The Current State of Electronic Consent Systems in e-Health for Privacy Preservation

Lelethu Zazaza[1,2(✉)], H. S. Venter[1], and George Sibiya[2]

[1] University of Pretoria, Pretoria, South Africa
ul3028023@tuks.co.za, hventer@up.ac.za
[2] Council for Scientific and Industrial Research, Pretoria, South Africa
gsibiya@csir.co.za

Abstract. Consent management is a significant function in electronic health information systems as it allows patients to manage the privacy preferences regarding their health information. Placing patients in control of the privacy of their health information ensures that the risks for reputational and personal harm are reduced. Several approaches towards patient consent management solutions, ranging from software prototypes to conceptual models, have been adopted in response to the need for privacy preservation. The purpose of this paper is to review these approaches and to identify areas that still need to be addressed – particularly in terms of the automated enforcement of consent directives, interoperability, as well as standardised healthcare data exchange.

Keywords: E-consent · Privacy by design · Information security

1 Introduction

Health Information Systems (HISs) have enabled healthcare staff to have easier access to patient information, however, they have also introduced the risk that patient information may be accessed by unauthorised personnel and not for purposes originally intended by the patient [1]. For this reason, patients should be informed not only why their data is being collected, stored or processed, but also who is accessing their data [2]. Such a requirement needs to be enforced through consent policies and privacy-preserving laws such as the Protection of Personal Information (PoPI) Act that allow the patient to permit or deny the disclosure of particular medical information from particular personnel [1, 3, 4]. Patients can choose who may access their medical information such as their HIV/AIDS status, previous abortions, substance abuse, psychiatric illnesses and genetic predisposition to diseases [5–7]. Improper disclosure of such sensitive information can influence decisions about a patient's education, access to credit, or employment, and it may even expose the patient to reputational or personal harm [5, 8]. An HIS has the obligation to protect patient data in accordance with their individual consent boundaries [2] and when the effective enforcement of consent directives prevents undue disclosure of information, patients gain greater trust in electronic health record (EHR) systems [9]. In addition to ensuring the privacy of patient data, the procurement of informed consent reduces medical errors such as incorrect medical dosages and consequently reduces the number of medical malpractice claims [10].

H. Venter et al. (Eds.): ISSA 2018, CCIS 973, pp. 76–88, 2019.
https://doi.org/10.1007/978-3-030-11407-7_6

Besides permitting and prohibiting the collection, access, use and disclosure of private health information, three other forms of consent directives exist, namely medical treatment consent, research participation consent, and advance care consent. It is imperative that a patient's consent be unambiguous, informed and given freely [4, 11, 12] – furthermore, it must be as easy to revoke consent as it is to give it [11].

The introduction of a consent management platform affords a patient the opportunity to update his/her consent directives as necessary [3, 13]. The availability of such a mechanism also places patients in control of their information, as they can decide which information may be made available and to whom. Unauthorised access is thus prevented and accountable parties can easily be identified. The available literature suggests that the widespread use and acceptance of e-consent remains a challenge owing to the following reasons:

- There is still a lack of privacy and security measures [14] in HISs, specifically regarding the enforcement and safeguarding of patients' consent directives;
- E-consent systems hinder the ease with which health practitioners can perform their medical duties [2] as the system will prohibit unauthorized users from performing specific actions until they are given the appropriate access rights;
- The lack of an intuitive e-consent system makes it difficult for patients to manage their consent directives [1].

This paper provides a comprehensive review of the current state of e-consent systems in health information systems and identifies areas that still need to be addressed in the electronic patient consent management domain. In the following section, background concepts relevant to the literature referred to in this paper are provided. Section 3 details the research methodology that was followed to collect data for the study. Section 4 presents the findings of the survey. A discussion follows in Sect. 5 and the paper concludes in Sect. 6.

2 Background

This section provides some background on electronic consent, privacy and information security as these concepts facilitate privacy preservation in e-health systems.

2.1 Electronic Consent

It is important to discuss electronic consent, as it is the mechanism that allows patients to exercise the directives relating to their medical treatment and personal health information. Consent is considered informed when the patient is provided with sufficient information on the relevant processes, when adequate opportunity is given to the patient to consider alternative options, and when all the patient's questions are answered [15].

Consent may be given in three formats, namely written, verbal and implied [16]. The **written** consent format is where the patient signs a document to confirm that he/she has entered into an agreement for a high-risk treatment or procedure [16]. Written consent is further categorised into paper-based and electronic-based formats.

With the introduction of e-health, physical signatures are no longer compulsory, and electronic signatures or activities such as ticking a box are acceptable instead [17]. Electronic consent can also be realised through tele-consent where video media are used to facilitate the consent process. Even with the adoption of e-health, patients are still giving written consent primarily through signing physical documents [7, 10, 15]. However, the continued use of physical documents is not ideal as paper and printing costs are expensive [10]; physical documents make patient information difficult to store, search and retrieve [15]; and it is difficult to enforce access control for physical documents [7]. Furthermore, forms filled in by hand are often incomplete, inaccurate or illegible [18]. In contrast, an electronic consent management system is considered a more efficient and reliable approach [14].

Verbal consent occurs where oral confirmation is given for a low-risk treatment or procedure [16], whereas **implied** consent is given when the patient indicates agreement to a health practitioner's instructions (e.g. extending the arm to provide a routine blood sample for testing; taking or swallowing medication provided; attending an appointment for the purpose of receiving information or advice regarding management of the current condition) [16].

In e-health, consent implies that agreement is given for

- the collection, access, use or disclosure of information;
- medical treatment (agreement to undergo or reject specific medical treatments);
- participation in research; and
- advance care directives (e.g. Do Not Resuscitate orders).

Five directive options are available for e-consent: no consent; opt-in; opt-in with exceptions; opt-out; and opt-out with exceptions. An e-consent directive should also specify the subject of care, the grantee, the purpose and the time period covered by the consent [2]. Figure 1 illustrates the elements of an e-consent directive.

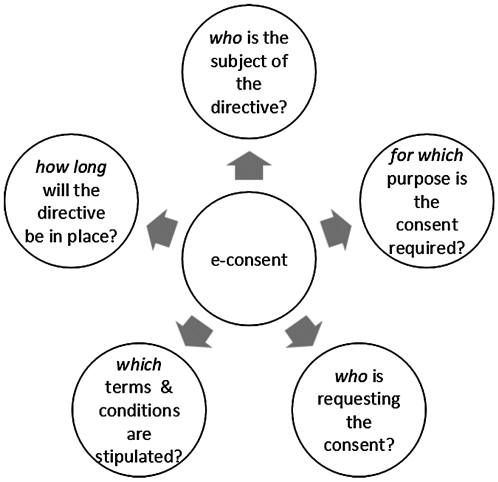

Fig. 1. e-Consent directive components [2]

The following section discusses the role of privacy and information security in e-consent.

2.2 Privacy and Information Security

Patients are the rightful owners of data that reside in HISs, and as such they may decline to disclose information that they feel may cause discrimination or stigma [19, 20]. In healthcare, the implications for practitioners who do not pay proper regard to the privacy of patients include sanctions from the Health Professions Council of South Africa, breach of privacy lawsuits, monetary penalty or even imprisonment [21]. The South African Protection of Personal Information (PoPI) Act recognises the right to privacy as stated in the Constitution and, as such, its purpose is to protect the processing of personal information by public and private bodies [21]. The PoPI Act is based on the best features of international privacy legislatures and it has given rise to eight information-processing principles. These PoPI principles [22] are summarised below:

1. Accountability: The responsible party must ensure that the eight information-processing principles are adhered to.
2. Processing limitation: Processing of information must be lawful and personal information may only be processed if it is adequate, relevant and not excessive for the purpose for which it is processed.
3. Purpose specification: Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.
4. Further-processing limitation: Sometimes personal information is received from a third party and must be passed on to the responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected.
5. Information quality: The responsible party must take reasonable and practical steps to ensure that the personal information is complete, accurate and not misleading. He/she must update the information where necessary, taking into account the purposes for which it was collected.
6. Openness: Personal information may only be processed by a responsible party that notified the Information Protection Regulator in advance. Furthermore, the responsible party must provide certain prescribed information to the data subject (the person/patient involved) by stating what information is collected, and whether or not the supply of the information by that data subject is voluntary or mandatory.
7. Security safeguards: The responsible party must secure the integrity of personal information in its possession or under its control by taking prescribed measures to prevent loss of, damage to, unauthorised destruction of, and unlawful access to or processing of personal data.
8. Data subject participation: A data subject has the right to request a responsible party to confirm, free of charge, whether the responsible party holds personal information about the data subject. The latter may also request from a responsible party the record or a description of the personal information held, including information

about the identity of all third parties (or categories of all third parties) who have (or have held) access to the information. In addition, a data subject may request a responsible party to

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading or obtained unlawfully;
(b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

When patient data are protected, patients gain greater trust in e-health systems and healthcare professionals [23–25]. Giving individuals control of their health information increases the quality and reliability of health data, which in turn reduces the occurrence of malpractice. When the quality and reliability of health research data is improved, the quality of healthcare is ultimately also enhanced [26].

An e-consent system or management platform needs to function beyond its responsibility to manage consent directives. It also needs to be supported by security functions that prevent unauthorised access to patient information [1]. A security layer ensures data integrity, data confidentiality, as well as nonrepudiation [1, 13]. Security approaches such as password protection, encryption, access control and audit trails can be used to monitor fraud and abuse, and to prevent unauthorised use and disclosure of data [24–26]. These approaches are essential, as insufficient data protection may subject a patient to embarrassment, social stigma and discrimination [23].

In the next section, the research methodology applied in the study is described.

3 Research Methodology

To provide an overview of the current state of electronic patient consent management, a literature review was conducted in the background section in which the information that is currently available on electronic patient consent management was examined and summarised. The information sources that were eligible, were papers that dealt with electronic consent in the e-health context. The specific criteria that were used to find eligible sources are discussed in the subsequent sections.

3.1 Search Criteria

Electronic journal databases such ACM Digital Library, IEEE Xplore Digital Library, PubMed Central, ScienceDirect and Springer Link were accessed during the period December 2017 to March 2018. Search terms including “patient consent management”, “e-consent”, “electronic consent”, “e-health”, “privacy” and “security” were applied. Boolean connectors such as AND and OR were used on the selected keywords in order to obtain more comprehensive search results. Altogether 33 papers met the required criteria and were used as literature sources for this paper.

3.2 Evaluation Criteria

The sources were subsequently evaluated against the concepts below:

- *Architectures, frameworks and standards* – whether the literature considered standards such as HL7, Basic Patient Privacy Consents (BBPC) or Clinical Document Architecture (CDA), because they help facilitate interoperability in health information systems. There is currently a lack of standards or guidelines on how e-consent systems can be implemented best [17].
- *Information security measures* – whether the literature considered information security approaches that value and ensure the privacy of patients' health information and maintain the confidentiality, integrity and availability of patient health information.
- *Patient directive management* – how patients are given control over their directives through settings that facilitate revocation, creation and modification.
- *Patient understanding* – whether the literature explains how the e-consent process will ensure that the patient is provided with sufficient information to ensure that the consent given is informed.
- *Policies or regulations* – whether the literature mentions the use of regulations that will guide the design of e-consent systems, as consent directives should be in line with the health institution's policies as well as privacy laws.

The above evaluation criteria are essentially design focused, and therefore the discussion in the authors' analysis will be divided into patient-centered design and privacy by design. Patient-centered design is aimed at asserting whether the design of a presented system had a patient's needs in. Privacy by design focuses on the use of secure and confidentiality-driven approaches that are adopted when systems that contain or use personal user information are implemented. A complete analysis follows in Sects. 4 and 5.

4 Findings

This section presents a concept matrix as well as figures that illustrate observations made from the selected literature sources.

Table 1 presents a comparison of topics that constituted the focus of the selected literature in the health e-consent domain. These focus areas are the same as the evaluation criteria specified in the previous section. From the concept matrix in Table 1, it is evident that even though several journal papers covered some of the focus areas, there is a lack of research that covers all of the concepts specified in the evaluation criteria.

Only 7 papers discussed the use of any standards or frameworks that should be used during the design of e-consent systems. Around 60% of the papers highlighted the importance of using security approaches that value and ensure the privacy of patients' health information and maintain the confidentiality, integrity and availability of patient health information. Only 2 papers mentioned how directives should be accessible and

Table 1. Concept matrix for electronic patient consent management

Paper(s)	Standard/framework	Information security	Directive management	Patient understanding	Policy/regulation
[26]		✓		✓	✓
[27]		✓			✓
[28]		✓		✓	
[1, 5, 7, 8, 30–32]		✓			
[2, 33]	✓	✓			
[4, 34]	✓				
[35]			✓	✓	
[36]		✓	✓		✓
[18, 37–40]					
[15, 25, 41, 42]				✓	✓
[10, 43, 44]	✓	✓		✓	
[45]					✓

manageable by patients within an e-consent system. The importance of patient understanding and policy regulation were discussed in 10 and 8 papers respectively.

A complete e-consent management system should implement all of these concepts as the application of information security techniques and regulations are essential for the pursuit of privacy preservation.

Figure 2 illustrates the components that encompass consent in healthcare. Four components of consent in healthcare were prominent, namely directive formats, types, attributes and options.

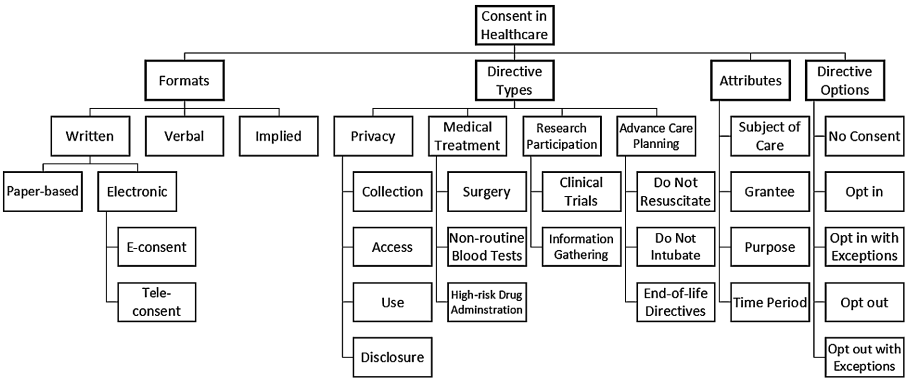

Fig. 2. Healthcare consent components

The directive options align with the need for patients to have the mechanism to manage their directives. The options should include no consent; opt-in; opt-in with exceptions; opt-out; and opt-out with exceptions.

The directive types that directly relate to information security are the privacy and research participation directives and it is also important for the appropriate privacy preserving policies and regulations to be applied.

A discussion of the foundational aspects of e-consent follows in Sect. 5.

5 Discussion

An e-consent system should have patient centricity as well as privacy centricity as its foundation; consequently, this section focuses on patient requirements and privacy by design in the e-health context.

5.1 Patient-Centred Design

The literature review found that comprehension, control and confidentiality are the main expectations that patients have when using e-consent systems.

Comprehension. Consent is informed when a patient had a conversation with a health practitioner during which the alternatives, advantages and disadvantages of a process were thoroughly discussed [17, 18] until the patient understood the situation and was able to assess the risks fully [45]. If a surgeon, for instance, does not obtain informed consent prior to a procedure, the patient may afterwards accuse him/her of battery or negligence. This is significant as most negligence claims are a result of patients not fully understanding the possible complications of a procedure [18].

One of the difficulties faced by patients during the consent process is the fact that they are unable to understand the policies or terms and conditions involved, often because of the lengthy and complex language used [17, 29, 46]. A study that explored user behaviours when providing electronic consent on health social networks showed that 73% of people did not carefully read the terms and conditions, and only 17% understood the contents [46]. Long and complex policies should be replaced with brief and lucid communications to help patients understand better. Additionally, multimedia can be employed to help enhance comprehension, particularly for children [29]. The use of multi-language support, additional educational resources, as well as quizzing mechanisms will increase the level of understanding and individuals will be in a better position to control their healthcare directives.

Control. Healthcare users have expressed the need for greater control over their consent directives [17]. This can be accomplished by adopting an individualised and transparent approach for each patient. Consent forms should be tailored for each patient [18] so that each component of the form is non-generic, relevant and complete. The patient should be able to express any of the consent directives, such as “no consent”, “opt-in”, “opt-in with exceptions”, “opt-out” or “opt-out with exceptions” – as illustrated in Fig. 2. This freedom is similar to social media privacy control settings and, coupled with transparency and usability, autonomy is given to the patient.

Confidentiality. Concern about security and privacy issues in e-health has persisted ever since the first IoT botnet attack in 2013 [17]. A botnet attack can be used for denial-of-service attacks, for the collection of user information, or for stealthy user monitoring. Besides botnets, cookies are also a threat because even though they facilitate the functions of targeted advertising or keep login sessions alive, they were designed without proper consideration for information security [46]. Therefore, it is important to build systems that will take information security into account. For European citizens, the General Data Protection Regulation (GDPR), which comes into effect as from May 2018, will require from data controllers and processors to ensure security [17]. Non-adherence to the GDPR may lead to financial penalties [17]. In view of the GDPR, the Privacy-by-Design approach has been highlighted to facilitate security and privacy. The following section presents a discussion on Privacy by Design.

Table 2 illustrates the requirements as considered from the perspective of patients and healthcare practitioners.

Table 2. Technical and non-technical requirements for electronic consent management

Requirements		
Patient non-technical requirements	Health practitioner non-technical requirements	Technical requirements
Intuitive	Intuitive	Automated
Multi-lingual support	Workflow-friendly	Interoperable
Transparent		Secure
Informative		Auditable

5.2 Privacy by Design

Privacy by Design (PbD) is a concept developed to promote privacy and data protection in information technology and communication systems. Table 3 draws a comparison between the PbD principles and the PoPI principles. The principles for PbD [17, 47] are described as follows:

Table 3. Technical and non-technical requirements for electronic consent management

Privacy by design principle	PoPI principle and patient/system requirement
Proactive, not reactive	PoPI (7), automation, auditing
Privacy as default setting	PoPI (1)–(4)
Privacy embedded into design	PoPI (7)
Full functionality	Modifiable directive settings (control), notifications
End-to-end security	PoPI (7), confidentiality, auditing
Visibility and transparency	PoPI (1), (6), (8), clear intentions (comprehension)
Respect for user privacy	PoPI (5), (8), confidentiality

- *Proactive, not reactive*: PbD should anticipate privacy risks and prevent them from materialising.
- *Privacy as the default setting*: Personal data should automatically be protected by default with no added action required from the user.
- *Privacy embedded into design*: Privacy measures should be embedded into the architecture and design of information technology systems as the integral component.
- *Full functionality*: PbD should ensure that even though privacy is the core objective, it does not impair other functionalities of the system.
- *End-to-end security*: Privacy should be continuously enforced across the entire lifecycle of the data. Without strong security, privacy cannot be realised.
- *Visibility and transparency*: All stakeholders should operate according to the stated promises.
- *Respect for user privacy*: A user-centric approach should be undertaken so that users can control their data. This involves requesting consent from the user and ensuring that the users have access to activities surrounding their information.

6 Conclusion

Health information systems enable the collection and use of electronic health data, which in turn provides benefits to various stakeholders [23, 24, 26, 46]. In most cases, the electronic health data found in medical systems is patient data. With their data being exchanged electronically, patients still need a means to give consent about who should and who should not access their data. This requires an electronic consent management mechanism. With proper consent management in place, medical researchers can conduct their work more efficiently as there is increased access to accurate information:

– researchers can also use available data to investigate how high-quality and cost-effective healthcare may be provided;
– the quality of clinical care is improved as immediate access to information enables quick and informed decision making regarding diagnoses and treatments for healthcare service providers;
– patients can benefit by making informed decisions about service providers, medical treatments and health conditions in general.

The purpose of this paper was to provide a literature review on the current state of electronic consent management in healthcare. It showed that implementing an e-consent management system, even with the identified shortcomings, should be consideration for future research work. A survey should also be conducted to obtain the opinions of South African health practitioners and administrators on electronic consent management.

References

1. Coiera, E., Clarke, R.: e-Consent: the design and implementation of consumer consent mechanisms in an electronic environment. J. Am. Med. Inform. Assoc. **11**(2), 129–140 (2004)
2. Can, O.: A semantic model for personal consent management. In: Garoufallou, E., Greenberg, J. (eds.) MTSR 2013. CCIS, vol. 390, pp. 146–151. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03437-9_15
3. Bursa, O., Sezer, E., Can, O., Unalir, M.O.: Using FOAF for interoperable and privacy protected healthcare information systems. In: Closs, S., Studer, R., Garoufallou, E., Sicilia, M.-A. (eds.) MTSR 2014. CCIS, vol. 478, pp. 154–161. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13674-5_15
4. Heinze, O., Birkle, M., Köster, L., Bergh, B.: Architecture of a consent management suite and integration into IHE-based regional health information networks. BMC Med. Inform. Decis. Making **11**(1), 58 (2011)
5. Gaba, A., Havinga, Y., Meijer, H.J., Jan, E.: Privacy and security for analytics on healthcare data (2014)
6. Rindfleisch, T.C.: Privacy, information technology, and health care. Commun. ACM **40**(8), 92–100 (1997)
7. Eskeland, S., Oleshchuk, V.A.: EPR access authorization of medical teams based on patient consent. In: ECEH, pp. 11–22 (2007)
8. Russello, G., Dong, C., Dulay, N.: Consent-based workflows for healthcare management. In: IEEE Workshop on Policies for Distributed Systems and Networks, POLICY 2008, pp. 153–161. IEEE (2008)
9. Hu, L.L., Sparenborg, S., Tai, B.: Privacy protection for patients with substance use problems. Subst. Abuse Rehabil. **2**, 227 (2011)
10. Yu, B., Wijesekera, D., Costa, P.C.G.: Informed consent in electronic medical record systems. In: Healthcare Ethics and Training: Concepts, Methodologies, Tools, and Applications, pp. 1029–1049. IGI Global (2017)
11. Mense, E., Blobel, B., et al.: Hl7 standards and components to support implementation of the European General Data Protection Regulation (GDPR). Eur. J. Biomed. Inform. **13**(1), 27–33 (2017)
12. Abbas, R.M., Carroll, N., Richardson, I., Beecham, S.: The need for trustworthiness models in healthcare software solutions. In: HEALTHINF, pp. 451–456 (2017)
13. Moss, L., Shaw, M., Piper, I., Hawthorne, C., Kinsella, J.: Sharing of big data in healthcare: public opinion, trust, and privacy considerations for health informatics researchers. In: HEALTHINF, pp. 463–468 (2017)
14. Elkhodr, M., Shahrestani, S., Cheung, H.: Preserving the privacy of patient records in health monitoring systems. In: Theory and Practice of Cryptography Solutions for Secure Information Systems, pp. 499–529. IGI Global (2013)
15. Madathil, K.C., et al.: An investigation of the efficacy of electronic consenting interfaces of research permissions management system in a hospital setting. Int. J. Med. Inform. **82**(9), 854–863 (2013)
16. ACT Health: Informed consent. http://www.health.act.gov.au/publicinformation/consumers/informed-consent. Accessed 22 Mar 2018
17. O'Connor, Y., Rowan, W., Lynch, L., Heavin, C.: Privacy by design: Informed consent and internet of things for smart health. Procedia Comput. Sci. **113**, 653–658 (2017)

18. St John, E., Scott, A., Irvine, T., Pakzad, F., Leff, D., Layer, G.: Completion of hand-written surgical consent forms is frequently suboptimal and could be improved by using electronically generated, procedure-specific forms. Surgeon **15**(4), 190–195 (2017)
19. Ghazvini, A., Shukur, Z.: Security challenges and success factors of electronic healthcare system. Procedia Technol. **11**, 212–219 (2013)
20. Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A.: Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. **46**(3), 541–562 (2013)
21. Buys, M.: Protecting personal information: implications of the protection of personal information (PoPI) act for healthcare professionals. SAMJ: South Afr. Med. J. **107**(11), 954–956 (2017)
22. Ramdhin, A.: Protection of personal information bill: what should you be asking? https://www.werksmans.com/legal-briefs-view/protection-ofpersonal-information-bill-what-should-you-be-asking/. Accessed 01 Mar 2018
23. Gostin, L.O.: National health information privacy: regulations under the Health Insurance portability and accountability act. JAMA **285**(23), 3015–3021 (2001)
24. McGraw, D.: Privacy and health information technology: executive summary. J. Law Med. Ethics **37**(2 suppl), 121–149 (2009)
25. Wang, L.: The privacy rule: HIPAA standards for the privacy of individually identifiable health information. Empl. Benefits J. **27**(3), 59–63 (2002)
26. Hodge Jr., J.G., Gostin, L.O., Jacobson, P.D.: Legal issues concerning electronic health information: privacy, quality, and liability. JAMA **282**(15), 1466–1471 (1999)
27. Antal, H., Bunnell, H.T., McCahan, S.M., Pennington, C., Wysocki, T., Blake, K.V.: A cognitive approach for design of a multimedia informed consent video and website in pediatric research. J. Biomed. Inform. **66**, 248–258 (2017)
28. Asghar, M.R., Russello, G.: Actors: a goal-driven approach for capturing and managing consent in e-health systems. In: IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), pp. 61–69. IEEE (2012)
29. Blake, K., et al.: Use of mobile devices and the internet for multimedia informed consent delivery and data entry in a pediatric asthma trial: Study design and rationale. Contemp. Clin. Trials **42**, 105–118 (2015)
30. Chávez, E., Finnie, G.: Empowering data sources to manage clinical data. In: 2010 IEEE 23rd International Symposium on Computer-Based Medical Systems (CBMS), pp. 203–208. IEEE (2010)
31. Ge, Y., Ahn, D.K., Unde, B., Gage, H.D., Carr, J.J.: Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. J. Am. Med. Inform. Assoc. **20**(1), 157–163 (2013)
32. Bergmann, J., Bott, O.J., Pretschner, D.P., Haux, R.: An e-consent-based shared EHR system architecture for integrated healthcare networks. Int. J. Med. Inform. **76**(2), 130–136 (2007)
33. Khan, A., McKillop, I.: Privacy-centric access control for distributed heterogeneous medical information systems. In: 2013 IEEE International Conference on Healthcare Informatics (ICHI), pp. 297–306. IEEE (2013)
34. Ko, Y.Y., Liou, D.M.: The study of managing the personal consent in the electronic healthcare environment. World Acad. Sci. Eng. Technol. **65**, 314 (2010)
35. Kondylakis, H., et al.: IEmS: a collaborative environment for patient empowerment. In: 2012 IEEE 12th International Conference on Bioinformatics and Bioengineering (BIBE), pp. 535–540. IEEE (2012)
36. Kondylakis, H., et al.: Donors support tool: Enabling informed secondary use of patients' biomaterial and personal data. Int. J. Med. Inform. **97**, 282–292 (2017)

37. Sonne, S.C., et al.: Development and pilot testing of a video-assisted informed consent process. Contemp. Clin. Trials **36**(1), 25–31 (2013)
38. Nwomeh, B.C., Hayes, J., Caniano, D.A., Upperman, J.S., Kelleher, K.J.: A parental educational intervention to facilitate informed consent for emergency operations in children. J. Surg. Res. **152**(2), 258–263 (2009)
39. Li, Y., Xie, M., Bian, J.: USign—a security enhanced electronic consent model. In: 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 4487–4490. IEEE (2014)
40. Lentz, J., Kennett, M., Perlmutter, J., Forrest, A.: Paving the way to a more effective informed consent process: recommendations from the clinical trials transformation initiative. Contemp. Clin. Trials **49**, 65–69 (2016)
41. Warriner, A., et al.: A pragmatic randomized trial comparing tablet computer informed consent to traditional paper-based methods for an osteoporosis study. Contemp. Clin. Trials Commun. **3**, 32–38 (2016)
42. Whiddett, R., Hunter, I., Engelbrecht, J., Handy, J.: Patients attitudes towards sharing their health information. Int. J. Med. Inform. **75**(7), 530–541 (2006)
43. Yu, B., Wijesekera, D., Costa, P.C.: An ontology for medical treatment consent. In: STIDS, pp. 72–79 (2014)
44. Pruski, C.: e-CRL: a rule-based language for expressing patient electronic consent. In: Second International Conference on eHealth, Telemedicine, and Social Medicine, 2010, ETELEMED 2010, pp. 141–146. IEEE (2010)
45. Yu, B., Wijesekera, D., Costa, P.: Consent-based workflow control in EMRs. Procedia Technol. **16**, 1434–1445 (2014)
46. Rowan, W., O'Connor, Y., Lynch, L., Heavin, C.: Exploring user behaviours when providing electronic consent on health social networks: a just tick agree approach. Procedia Comput. Sci. **121**, 968–975 (2017)
47. Cavoukian, A.: Privacy by Design. Take the Challenge. Information and Privacy Commissioner of Ontario, Toronto (2009)