed) Digital identity management – technological, business and social implications. Gower, Aldershot, pp 103–112
Mauro C, Leimeister JM, Sunyaev A, Krcmar H (2008) Zentrale Verwaltung von Gesundheitskarten im stationären Krankenhausumfeld – Das IQ-Medi-LOG-Produkt als Alternative zu gematik-Konzepten. Wirtschaftsinformatik 6(6):489–499
Mentges G (2006) Vom Prinzip Zufall zum geordneten Patientenpfad. In: Debatin JF, Goyen M, Schmitz C (eds) Zukunft Krankenhaus. ABW, Berlin, pp 100–124
Mettler T, Fitterer R, Rohner P (2007) Strategies for a systematical patient identification. In: Proc of the 2nd European conference on eHealth, GI-edition. Lecture notes in informatics (LNI). Oldenburg, Germany
Mettler T, Rohner P (2009) Management digitaler Identitäten von Health Professionals am Universitätsspital Zürich. In: Winter R (ed) Management von Integrationsprojekten: Konzeptionelle Grundlagen und Fallstudien aus fachlicher und IT-Sicht. Springer, Berlin, pp 123–133
Mezler C (2008) In: Identity Management – Grundlagen, Technik, wirtschaftlicher Nutzen. dpunkt, Heidelberg
Münz JO, Müller L, Behavka P (2008) Integration and management of large heterogeneous healthcare information systems. In: Proc of the CeHR 2007 international conference, Regensburg, Germany
Niemann H, Hasselbring W, Wendt T, Winter A, Meierhofer M (2002) Kopplungsstrategien für Anwendungssysteme im Krankenhaus. Wirtschaftsinformatik 44(5):425–434
Palm J (2009) Prozessoptimierung durch Klinische Pfade – Personal und Patienten profitieren von Leitlinienorientierung. f&w Strategie und Organization 26(5):493–496
Paulk MC et al (1993) Capability maturity model, Version 1.1. IEEE Software 10(4):18–27
Peffers K, Tuunanen T, Rothenberger M, Chatterjee S (2007) A design science research methodology for information systems research. Journal of Management Information Systems 24(3):45–77
Richter M (2007) Identity Management – Integration der Benutzerverwaltung in einer heterogenen Systemlandschaft. VDM, Saarbrücken
Rotter T, Kinsman L, James E, Machotta A, Gothe H, Willis J, Snow P, Kugler J (2010) Clinical pathways: effects on professional practice, patient outcomes, length of stay and hospital costs. Cochrane Database of Systematic Reviews 2010. Wiley, New York
Royer D, Meints M (2009) Enterprise Identity Management—Towards a Decision Support Framework Based on the Balanced Scorecard Approach. Bus Inf Syst Eng 1(3):245–253
Santana Tapia RG, Daneva M, van Eck PAT, Wieringa RJ (2008) Towards a business-IT alignment maturity model for collaborative networked organizations. In: Proc of the international workshop on enterprise interoperability. Centre for Telematics and Information Technology, Munich, pp 70–81
Satchell C, Shanks G, Howard S, Murphy J (2006) Knowing Me, Knowing You: end user perceptions of identity management systems. In: Proc of the 14th European conference on information Systems, Göteborg, Sweden
Sward D (2006) Measuring the business value of information technology. Intel Press, Hillsboro
Todorov D (2007) Mechanics of user identification and authentication – fundamentals of identity management. Taylor & Francis, Boca Raton
Tsolkas A, Schmidt K (2010) Rollen und Berechtigungskonzepte – Ansätze für das Identity- und Access Management im Unternehmen. Vieweg & Teubner, Wiesbaden
Van Bemmel J, Musen M (2000) Handbook of medical informatics. Springer, New York
Vera A, Kuntz L (2007) Process-based organization design and hospital efficiency. Health Care Management Review 32(1):55–65
Vogd W (2006) Die Organization Krankenhaus im Wandel – Eine dokumentarische Evaluation aus Sicht der ärztlichen Akteure. Hans Huber, Bern
Walston S, Chadwick C (2003) Perceptions and misperceptions of major organizational changes in hospitals: do change efforts fail because of inconsistent organizational perceptions of restructuring and reengineering? International Journal of Public Administration 26(14):1581–1605
Windley PJ (2005) Digital identity. O'Reilly, Sebastopol
Winter R (2003) Modelle, Techniken und Werkzeuge im Business Engineering. In: Österle H, Winter R (eds) Business Engineering: Auf dem Weg zum Unternehmen des Informationszeitalters. Springer, Berlin, pp 87–118
WHO (World Health Organization) (2008) Focus groups on health care experiences. Verfügbar unter http://www.who.int/responsiveness/surveys/Focus-Group-Mod-Guide-final.pdf. Accessed 2009-11-05
Wortmann F, Winter R (2007) Vorgehensmodelle für die rollenbasierte Autorisierung in heterogenen Systemlandschaften. Wirtschaftsinformatik 49(6):439–447