Sharing With Care
Multidisciplinary Teams and Secure Access to Electronic Health Records

Mohamed Abomhara[1], Berglind Smaradottir[2], Geir M. Køien[1] and Martin Gerdes[2]
[1]*Department of Information and Communication Technology, University of Agder, Norway*
[2]*Centre for eHealth, University of Agder, Norway*

Keywords: Multidisciplinary Team, Collaborative Healthcare, Electronic Health Record, Access Control, Security, Privacy.

Abstract: Ensuring patient privacy and improving patient care quality are two of the most significant challenges faced by healthcare systems around the world. This paper describes the importance and challenges of effective multidisciplinary team treatment and the sharing of patient healthcare records in healthcare delivery. At present, electronic health records are used to create, manage and share patient healthcare information efficiently and effectively. The security and privacy concerns with sharing and the proper use of protected health information need to be highlighted. Additionally, an access control solution is presented, which is suitable for collaborative healthcare systems to address concerns with information sharing and information access. In this access control model, the multidisciplinary team is classified based on Belbin's team role theory to ensure that access rights are adapted dynamically to the actual needs of healthcare professionals and to guarantee confidentiality as well as protect the privacy of sensitive patient information.

1 INTRODUCTION

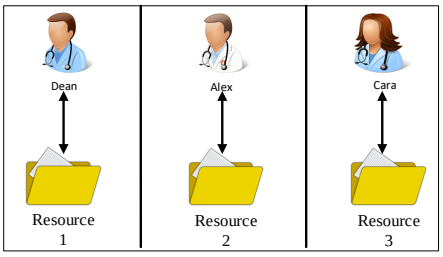
Electronic health records (EHRs) and multidisciplinary teams (MDTs) have become a vital part of modern healthcare delivery (Smaradottir et al., 2016b; O'Daniel and Rosenstein, 2008; Firth-Cozens, 2001). Daily clinical care necessitates the collaborative support of MDTs including healthcare professionals (physicians, specialists, and nurses) and healthcare organizations (clinics and hospitals) (Abomhara and Køien, 2016). Such MDT treatment within or among healthcare organizations has been shown to have immediate and positive impact on patient care (Jnr, 2011; Kim et al., 2010). Moreover, EHRs are widely adopted by healthcare providers and patients to create, manage and share patient healthcare information efficiently and effectively (Chao, 2016). The barrier that currently overshadows the effective use of EHRs is the lack of security control over information flow, whereby protected health information is shared among a group of people within or across healthcare organizations (Abomhara and Yang, 2016; Fernández-Alemán et al., 2013). A major concern is to avoid unauthorized disclosure and improper access to patient healthcare records. Patient records contain sensitive information, which calls for the enhancement and development of existing security mechanisms (particularly access control) to ensure secure sharing of health information (Vodicka et al., 2013; Alhaqbani and Fidge, 2008).

In this study, an investigation is conducted on the collaboration requirements, patient data confidentiality and the need for flexible access of the MDTs corresponding to the requirements to fulfill their duties (section 2), followed by an overview of the existing access control models (section 3). Section 4 demonstrates how the proposed work-based access control model (WBAC) (described earlier by (Abomhara and Køien, 2016; Abomhara and Yang, 2016; Abomhara and Nergaard, 2016; Abomhara et al., 2017)) is suitable for supporting MDT treatment of information sharing and information security. Discussion and critical observations are presented in section 5. Section 6 concludes the study.

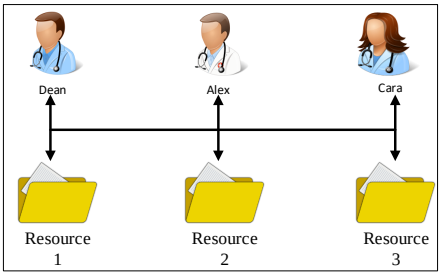
2 BACKGROUND

This section provides a background of MDTs care, EHRs and healthcare record security.

Abomhara, M., Smaradottir, B., Køien, G. and Gerdes, M.
Sharing With Care - Multidisciplinary Teams and Secure Access to Electronic Health Records.
DOI: 10.5220/0006562403790386
In *Proceedings of the 11th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2018) - Volume 5: HEALTHINF*, pages 379-386
ISBN: 978-989-758-281-3



(a) Resource in isolation



(b) Resource sharing in collaborative environment

Figure 1: Resource in isolation and resource sharing (Abomhara and Yang, 2016).

2.1 Multidisciplinary Team Care

A MDT is defined as a group of healthcare professionals from different disciplines, who ideally possess a variety of skills necessary to provide specific patient services with the aim of delivering effective patient care (Jnr, 2011; Firth-Cozens, 2001) and improving the outcomes of patients with complex chronic diseases (Monteleone et al., 2016; Kim et al., 2010). The importance and the effectiveness of MDT have been particularly highlighted in many studies (Jnr, 2011; Kim et al., 2010). A typical example of patient care involving MDT is a pregnant woman (*Amy*) with diabetes who develops a pulmonary embolism (PE) (Monteleone et al., 2016). Her medical care team could include (but is not limited to) an obstetrician, an endocrinologist, a respiratory physician, nurses and others.

One of the key aspects of an MDT is resource sharing (Fabian et al., 2015). To cooperate, each team member must be prepared to gather and share their findings with the other team members. In order to analyze, decide and solve a certain patient case collaboratively, the team members must have similar knowledge of the actual situation. According to Figure 1, each healthcare professional initially accesses their own resource in isolation (Fig. 1(a)). However, upon establishing the MDT treatment, the process of sharing progresses (Figure 1(b)).

Although MDT treatment generally improves patient outcome, there are a number of challenges and barriers to the success of the MDT. These challenges can be insufficient organization and resource management, poor coordination and communication (O'Daniel and Rosenstein, 2008; Firth-Cozens, 2001) as well as health records security and privacy violation (Fernández-Alemán et al., 2013; Coorevits et al., 2013). If the effort in an MDT is not properly managed and organized, productivity may suffer. Good coordination and communication skills are at the core of patient safety and effective teamwork. When healthcare providers engage in an MDT activity, they are required to switch between varying tasks and roles of distinct nature. It implies that the MDT environment must include a systems such as EHRs that assist with task switching accordingly, allows good resource communication between the MDT and the patient, as well as ensures the availability, confidentiality, and integrity of resources by providing them only to those with proper authorization.

2.2 Electronic Health Records

EHRs are compilations of the various types of health records of patients and are stored in electronic format. EHR integration in healthcare organizations (clinics and hospitals) offers potential benefits in terms of improved care quality (Chao, 2016), simplified management and enabling efficient in- and out-patient record exchange. Thus, costs associated with patient care and administrative overhead are reduced (Bain, 2015; Alhaqbani and Fidge, 2008). A significant component of EHRs is the key role in various aspects of facilitating the MDT to fulfil the information requirements of daily clinical care (Chao, 2016). Both healthcare providers (healthcare professionals and/or organizations) and patients can benefit from the EHR feature of health record management and sharing. Patient records can be created by one healthcare professional and digitally shared and reviewed by other professionals instantly.

EHRs can overcome the traditional barriers to MDTs by enabling communication between participants and providing rapid access to healthcare records when distance separates the participants (Vawdrey et al., 2011). It improves how the MDTs work and enables more fluid cooperation and information exchange between healthcare professionals within and among healthcare organizations. To cite an example, within the EU project United4Health (United4Health, 2017), a collaborative telemedicine system for remote monitoring of chronic obstructive pulmonary disease (COPD) was developed to support MDT work across the organization of health care services. Both hospitals and municipal healthcare services have access to

patient information (Smaradottir et al., 2016a). In a related study, a similar system was developed to support collaborative MDT work in dementia healthcare (Smaradottir et al., 2016b; Smaradottir et al., 2015).

Although EHR systems may improve healthcare quality, the digitalization of health records, the collection, evaluation and provisioning of patient data, and the transmission of health data over public networks (the Internet) pose new privacy and security threats (Abomhara et al., 2015; Rostad et al., 2007). Such threats include, among others, (1) improper disclosure of sensitive healthcare information by privileged healthcare professionals, (2) unauthorized access to healthcare information by persons taking advantage of the MDT environment and (3) cyber criminals gaining access to valuable data such as protected health information (PHI) (Abomhara et al., 2015).

Improper disclosure or unauthorized access may occur when someone within the MDT accesses shared resources for unethical reasons (insider threat (Probst et al., 2010)), for instance accessing a patient's private information for personal gain. One of the main causes of an improper disclosure is information leakage, which emerges when a supporting party is granted access beyond what is actually required. In Figure 2, it is assumed that three physicians are working collaboratively on a pregnant woman example (section 2.1) at the hospital. They are discussing the possible treatment for a patient. To do so, they must analyze her medical file but not her personal information. However, the 2nd physician (Alex) is curious about the patient. He exploits the collaborative environment to obtain more personal information without permission.

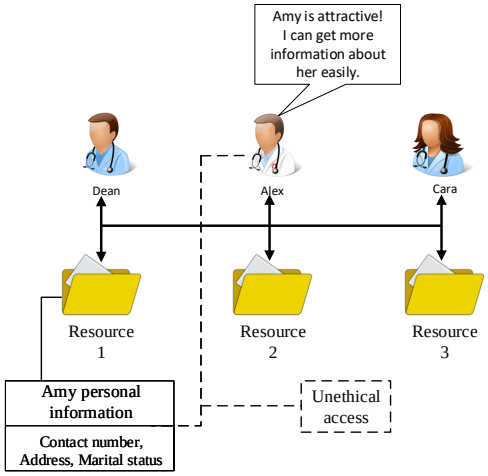


Figure 2: Insider threat.

2.3 Security and Privacy of EHRs

Security and privacy have been a major concern for patient and healthcare providers worldwide (Fernández-Alemán et al., 2013; Liu et al., 2011). These concerns have limited the international adoption of EHRs and their uptake by healthcare providers. Vodicka et al. (2013) carried out a survey on considering online access to patient records and found that approximately one-third of participants had concerns about the security and privacy of their health records. Moreover, according to "the 2017 cost of a data breach study: global overview" report (survey done by IBM and Ponemon Institute (Snell, 2017)), a report on "improving cybersecurity in the healthcare industry" (US Department of Health and Human Services et al., 2017), and a report entitled "hacking healthcare IT in 2016 lessons the healthcare industry can learn from the opm breach" (Institute for critical infrastructure technology, 2016), healthcare data breach costs are the second highest category in comparison. Breaches include stealing protected health information for later use to launch numerous fraud attacks on related medical parties. Thus, the findings of these studies demonstrate that the security and privacy concerns regarding EHRs need to be addressed before EHRs can be fully accepted by patients and health providers.

The "Health Insurance Portability and Accountability Act" (HIPAA) (Nosowsky and Giordano, 2006) and "code of conduct for information security" (Norwegian Directorate of eHealth, 2017) are examples for legislation to protect the privacy of patients' medical records as well as ensure the way health information is used, disclosed and maintained by healthcare organizations and healthcare professionals. They provided a list of security and privacy suggestions and legal requirements to address the need to protect healthcare information. As a means of overcoming authorization and improper access issues associated with EHRs, access control models such as role-based access control (RBAC) (Ferraiolo et al., 2001), attribute-based access control (ABAC) (Hu et al., 2014) and others (Tolone et al., 2005) may prove to be the answers.

3 ACCESS CONTROL MODELS

Access control is the most popular approach for developing an active form of mitigating authorization threats (Rubio-Medrano et al., 2013; Tolone et al., 2005). The most challenging concern with deploying access control in a collaborative healthcare environment is deciding on the extent and limit of information sharing. For instance, if the main physi-

cian is treating a patient with sensitive data, the question is which data should be disclosed to an assisting practitioner so that collaboration can be effective, and which should be hidden to safeguard the patient's privacy (Fernández-Alemán et al., 2013). According to our survey and others' (Fernández-Alemán et al., 2013), it appears that, RBAC is a popular model for access control and it widely employed in medical industry (Rostad et al., 2007). RBAC provides security by utilizing the role of a person in a particular organization. However, it is quite difficult to define access when considering other relevant aspects beyond the one specified by role (e.g., time and location). This was one of the motivations for developing ABAC (Hu et al., 2014). The result of using RBAC is not quite satisfactory. The main reason is that, among others, RBAC are not well-suited with EHRs to handling unplanned and dynamic events (e.g., when healthcare provider asked for second opinions from other healthcare provider) (Fernández-Alemán et al., 2013; Rostad et al., 2007).

It can be concluded that current access control models in most previous studies do not support policies for collaborative MDT environments. This limits these methods to single access to the resources in centralized environments. Thus, extended fine-grained components need to be developed for collaborative healthcare MDT environments (Abomhara and Køien, 2016).

4 SECURE SHARING OF EHRs

To combine the strengths of both RBAC and ABAC approaches without being hindered by their limitations, work-based access control (WBAC) has been proposed by introducing the team role (section 4.1) concept and modifying the team user-role assignment model from RBAC and ABAC (Abomhara et al., 2017; Abomhara and Køien, 2016; Abomhara and Yang, 2016). WBAC enforces a three-layer access control that applies RBAC, a secondary RBAC and ABAC. The secondary RBAC layer, with extra roles extracted from the MDT work requirements, is added to manage the complexity of cooperative engagements in the healthcare domain. Policies related to collaboration and MDT's work are encapsulated in this coordination layer to ensure that the RBAC layer and ABAC layer are not overly burdened. The WBAC model is defined in terms of individuals being assigned to roles or teams, team members being assigned to team roles, work being assigned to teams and permissions being associated with roles and team roles. Role and team role are used in conjunction with dealing with access control in dynamic collaborative environments.

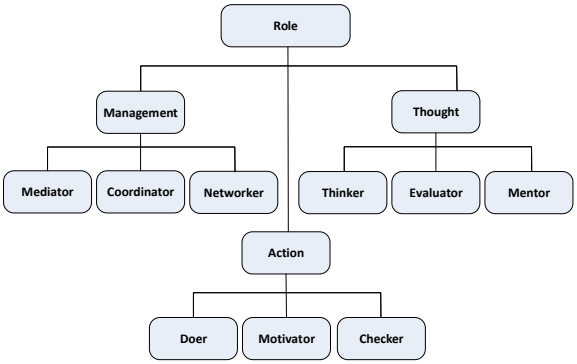


Figure 3: Taxonomy of team role (Abomhara and Køien, 2016).

4.1 Team Role Classification

Hospital personnel roles are often simplistically split into medical practitioners, nurses and administrators, to name a few. However, their roles in an MDT can be further categorized using the team role theory (so-called also Belbin's team roles) (Belbin, 2012; Belbin, 2010).

The effectiveness of MDTs is limited unless they have a clear role and position in organizational structure of the service. Belbin's team role theory is very useful for higher level team building processes, as it helps an experienced facilitator identify patterns that exist within any team and thus underpin their strengths and weaknesses. In previous works (Abomhara et al., 2017; Abomhara and Køien, 2016; Abomhara and Yang, 2016), the MDT was segregated into `thought`, `action` and `management` (Figure 3) based on contributions to the MDT work.

- ***Thought*** denotes a role that is dominated mostly in thinking, analyzing problems and/or providing technical expertise. To be a successful thought collaborator, the person may need to understand the medical predicament in detail without necessarily knowing the patient. A worker in this role could be involved in devising strategies to confront particular medical enigmas. Thus, a cardiology specialist may offer his expertise regarding the best practices of performing a heart transplant on a child without being involved in the actual operation.
- The ***action*** role pertains to team leaders (e.g., primary doctor) and members who are involved in the direct care of the patient, such as meeting the patient for a medical checkup. These team members like physicians and nurses are generally

based where the patient receives treatment. Having an action role usually implies close interaction with the patient. Nevertheless, discretion is still feasible with care.

- The ***management*** category comprises personnel who are mostly involved in managing others (e.g., guide, listen, delegate, and solve conflicts). These types of collaborators are adept at coordinating teamwork. For example, in conflict management, they may have to resolve series of opposing diagnoses made by medical practitioners that may otherwise escalate into serious altercations. In this regard, such personnel's need for information is inwardly oriented. They have a greater need to know personal information about other team members rather than about patients.

4.2 Resource Classification

Medical record classification requires a great deal of effort and skills to accomplish. This is due to problems like, for one, medical records containing a wide range of information (Thomas, 2009), not all of which may be shareable (Asif et al., 2007). It may include personal names, phone numbers, addresses, appointment schedules, to do lists, as well as medical history and surgical history records, to name a few. Some elements of this information may be confidential and sensitive, while others may be open for access. In an environment that supports resource sharing (Figure 1(b)), unwanted parties could retrieve confidential information (Figure 2), thus causing information leakage and leading to the violation of patient privacy. Second, healthcare providers cannot decide on what appropriate information is really necessary in a patient's treatment case.

In general, information sharing is required for treatment; therefore, healthcare providers may use and disclose patient records on the patient's treatment without that patient's authorization. This may occur during consultation between healthcare providers regarding a patient or patient referral by one provider to another. However, in most cases when healthcare providers are dealing with sensitive information regarding the patient, patient authorization is required for disclosure, for instance, the disclosure of psychotherapy notes. According to HIPAA Privacy Rule (US Department of Health and Human Services et al., 2014), psychotherapy notes are treated differently from other mental health information. This is because they contain particularly sensitive information and they are the therapist's personal notes, which are not typically required or useful for treatment or healthcare operation purposes, other than by the mental health professional who created the notes.

It can be said that the amount of information healthcare providers need to complete their tasks may vary greatly. The number of medical records a healthcare provider needs to access over a certain period of time depends on many factors, including the number of patients they serve, the case they are working on, and so on. Moreover, such factors vary among healthcare providers and may change from time to time. It is thus very hard to determine how much risk should be tolerated for a healthcare provider, if the healthcare provider believes that knowing more information that is relevant to their patients conditions enables them to make better decisions (Rostad et al., 2007).

A realistic way of handling collaboration risks is to minimize the discrepancy between granted and required access based on the "minimum necessary" standard to use and disclose records for treatment (Agris, 2014). Thus, resources within WBAC are mainly divided into two types: *protected* and *private* resources. *Protected* resources can be shared within an MDTs work. This depends on whether the collaborative work needs access to the *protected* resources. Contrary to the former type, *private* resources are highly classified pieces of information in medical records that would be shared during the MDT work only if needed. As such, the spreading of access control on the basis of collaboration will not affect *private* resources. It is meant to safeguard certain confidential information from being leaked out accidentally through collaborative means. Consider the example of patient *Amy* given in section 2.1, in WBAC model, it was assumed that personal information (e.g. name, phone number, address, and/or ID, etc) and any medical records unrelated to the current medical case are *private* resources. In this case, only the main practitioner (e.g., primary doctor) should be aware of the patient's personal information. The other medical practitioners with supporting roles are given only information essential for diagnosis (*protected resource*) based on their contributing roles.

4.3 Flow Model of WBAC

The WBAC model utilizes role, team role and WBAC policies to perform an access control evaluation process. First, it checks the access request to verify whether the requesting user (healthcare provider) possesses a valid role specified in the system (first RBAC layer). If the requesting user holds the right role, WBAC will check the permission associated with the role and then inspect the rule(s) within the main WBAC policies for additional constraints (ABAC layer) on access. In other models such as RBAC, fail-

ure in this stage results in the complete termination of the decision process. WBAC, however, treats this differently. If the requesting user does not hold a valid role (in most cases, the requesting user might be an outsider who is invited to collaborative work and does not hold a role in the organization), WBAC investigates further to determine whether the requesting user is part of the collaborative work (a secondary RBAC layer). If so, the respective user's team role is extracted and examined for whether the requesting user possesses a valid team role over the resource. WBAC also checks the permission associated with the team role and checks the rule(s) within WBAC collaborative policies for additional constraints (ABAC layer) on access.

According to the security and performance analysis of the proposed model (Abomhara et al., 2017), WBAC is suitable for collaborative healthcare systems in addressing information sharing and information security matters. It caters to the requirements of access control in collaborative environments and provides a flexible access control model without compromising the granularity of access rights. Moreover, this model is secure and easy to manage for supporting cooperative engagements that are best accomplished by organized, dynamic teams of healthcare practitioners within or among healthcare organizations whose objective is to achieve a specific work (patient treatment case).

5 DISCUSSION AND OBSERVATIONS

MDTs are likely to benefit everyone, but for such teams to keep working well, skills and sufficient coordination as well as resource management are needed. EHRs can improve the work within MDTs, through which medical providers share healthcare information more easily and work together as a team to solve particular medical cases. However, the EHRs might also leave patients more susceptible to privacy violation where confidential information is improperly accessed and exploited by MDT members. It is challenging to predefine all access needs for MDTs based on the subject-object model. One example of such a situation is explained in our example (section 2.1), which may not be predictable and it would be hard to express the condition of who should join the MDT. Moreover, in deciding on the extent and limit of resource sharing, for instance, in the case of *Amy*'s treatment (section 2.1), which sensitive data should be disclosed to an assisting practitioner so collaboration can be effective, and which should be hidden to safeguard the patient's privacy?

There are certain observations that we have learned from the previous studies that should be considered before we could decide on the security model. Observations as follows:

1. **What do patients and healthcare providers want from EHRs?** From the patient perspective, patients found EHRs are useful and acceptable. The majority were concerned about security and confidentiality, including access and disclosure of their records. It's clear that, on the one hand, patients want EHR systems to make health data accessible, available and easy for healthcare provider to find and use. However, on the other hand, they also want to be informed regarding access, disclosure and use of their data. From the perspective of healthcare providers, they want EHRs to make their practice work better, easy to manage and be able to coordinate patient care easily by communicating with one another, deciding who will be doing what interventions and then sharing the information across all of them in a way that EHRs really facilitate (O'Daniel and Rosenstein, 2008).

2. **What is good for security is not necessary useful for MDT practice?** Bridging the gap between security requirements and MDT practice is a critical focus for security researchers. This is a challenge because what is good for security is not always what healthcare providers want. On the one hand, healthcare provider (members of MDTs) need tools such as EHRs to provide, among others, an easy sharing of health information, real-time access to health records and should be easy to use. On the other hand, security seeks to ensure the healthcare records' availability, confidentiality, and integrity while providing them only to those with proper access rights. Security researchers, specifically in access control and authorization, have made the best effort to propose an access control model that balances between security and MDT requirements. Yet, these models do not always meet the needs of MDTs due to the inconsistencies that exist within the MDT workflow and these models' approaches.

3. **How do MDTs form and develop?** In general, many studies (Monteleone et al., 2016; Jnr, 2011; Firth-Cozens, 2001) have discussed the need and the effectiveness of MDTs in healthcare delivery. Yet, however, few address the development of the MDTs in healthcare organization. It would be worthwhile if studies could also be conducted on the forming, storming, norming and performing

of MDTs similar to other industries (Arrow et al., 2000).

4. **EHRs require better ways to securely exchange information:** EHRs are promising to be an ideal solution for addressing the information exchange challenges that today's MDTs are facing. It provides an automated and fast information exchange to healthcare providers within or among healthcare organizations. However, security and privacy mechanisms to ensure secure interoperable EHR applications are slowly beginning to emerge. For access (uses and disclosures) of patient health information, access control policies and procedures must be in place to identify and authorize a healthcare provider or MDT member who needs access to the health information to carry out their job duties, the type of information needed, and conditions appropriate to such access. For example, access control policies should permit only doctors, or other involved in treatment, to have access to patient medical records, as needed.
5. **Legislation and regulation of electronic exchange of health information:** According to HIPPA (Nosowsky and Giordano, 2006) and the code of conduct for information security (Norwegian Directorate of eHealth, 2017), healthcare providers should inform and obtain a patient's permission (e.g., consent or authorization) on how the patient's records are used or disclosed. Under the terms of HIPAA (Agris, 2014), a valid authorization to use or disclosure health information must contain "a description of the information to be used or disclosed"; "the name of the person or entity authorized to make the use or disclosure"; "the name of the person or entity to whom the disclosure may be made"; "a description of each purpose of the requested use or disclosure"; "an expiration date or expiration event" and "the signature of the individual and date".

As a result of this, it could be concluded that, if we don't coordinate the MDT and shared information, we cannot coordinate the patient care, and if we don't coordinate the patient care, we will have inefficiency and poor healthcare quality.

6 CONCLUSIONS

It is evident that EHRs have a great potential to support MDTs work, including but certainly not limited to create, manage and share patient healthcare information as well as facilitate an easy coordination and communication between healthcare providers, thus improving patient satisfaction and engagement. However, unauthorized disclosure and improper access to patient healthcare records are a major concern of this study, where sensitive healthcare data is shared among a group of healthcare professionals within or across organizations.

WBAC was proposed to address these concerns and support the security and MDT requirements on access control. The major contributions of the WBAC model include ensuring that access rights are dynamically adapted to the actual needs of healthcare providers, and providing fine-grained control of access rights with the least privilege principle, whereby healthcare providers are granted minimal access rights to carry out their duties.

REFERENCES

Abomhara, M., Gerdes, M., and Køien, G. M. (2015). A stride-based threat model for telehealth systems. *Norsk informasjonssikkerhetskonferanse (NISK)*, 8(1):82–96.

Abomhara, M. and Køien, G. M. (2016). Towards an access control model for collaborative healthcare systems. In *HEALTHINF'16, 9th International Conference on Health Informatics*, volume 5, pages 213–222.

Abomhara, M. and Nergaard, H. (2016). Modeling of work-based access control for cooperative healthcare systems with xacml. In *Proceedings of the Fifth international conference on global health challenges (GLOBAL HEALTH 2016)*, pages 14–21.

Abomhara, M. and Yang, H. (2016). Collaborative and secure sharing of healthcare records using attribute-based authenticated access. *International Journal on Advances in Security Volume 9, Number 3 & 4, 2016*.

Abomhara, M., Yang, H., Køien, G. M., and Lazreg, M. B. (2017). Work-based access control model for cooperative healthcare environments: Formal specification and verification. *Journal of Healthcare Informatics Research*, pages 1–33.

Agris, J. L. (2014). Extending the minimum necessary standard to uses and disclosures for treatment: Currents in contemporary bioethics. *The Journal of Law, Medicine & Ethics*, 42(2):263–267.

Alhaqbani, B. and Fidge, C. (2008). Access control requirements for processing electronic health records. In *Business Process Management Workshops*, pages 371–382. Springer.

Arrow, H., McGrath, J. E., and Berdahl, J. L. (2000). *Small groups as complex systems: Formation, coordination, development, and adaptation*. Sage Publications.

Asif, K., Ahamed, S. I., and Talukder, N. (2007). Avoiding privacy violation for resource sharing in ad hoc networks of pervasive computing environment. In *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*, volume 2, pages 269–274. IEEE.

Bain, C. (2015). The implementation of the electronic medical records system in health care facilities. volume 3, pages 4629–4634. Elsevier.

Belbin, R. M. (2010). Management teams: Why they succeed or fail. *Human Resource Management International Digest*, 19(3).

Belbin, R. M. (2012). *Team roles at work*. Routledge.

Chao, C.-A. (2016). The impact of electronic health records on collaborative work routines: A narrative network analysis. *International journal of medical informatics*, 94:100–111.

Coorevits, P., Sundgren, M., Klein, G. O., Bahr, A., Claerhout, B., Daniel, C., Dugas, M., Dupont, D., Schmidt, A., Singleton, P., et al. (2013). Electronic health records: new opportunities for clinical research. *Journal of internal medicine*, 274(6):547–560.

Fabian, B., Ermakova, T., and Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, 48:132–150.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3):541–562.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):224–274.

Firth-Cozens, J. (2001). Multidisciplinary teamwork: the good, bad, and everything in between.

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., and Scarfone, K. (2014). Guide to attribute based access control (abac) definition and considerations. *NIST Special Publication*, 800:162.

Institute for critical infrastructure technology (2016). Hacking healthcare it in 2016 lessons the healthcare industry can learn from the opm breach. Institute for critical infrastructure technology.

Jnr, G. O. A. (2011). The effect of multidisciplinary team care on cancer management. *Pan African Medical Journal*, 9(1).

Kim, M. M., Barnato, A. E., Angus, D. C., Fleisher, L. F., and Kahn, J. M. (2010). The effect of multidisciplinary care teams on intensive care unit mortality. *Archives of internal medicine*, 170(4):369–376.

Liu, L. S., Shih, P. C., and Hayes, G. R. (2011). Barriers to the adoption and use of personal health record systems. In *Proceedings of the 2011 iConference*, pages 363–370. ACM.

Monteleone, P. P., Rosenfield, K., and Rosovsky, R. P. (2016). Multidisciplinary pulmonary embolism response teams and systems. volume 6, page 662. AME Publications.

Norwegian Directorate of eHealth (2017). Code of conduct for information security the healthcare and care services sector.

Nosowsky, R. and Giordano, T. J. (2006). The health insurance portability and accountability act of 1996 (hipaa) privacy rule: implications for clinical research. *Annu. Rev. Med.*, 57:575–590.

O'Daniel, M. and Rosenstein, A. H. (2008). Professional communication and team collaboration.

Probst, C. W., Hunker, J., Gollmann, D., and Bishop, M. (2010). *Insider Threats in Cyber Security*, volume 49. Springer Science & Business Media.

Rostad, L., Nytro, O., Tondel, I., and Meland, P. H. (2007). Access control and integration of health care systems: An experience report and future challenges. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages 871–878. IEEE.

Rubio-Medrano, C. E., D'Souza, C., and Ahn, G.-J. (2013). Supporting secure collaborations with attribute-based access control. In *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*, pages 525–530. IEEE.

Smaradottir, B., Gerdes, M., Martinez, S., and Fensli, R. (2016a). The eu-project united4health: User-centred design of an information system for a norwegian telemedicine service. *Journal of telemedicine and telecare*, 22(7):422–429.

Smaradottir, B., Martinez, S., Holen-Rabbersvik, E., Vatnøy, T. K., and Fensli, R. W. (2016b). Usability evaluation of a collaborative health information system. lessons from a user-centred design process. In *HEALTHINF'16, 9th International Conference on Health Informatics*, volume 5, pages 306–313.

Smaradottir, B. F., Martinez, S., Holen-Rabbersvik, E., and Fensli, R. (2015). ehealth-extended care coordination: Development of a collaborative system for inter-municipal dementia teams: A research project with a user-centered design approach. In *International Conference on Computational Science and Computational Intelligence (CSCI2015)*, pages 749–753. IEEE.

Snell, E. (2017). Healthcare data breach costs highest for 7th straight year. HealthITSecurity.com.

Thomas, J. (2009). Medical records and issues in negligence. *Indian journal of urology: IJU: journal of the Urological Society of India*, 25(3):384.

Tolone, W., Ahn, G.-J., Pai, T., and Hong, S.-P. (2005). Access control in collaborative systems. *ACM Computing Surveys (CSUR)*, 37(1):29–41.

United4Health (2017). European commission competitiveness innovation programme.

US Department of Health and Human Services et al. (2014). Hipaa privacy rule and sharing information related to mental health.

US Department of Health and Human Services et al. (2017). Health care industry cybersecurity task force.

Vawdrey, D. K., Wilcox, L. G., Collins, S., Feiner, S., Mamykina, O., Stein, D. M., Bakken, S., Fred, M. R., Stetson, P. D., et al. (2011). Awareness of the care team in electronic health records. *Appl Clin Inform*, 2(4):395–405.

Vodicka, E., Mejilla, R., Leveille, S. G., Ralston, J. D., Darer, J. D., Delbanco, T., Walker, J., and Elmore, J. G. (2013). Online access to doctors' notes: patient concerns about privacy. *Journal of medical Internet research*, 15(9).