Journal of Diabetes Science and Technology
Volume 5, Issue 3, May 2011
© Diabetes Technology Society

REVIEW ARTICLE

Telemedicine Security: A Systematic Review

Vaibhav Garg, M.S.,[1] and Jeffrey Brewer, M.S.[2]

Abstract

Telemedicine is a technology-based alternative to traditional health care delivery. However, poor security measures in telemedicine services can have an adverse impact on the quality of care provided, regardless of the chronic condition being studied. We undertook a systematic review of 58 journal articles pertaining to telemedicine security. These articles were selected based on a keyword search on 14 relevant journals. The articles were coded to evaluate the methodology and to identify the key areas of research in security that are being reviewed. Seventy-six percent of the articles defined the security problem they were addressing, and only 47% formulated a research question pertaining to security. Sixty-one percent proposed a solution, and 20% of these tested the security solutions that they proposed. Prior research indicates inadequate reporting of methodology in telemedicine research. We found that to be true for security research as well. We also identified other issues such as using outdated security standards.

J Diabetes Sci Technol 2011;5(3):768-777

Introduction

Traditional health care services for the treatment of chronic conditions are expensive.[1] The cost of diabetes care alone is estimated at $132 billion annually, $92 billion of this in the United States.[2] Telemedicine services for diabetes are an effort to lower cost and improve quality of care.

Telemedicine, though promising in trial stages, has been less successful in real life.[3,4] Reporting of research methodology used in the trials has been inadequate,[5] which makes it difficult to analyze the gap between real life and trial stages.[6] Security has also been identified as a determinant for successful telemedicine implementations.[7] Thus, in this article, we look at the research done in the field of telemedicine security. In particular, we address the reporting of methodology in telemedicine security research. The articles reviewed include several different chronic diseases, including diabetes. The research does not break out diabetes separately, as the issues in security discovered apply across all studies.

Telemedicine security includes problems such as authorization, authentication, and accounting[8] that are common with other information technology applications such as banking and manufacturing support. There are, however, many new challenges as well. Telemedicine requires information security and privacy as well as

Author Affiliations: [1]School of Informatics and Computing, Indiana University, Bloomington, Indiana; and [2]Department of Computer and Information Technology, Purdue University, West Lafayette, Indiana

Abbreviations: (HIPAA) Health Insurance Portability and Accountability Act, (HL7) Health Level Seven

Keywords: diabetes, privacy, safety, security, telecare, telemedicine

Corresponding Author: Vaibhav Garg, M.S., School of Informatics and Computing, Indiana University, Bloomington, 901 E. 10th St., Room 202, Bloomington, IN 47408; email address gargv@indiana.edu

physical safety. Physical safety, for example, detection of falls in older adults, has to be evaluated remotely. The patient should be able to trust the system and not feel that human contact in terms of an onsite caregiver is needed. Thus reliability is an important concern. Fischhoff and colleagues[9] noted, "Acceptable risk for a new technology is defined as that level of safety associated with ongoing activities having similar benefits to society." Thus telemedicine systems should also be evaluated for perceptions of both patients and caregivers since they may be perceived as intrusive and ineffective.[10]

According to Broens and associates,[7] both patient physical safety and patient information security are crucial to support the trust relationship between health care providers and patients and for acceptance of telemedicine implementations. Savastano and coworkers[10] note that lack of patient trust means that patients would not reveal accurate and complete information, which lowers the quality of care. This is a critical consideration because a big part of the treatment of diabetes patients is in the accurate self-reporting of blood glucose levels. Poor quality of care would further reduce the confidence of both providers and consumers of telemedicine services. Lack of confidence would make it less likely for these services to be deployed widely.

Earlier research[11] suggests that security is not the primary focus of the telemedicine research community. But this needs to change if telemedicine is to become widely acceptable.[7] Several articles[10,12] have suggested that poor security may lead to lesser quality of care and lack of confidence in the services for both providers and consumers and cause legal liability. These are unique challenges, separate from other forms of health-care-technology-related initiatives such as electronic medical record systems that need to be identified. Not addressing these issues in telemedicine services not only lowers the quality of care but may also have fatal consequences.[13]

Thus, in this review, we consider the following research questions:

1. What methodological details are commonly reported in telemedicine research?
2. What security problems are specifically targeted?
3. What security problems have not been adequately addressed in the literature?
4. What are the criteria for reliability, or how accurately and widely are the proposed solutions tested?

Methods

The framing of this research is based on Whitten and colleagues[5] who conducted a systematic review of methodology in telemedicine research. We modified their approach to incorporate the research questions outlined earlier as pertaining to security. A keyword search was done on 14 journals. These journals were selected because they were focused primarily on telemedicine research from a caregiver's perspective. All 14 journals were searched through PubMed. In all, 66 articles were found. Eight articles, found with the search phrase "telemedicine and safety," were excluded because they dealt with nontechnology-based safety issues. The dates of publication were between 1994 and 2009.

We did a keyword search on the following journals:

1. *Journal of Telemedicine and Telecare*
2. *Journal of the American Medical Informatics Association*
3. *Journal of Nursing Management*
4. *International Journal of Medical Informatics*
5. *International Journal of Telemedicine and Applications*
6. *Health and Social Care in Community*
7. *Computer Methods in Biomedicine*
8. *Quality Assurance and Devices in Telemedicine*
9. *Medical Journal of Australia*
10. *EBMS Annual International Conference*
11. *Informatics for Health and Social Care*
12. *Telemedicine Journal and e-Health*
13. *Telemedicine Today*
14. *Studies in Health Technology and Informatics*

The following keywords were used:

1. Telemedicine and security
2. Telemedicine and safety
3. Telemedicine and privacy

4. Telecare and security

5. Telecare and safety

6. Telecare and privacy

We modified the coding scheme used by Whitten and colleagues[5] to answer the specific research questions pertaining to telemedicine security. The modified coding scheme is given here:

1. Research questions

2. Security questions

3. Type of security questions, e.g., privacy, physical safety

4. Threat model

5. Metrics (yes/no). If yes, what metrics?

6. Significance of problem

7. Solution proposed

8. Solution tested (yes/no). If yes, what were the results?

9. Limitation of the solution

Results

We found 58 articles in 14 journals (see **Appendix**; assuming no constraint on the date of publication). These articles were coded according to the scheme given in the previous section. On average, these journals publish less than 1 article per year on security. **Figure 1** gives a distribution of the number of articles for each journal.

Six of the articles were quantitative, 13 were qualitative, and the remaining articles were theoretical. Reporting of methodology in quantitative and qualitative articles was inadequate. Fifteen percent of the articles did not report population size. Fifty percent of the articles did not report age range. Eighty percent of the articles did not represent the age mean or median.

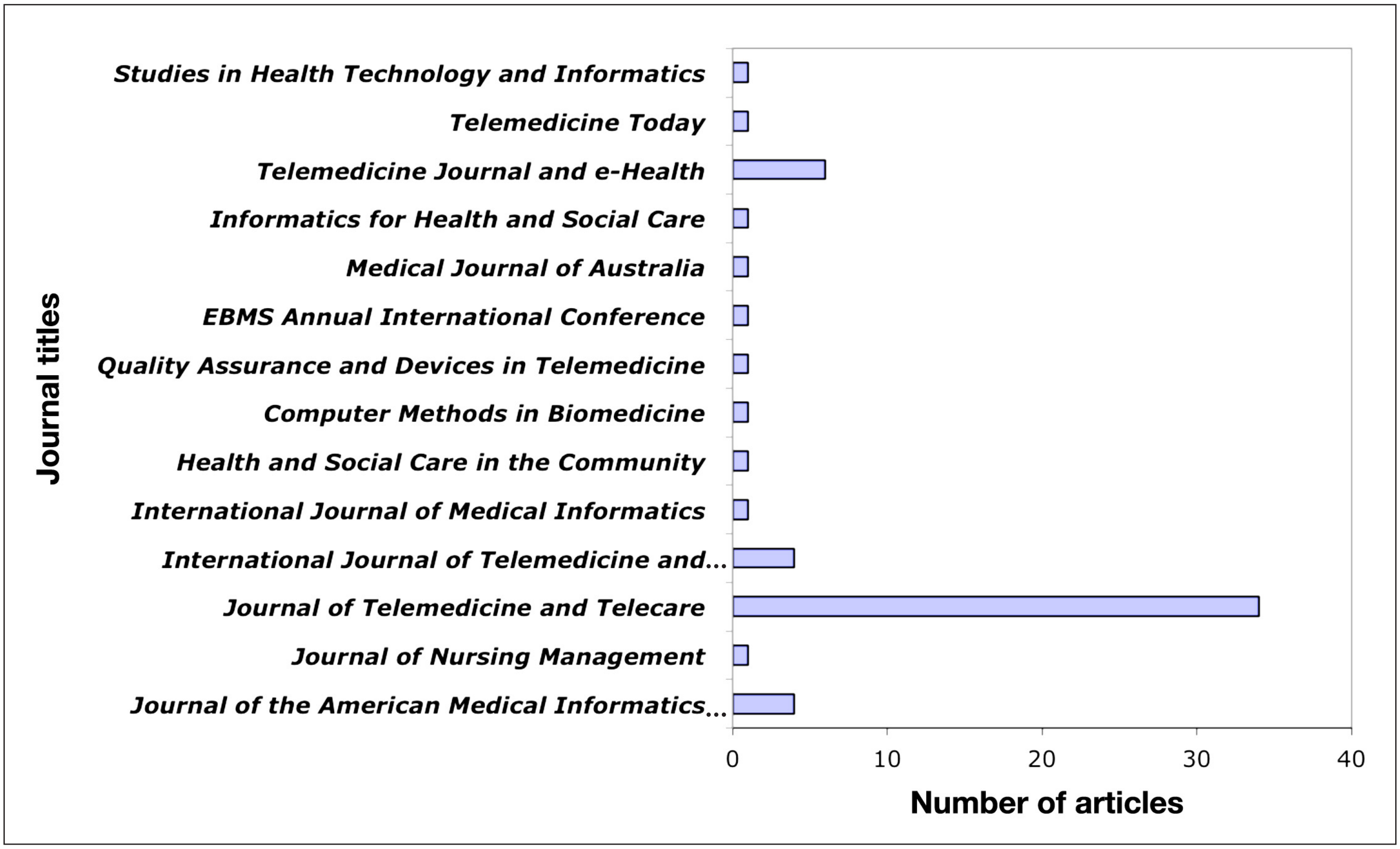

Figure 1. Distribution of articles over journals.

Figure 2 gives a distribution of articles by country. Europe accounts for almost half of the security research. While 20 of the articles were based in the United States, only 6 mentioned the Health Insurance Portability and Accountability Act (HIPAA).

Seventy-six percent of the articles defined a security problem, and only 47% formulated a research question specific to security. Of these, 61% proposed a solution. Only 20% of these tested their solutions. None of the articles specifically tested for security. Ninety-three percent of the articles did not have a threat model. Different articles dealt with different security issues. **Figure 3** shows a distribution of articles by security topics. Privacy and data integrity were most represented, but privacy is hard to maintain without addressing authentication and authorization (represented by merely nine and five articles, respectively).

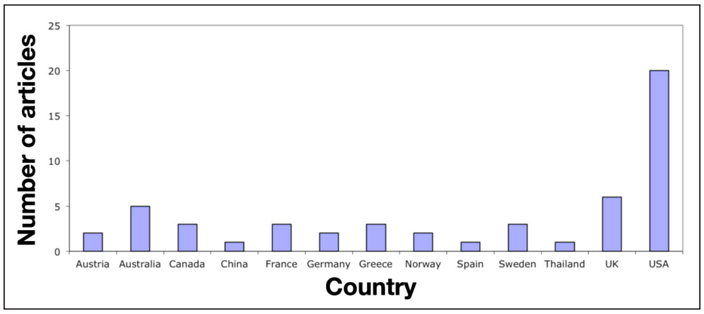

Figure 2. Distribution of articles across countries.

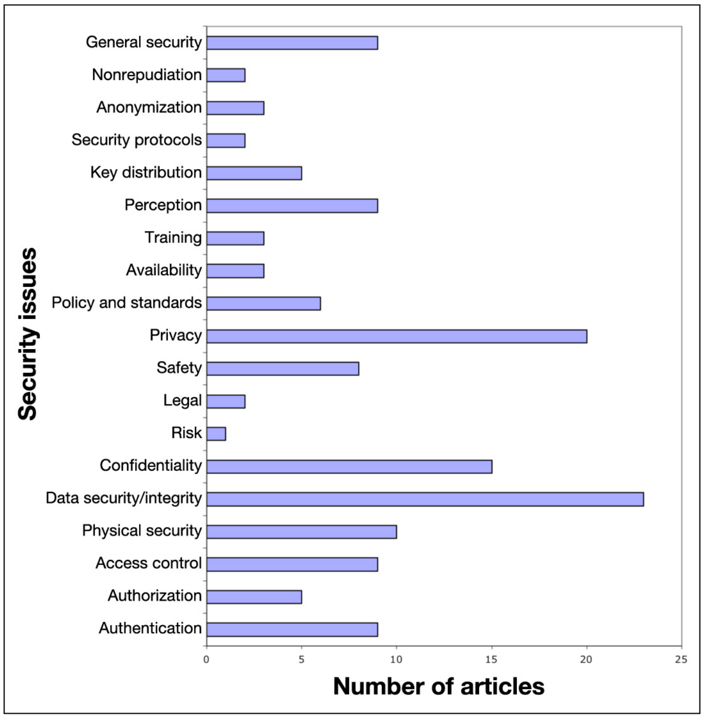

Figure 3. Distribution across security issues.

Figure 4 shows the distribution of articles over the types of consumers. Most papers addressed older adults and diabetes patients. For both these groups, security can be very important. For example, in the cases of the elderly, timely intervention in the event of a fall is important[14]. Older adults also suffer from an increasing occurrence of Alzheimer disease.[15] Thus they should not be made to wear devices that make them stand out, or they might become targets of crime (see *http://www.quackwatch.org/01quackeryrelatedtopics/hearing/fbi.html*).

The number of publications pertaining to security in telemedicine is very low compared to the overall number of publications in telemedicine. **Figure 5** shows the distribution of articles over years. The graph is left skewed, which suggests that the number of security-related publications has increased, but that might be due to an increase in the overall number of telemedicine publications.

Discussion

Missing Subject Data

Many qualitative and quantitative papers did not report population characteristics such as age range and average. This seems to be an important oversight because age is an important factor in the adoption of telemedicine

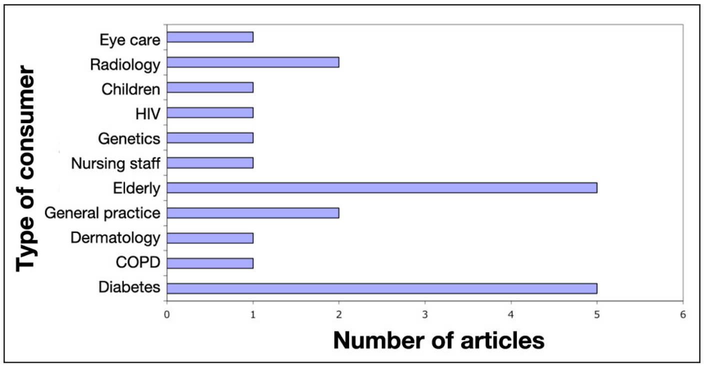

Figure 4. Distribution across consumers.

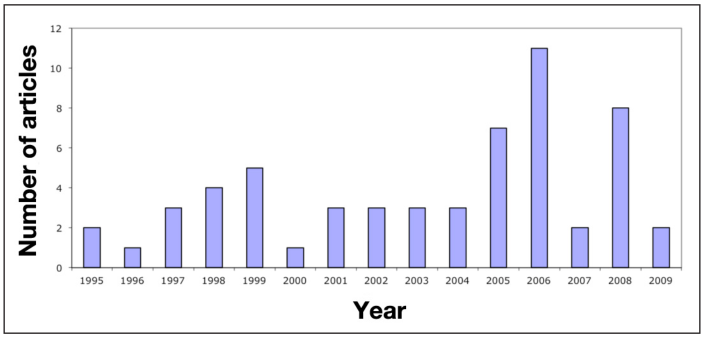

Figure 5. Distribution of articles across years.

services, as older adults are less likely to accept new technology than their younger cohorts.[16]

Many articles did not report the kind of users that they were catering to. This is important because security solutions cannot always be generalized. Different systems will have a different threat model. For example, physical safety is important for the elderly, but for individuals suffering from HIV/AIDS, privacy may be a bigger concern. No security solution can be all-encompassing, protecting the system against everything. The articles need to report a threat model so that the reader would know what the solution is going to protect against (see *http://insecure.org/stf/whycrypto.html*).

Merely three articles address training of personnel. This is an important area that needs to be addressed. One of the drawbacks of traditional care is negligence by caregivers; it is bound to happen in telemedicine as well unless the caregivers are trained well. Not only the caregivers need to be trained, but also the patients and other personnel who interact with the system directly or indirectly. Most systems are vulnerable because the users do not use them correctly. Training also prevents other attacks like social engineering.[17]

Legalities, Policies, and Standards

Only two articles addressed the legal issues, and five articles addressed policies and standards. Legislation and policy has been identified as one of the five determinants for successful telemedicine implementation.[7] Legal issues in telemedicine are very different from legal issues in traditional caregiving, especially when it comes to legal liability. Disclosure of sensitive data can be a big problem for caregivers. Stanberry[18] notes that, other than information leakage, interception and modification of telemedicine transmissions leading to inaccurate or incomplete data can have catastrophic consequences for patient care. Network-related issues such as packet dropping and jitter could also lower the quality of medical data being transmitted, leading to further liability. The only two papers[18,19] that discuss legal liability were published in 1998 and 1999 and were conducted in United Kingdom. This needs to be addressed further because legal liability can often be a big hurdle in the adoption of a new technology.

Legal liability can be avoided by providing policies and standards for health care providers to observe. However, only five articles addressed policy and standards. Most articles did not talk about HIPAA or Health Level Seven (HL7) compliance. Policy and standards help in building confidence among the consumers and providers regarding the reliability and safety of the service. Savastano and coworkers[10] note that certain biometric sensors might be seen to cause infections, in the case of touch-based sensors, or can be seen to cause safety concerns when the biometric technology requires the emission of infrared light as is the case with iris recognition. Standardization would reduce the fear of using these technologies. Certain other technologies like radio-frequency identification might raise privacy concerns. If a well-established standard is used, it may alleviate worries. Standardization also implies that device developers would repeatedly implement the same framework. This allows researchers to borrow from previous implementations and improve on them. Yellowlees and Harry[20] also talk about standards, but their focus is on how standardization helps in quicker dissemination of technology. Alexander[21] talks about developing a nationwide privacy policy for health care data in Australia. None of the papers talks about HL7, even though three of the studies have been conducted in the United States and the United Kingdom, where HL7 is the standard for storing medical data.

However, no standards are better than bad standards. Makris and associates[22] use Data Encryption Standard for encryption. This paper was published in 1997. However, the algorithm was already broken in 1993.[22] Makris and associates[22] also describe two authentication protocols. They do not provide a proof of security for either of the protocols. Neither of the protocols is referenced, so it can be assumed that the authors constructed both protocols themselves. However, designing security protocols can be a tricky task. While protocols can be checked for attacks, using either logic-based proofs or automated modeling tools, security is not guaranteed. For example, the Needham–Schroeder protocol was proven insecure more than a decade after its publication even though the protocol had been proven secure using Burrows–Abadi–Needham logic.[23,24] The researchers used an insecure algorithm for encryption and unproven security protocols for communication. This would be a concern because an insecure system can reveal private data and lead to various attacks, some even fatal.[13]

Another area that seems to be neglected is research on availability. Only three papers discuss availability.[10,25,26] None of the papers discuss the importance of availability, the implications, or lack of it. They do not mention any measures that can be used to ensure availability. This is an important issue because it is a necessary condition for reliability of the service, especially for patients with type 1 diabetes who need to frequently monitor and report glucose levels for proper insulin therapy and lifestyle changes.

Another important property is nonrepudiation. It implies that a person cannot deny responsibility for a certain transaction. This is important to maintain audit trails because a person implicated by an audit should not be able to repudiate responsibility. Only two papers mention this property.[22,27] Ferrante[27] states that nonrepudiation is necessary to comply with HIPAA and thus needs to be addressed by all telemedicine systems targeted toward the United States.

Conclusion

There is a dearth of standardization in telemedicine security across all chronic illnesses under study. It also appears that many telemedicine researchers are unfamiliar with the field of security in general. There were instances of use of poor encryption standards. In some articles, authors designed their own protocols for communication without giving any proof of security, formal or otherwise. Many of these systems would have to comply with HIPAA and HL7. However, there is no discussion of how those requirements are being met. There is also insufficient reporting of methodological details that severely limits the inferences one can draw from the articles. The same system may provide good results for older adults but fail for cognitively challenged adults. Most of the articles did not try to solve the security problems they faced. The few articles that provided solutions neither formally proved them nor tested them. Most articles failed to mention the security guarantees their system would provide and did not present a threat model.

While several security challenges in telemedicine are common to all information-technology-based systems, there are unique questions that need further attention. Reliability and availability is a key issue, as many of these systems might be critical life-supporting systems. It is also important to maintain the usability of these systems without compromising the security. Usability among other factors would drive adoption. This means that these systems cannot be developed in isolation and must be developed in conjunction with the organizations they target to ensure success.[28]

Challenges in diabetes technology are similar to other telemedicine services. There is a need for data confidentiality during both transmission and retention. Data integrity is also a key concern to ensure correct diagnosis and quality of care. There is a need to define standards for minimum requirements. Researchers need to address these security concerns in order to increase the dissemination of telemedicine services and to improve the quality of care provided. Also, both in terms of reporting and design, the quality of security research should be improved. One recommendation would be for researchers to collaborate with researchers in security and associated fields who may have a better understanding of technology. It is also recommended to review literature in information security, especially network security and cryptography.

Acknowledgments:

We thank Prof. Eugene Spafford, Prof. Victor Raskin, and Prof. Teresa Doughty who helped with the Master's thesis on which this article is based. We also thank Prof. Sheba M. George who took time to provide valuable insights.

References:

1. Huang ES, Basu A, O'Grady M, Capretta JC. Projecting the future diabetes population size and related costs for the US. Diabetes Care. 2009;32(12):2225–9.
2. Hogan P, Dall T, Nikolov P; American Diabetes Association. Economic costs of diabetes in the US in 2002. Diabetes Care. 2003;26(3):917–32.
3. Berg M. Patient care information systems and health care work: a sociotechnical approach. Int J Med Inform. 1999;55(2):87–101.
4. Tanriverdi H, Iacono CS. Diffusion of telemedicine: a knowledge barrier perspective. Telemed J. 1999;5(3):223–44.
5. Whitten P, Johannessen LK, Soerensen T, Gammon D, Mackert M. A systematic review of research methodology in telemedicine studies. J Telemed Telecare. 2007;13(5):230–5.
6. Whetton S. Success and failures: what are we measuring? J Telemed Telecare. 2005;11 Suppl 2:S98–100.
7. Broens TH, Huis in't Veld RM, Vollenbroek-Hutten MM, Hermens HJ, van Halteren AT, Nieuwenhuis LJ. Determinants of successful telemedicine implementations: a literature study. J Telemed Telecare. 2007;13(6):303–9.
8. Stell A, Sinnott R, Ajayi O. Secure federated data retrieval in clinical trials. In: Proceedings of the 2nd IASTED International Conference on Telehealth. Anaheim: ACTA; 2006.