CERIAS Tech Report 2009-11
Security Concerns in Telecare and Telemedicine
by Vaibhav Garg
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Vaibhav Garg

Entitled Security Concerns in Telecare and Telemedicine

For the degree of Master of Science

Is approved by the final examining committee:

Jeffrey Brewer Chair	Victor Raskin
Eugene Spafford	Teresa Doughty

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Jeffrey Brewer

Victor Raskin

Approved by: Eugene Spafford 19 April 2009
Head of the Graduate Program Date

Graduate School Form 20
(Revised 10/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

Security Concerns in Telecare and Telemedicine

For the degree of Master of Science

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Vaibhav Garg
Signature of Candidate

04/20/2009
Date

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

SECURITY CONCERNS IN TELECARE AND TELEMEDICINE

A Thesis

Submitted to the Faculty

of

Purdue University

by

Vaibhav Garg

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2009

Purdue University
West Lafayette, Indiana

To my family and friends for their encouragement and support.

ACKNOWLEDGMENTS

I would like to thank my advisors Prof. Jeffrey Brewer and Prof. Victor Raskin for their guidance. I am also indebted to my committee members Prof. Eugene Spafford and Prof. Teresa Doughty for their assistance and guidance. A special thanks for Marlene Walls for her help on countless occasions.

A thank you to my fellow graduate student Ankur Chakraborty for giving me hope. Thank you Shweta and Prashant for providing sanity. Finally I thank all my friends at Purdue, specially Ravi, Mona, Sahil, Aman, Padma, Shaunak, Gauri, Madalina, Jagadeesh, Chirag, Girish, Deepak, Youjung, Shalini and Ashwin, for making life more enjoyable.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Garg, Vaibhav. M.S., Purdue University, May, 2009. Security Concerns in Telecare and Telemedicine. Major Professors: Jeffrey Brewer and Victor Raskin.

Telecare and Telemedicine services are a technology-based replacement for in-home care services provided primarily to the elderly and consumers recovering from certain ailments. While these services are mostly successful in the pilot stages they tend to fail in real life settings. One major reason for this failure may be attributed to security issues associated with these services. This research attempts to identify the various Telecare/Telemedicine-related areas whose security issues need to be addressed. The research looks at the work conducted in the field and the issues still to be addressed.

CHAPTER 1. THE PROBLEM

In-homecare services are currently used to provide assisted living for people with disabilities, the elderly and individuals recovering from medical procedures. A major component of these services includes an in-home caregiver who provides continuous support to consumers with their needs and tasks. There is, however, a downside to these services. These services are expensive (Absher, 2009) and they may also curb individual autonomy. Other problems associated with in-home care include physical abuse and negligence leading to consumer death (Nerenberg, 2002) and staff shortages. Logistics of services may also lead to the need for consumer relocation. One promising alternative to in-home care services is the use of Telecare services.

1.1. Introduction

Access to quality medical care and diagnosis can be a problem in remote areas with low population density and/or poor connectivity to other areas. In these areas hospitals may suffer from lack of specialists. Even in areas with ample medical resources having a round the clock specialist might not be a feasible option. Telemedicine seems to be a promising solution. It allows consumers to transfer medical data over networks to doctors and other health

care professionals who make a diagnosis on the basis of this data. So if a patient needs a radiologist in one part of the world their data can be sent to a radiologist in another corner of the world where one is available and a diagnosis can be obtained at any time of the day.

Telecare/Telemedicine is a technology-based replacement for traditional care and provides a relatively inexpensive solution that allows consumers to remain in their own homes while maintaining their independence. A basic telecare system consists of a monitoring device and a response system. The monitoring system (for example a camera) allows the caregivers to keep a check on the consumers' condition. The response system, for example a two-way audio, allows the remote caregivers to communicate/interact with the consumer and provides them instructions. Should an emergency arise, a nearby team of caregivers is immediately dispatched to the consumer's home.

Telecare is used to provide assisted living to the elderly and was recently piloted in the homes of adults with intellectual disabilities (Buono et al., 2007). Telecare may be used to provide nursing assistance (or monitor) to consumers (e.g. diabetes) (Malasanos et al., 2005) and to assist alcoholics (Linke et al., 2005). In the case of recovering consumers, for example individuals suffering from diabetes, sensors specific to the recovery or support needs of the consumer would be used, for example glucose meters (Malasanos et al., 2005).

Several trials of Telecare and Telemedicine services are reported the world over and an effort is being made by different countries to use them in place of traditional care. Some of the positives cited are cost effectiveness and better

accessibility. Many of the trials report positive results in pilot stages. However they prove to be less successful in real life implementations (Tanriverdi, Iacono, 1998; Berg, 1999). Some researchers found the research methodology used in the trials to be suspect (Whitten et al., 2007). At the same time, researchers (Broens, et al., 2007) state that there are five determinants that ensure that Telemedicine projects that are successful in the research stages are also successful in the real world. Unless all of them are addressed success in pilot stages may not be reflected in real life implementations. One of these determinants is Policy and Legislation. Security is described as a part of this determinant. This research attempts to look at how well security is addressed in Telecare and Telemedicine research.

1.2. Statement of the Problem

Networks are central to the success of Telecare/Telemedicine services. These services allow data to be collected in a remote location and then sent over a network to a central location where qualified professionals can process information. Networks are the backbone for this to occur and thus need to be robust. Data must be secure when it is transferred. Once it reaches the desired location it should only be accessed by authorized individuals. It should be possible to follow audit trails to ensure that no information is accessible to anyone other than authorized individuals. At the remote location these services use sensors to monitor the consumer. There is a need to authenticate the

consumer to ensure that the data obtained from the sensor are that of the consumer and not someone else's, especially in cases where the consumer is living with other individuals like children. For example a thermometer that does not authenticate the consumer might send the temperature of consumer's children and not the consumer. Physical security and safety also become a cause for concern in remote locations that might not be easily accessible by emergency caregivers. Data must be accurate and arrive in time to make an early intervention.

To make a service completely secure one would require infinite resources. Telecare and Telemedicine services are bounded by resource constraints just like any other real world service. Thus individual services need to analyze what vulnerabilities from which they suffer. For different services, different vulnerabilities would have a different level of importance. For example, for consumers with AIDS, privacy would be most important. On the other hand, for elderly people in remote locations physical safety might be more important. Thus, threat modeling is important. It is important that the service not only be secure but that it states what it is secure against. Research in telemedicine is inadequate (Huston, 1999a; Huston 1999b). It either does not address security concerns or provides security solutions without building a threat model.

1.3. Significance of the Problem

The number of people requiring assisted living is steadily increasing (Haigh et al., 2002). Concurrently, the number of healthcare providers is decreasing (Dutch ministry of health welfare and sport, 2004). Conventional care-giving services suffer from various issues including high attrition rates amongst the caregivers, costly training of new staff and cases of abuse and negligence (Hawes, 2002). Thus the need exists to identify an alternative to conventional in-homecare services. One of the available alternatives is group homes in which residents experience the same issues as those receiving homecare services including negligence, staff abuse, high costs and loneliness (Emerson, 2004; Felce, et al., 2008; Stancliffe et al., 2007). Group homes generally house two or more consumers who live together, which may have a negative impact on personal safety (Emerson, 2004).

One promising alternative to in-homecare is Telecare. It is a relatively new technology and yet to be fully tested. Public perception of this service is not highly favorable as consumers may be reluctant to allow for continual video monitoring and the fear of “big brother watching” (Erkert, 1997; Percival et al., 2006) in the home. Elderly consumers may be perceived as less responsive to technology (Loera, 2008). Other stakeholders e.g. service providers, independent case managers, legal guardians and relatives may also not perceive Telecare to be a very reliable technology and are concerned safety, security and privacy. One major concern is the presence of a camera in their homes (Erkert, 1997;

Percival et al., 2006; Whitehouse et al., 2002). A consumer can view and account for a caregiver's actions in a traditional setting. But when the caregiver is remote their actions are not visible to the consumer. Thus there might be concerns about a caregiver abuse. Thus researchers need to be able to improve perception of safety, security and privacy. As Telecare becomes widespread the data it transfers will be covered under HIPPA and other privacy laws and it will need to meet standards like HL7. Issues of safety, security, privacy, poor perception of technology are common to both Telecare and Telemedicine and have to be addressed before Telecare/Telemedicine can become more widely accepted.

1.4. Statement of the Purpose

The purpose of the study is to review the literature examining the security issues associated with Telemedicine services in general and Telecare services in particular. There are two aspects of security, one is the actual level of security and the other is the perceived level of security. Research addressing either aspect will be covered by this study, which proposes to identify the areas that require greater attention. It is also necessary to examine the proposed solutions and determine if they are adequate. While examining these solutions, this review will discuss how they were tested, the scope of testing, and the generalizability of findings. The framing of this research is based on Whitten et al. (2007) who conducted a systematic study of research methodology in telemedicine studies.

This research will replicate their methodology when applied to *security issues in Telemedicine and Telecare.*

1.5. Definitions

1. Telemedicine: Telemedicine is the umbrella term that covers various technology-based solutions that allow medical care to be provided from remote facilities.
2. Telecare: Refers to remote care services wherein consumers are monitored by a remote staff by means of sensors. A basic Telecare setup consists of a two-way audio communication channel and a video monitoring system on the consumer end. For the purpose of this article Telecare and Telemedicine are going to be used interchangeably.
3. Privacy: It is the virtue by which an individual can control access to his or her information.
4. Safety: Safety is defined as a passive risk like falling from the stairs.
5. Security: In this study security acts as an umbrella term to the various kinds of risks a Telecare consumer might be exposed to. These risks might be active like a thief entering the house or passive like the consumer falling from the stairs. These risks can also be technological in nature like the consumer's data being sent over unencrypted channel.

6. Assisted Living: Consists of all kinds of living facilities for the consumer, e.g. elderly and the intellectually disabled, that does not include Telecare like group homes and in-home care and nursing facilities.
7. In-home care: In-home care refers to on site care. In this setting the consumer is usually provided with round the clock care by an onsite caregiver. The consumer lives independently either by themselves or with a relative.
8. Group Homes: In this setting a group of consumers live in a community home. Caregivers provide round the clock assistance. It is different from In-home care as the consumer lives along with other consumers.

1.6. Assumptions

The study assumes that a review of articles would be adequate to build an idea about the state of research in security in Telecare/Telemedicine.

1.7. Delimitations

The purpose of the study is to identify the prevailing security-related issues using Telecare/Telemedicine. The second purpose is to identify the solutions, if any, proposed for those problems and the limitations of those proposed solutions. It is not the purpose of the study to provide original solutions to the problems.

1.8. Limitations

Due to constraints of resources, the study can only review a limited number of articles. Currently the study as it is designed only reviewed 58 articles. It is also possible that the automated search using keywords may entirely miss articles whose primary purpose was not to address a security related issue, but who however talk about security as a part of their research.

CHAPTER 2. LITERATURE REVIEW

Thompson (1984) marked a change in how we viewed computers and networks. It established the ease in which malicious components can be hidden inside a system without the users knowledge. We could no longer trust a system even if we studied all its components. The latest systems with Windows Vista (50 million lines of code) (Manes, 2007) and Intel processor (2,100,000,000 transistors) (Sinyee, 2008) are often too complex for the consumers to even check each component. Then we also have the human component of training and the lack of which allows for social engineering (Mitnick, Simon, 2002). The threat now went from being technology based to being human based. The best security services were worth nothing if the staff gave the secrets out. This led to the concept of insider threats (Schneier, 2005). Recently attacks on epilepsy patients (Poulsen, 2008) showed that miscreants can use networks to cause harm not only in the digital world but also in the physical world.

2.1. Why Bother: Why do we need Security?

Networks are central to the existence of Telecare services. Networks allow communication between the remote site where the consumer is being provided care and the base site where they are being monitored by the care-giving staff.

Without this communication it would not be possible for the caregivers to ensure that the consumer is safe and secure. Data are transmitted in various forms including video (from the camera), audio (from the microphone), location-based (from the sensors placed on doors) or medical (like from glucose meters). As such, it is essential that the security of this system is robust and reliable. But by nature of being a network Telecare services may suffer the same security issues encountered by standard networks.

For example, providing secure reliable data transfer between the consumer's home and the remote site where the consumer is being monitored is a concern. Often, the data transmitted from the consumer's home are medical in nature and thus, fall under the confidentiality guidelines afforded to consumers under the Health Insurance Portability and Accountability Act (HIPPA). There is also the problem of access control. A video that is sent to the remote site can easily be re-recorded and then accessed by unauthorized personnel. There are also issues of trust. An onsite caregiver can be viewed by the consumer and thus, their actions may be perceived to be more safe since there can be accountability for their actions. On the other hand, most telecare services engage a one way video communication channel at best that does not let the consumer view the actions of the remote caregiver.

Broens et al. (2007) state the following:

> Security is important in two ways: patient physical safety and patient information security. For acceptance of telemedicine implementations

> adequate security mechanisms have to be taken into account. These security mechanisms should support the crucial trust relation between health-care providers and patients. The review showed that there is also need for secure information transfer and authorization mechanisms. (p. 306)

Telecare is also covered under the umbrella term of telemedicine and thus, is subject to the same determinants as telemedicine. Thus, security is as important in telecare as in other applications of telemedicine. A consumer using telecare services should be ensured information security. The information collected (audio, visual and textual) on a consumer should be transferred over secure lines and should be accessible only by authorized individuals. If a transgression is made it should be possible to audit and the entity responsible held accountable. Similar to other information technology applications, the problem is of Authorization, Authentication and Accounting (Stell, Sinnott, Ajayi, 2006). Savastano et al. (2008) notes, “If patients are not confident that their information is acquired, transmitted and stored in a secure and confidential way, they will probably not be keen to reveal accurate and complete information. (p.386)” Lack of accurate and complete information lowers the quality of healthcare. Poor quality of care would reduce the confidence of both the providers and the consumers in Telemedicine/Telecare services.

Security issues need to be addressed in a methodological and thought out manner. In software, it is an acceptable practice to release patches after an incident reveals a vulnerability. However, this might not be acceptable in the field

of medicine since the damage here would not be in terms of data, but it would be in terms of human life. Thus, a good design for security analysis is warranted.

2.2. Step One: Threat Modeling

Bruce Schneier (1996) states the following:

> A good design starts with a threat model: what the system is designed to protect, from whom, and for how long. The threat model must take the entire system into account-not just the data to be protected, but the people who will use the system and how they will use it. What motivates the attackers? Must attacks be prevented, or can they just be detected? If the worst happens and one of the fundamental security assumptions of a system is broken, what kind of disaster recovery is possible? The answers to these questions can't be standardized; they're different for every system. Too often, designers don't take the time to build accurate threat models or analyze the real risks.
>
> Threat models allow both product designers and consumers to determine what security measures they need. Does it makes sense to encrypt your hard drive if you don't put your files in a safe? How can someone inside the company defraud the commerce system? Are the audit logs good enough to convince a court of law? You can't design a secure system unless you understand what it has to be secure against. (Why Cryptography is harder than it looks, para. 16)

Threat modeling allows a developer to identify the attack vectors to which a system may be subjected. Telemedicine systems have both human and technology components and thus they are subject to attacks suffered by both as well as attacks specific to the overlap of these components. Different telemedicine implementations would suffer from different kinds of attacks. While a generic threat modeling is required, there should be a provision for threat modeling of each individual implementation. In the case of older adults, special attention needs to be paid to physical safety measures, like detection of falls. On the other hand, for diseases like HIV/AIDS, which can lead to social implications, special attention needs to be paid to privacy. Telemedicine implementations used for clinical trials need to pay more attention to anonymization of data. Implementations using medical information essential for diagnosis would require data integrity. If multiple people are using a system there would be a need for authentication and access control.

2.3. Step Two: Solving the Puzzle

Once threats are identified, they need to be prioritized. To make something completely secure one would require infinite resources. However, most Telemedicine service providers are resource constrained. It is especially difficult to justify spending money on security, since security works best when nothing happens. Thus it is important that resources are being spent on more ominous threat vectors.

Once the provider identifies the major security threats, they need to make sure that they opt for the right solutions. One way of doing this is by adhering to standards. For example using Secure Socket Layer to establish a secure channel for data transfer. But even using standards would not end the problem. There is the question of implementation. If a standard were not implemented correctly it would still be vulnerable. Sometimes standards outlast their utility. For example, DES and WEP continued to be the standards long after they were proven insecure.

Then there is the issue of usable security. If a system is secure but not usable it would either be underutilized or used in improper manner. For example too many alerts can render the user insensitive to the importance of the alert. Haigh et al. (2002) notes, “One of the greatest challenges for systems in this domain is to provide an interface for potentially technophobic users with varying capabilities and constraints. Older adults have more difficulty learning new computer skills, and interfaces that are poorly designed cause devices to be abandoned. (p. 7)”

2.4. Step Three: Testing

Once the solution is implemented it should be tested. Reliability is one issue. Does the system give false positives or false negatives? What is the threshold above with false positives/negatives would become unacceptable? Availability is another issue. A lot of network based systems are susceptible to

Denial of Service attacks. This might be a problem for certain implementations. For example, in case of patients requiring critical care, Denial of Service can lead to psychological and physical injuries. Recovery and backup is the final issue that should be tested. What happens when a system fails? How effective are the emergency measures? How much time is spent before the system is running again? All these questions need to be answered and should be evaluated by using metrics.

Training is the most important and probably the most neglected part of building a secure system. Most providers do not realize that no system can be secure unless the people who are handling these systems are trained to use them in a secure and reliable manner. There have been several cases of systems failure due to human negligence. This is especially true when systems fail due to social engineering (Mitnick et al., 2002).

2.5. How Safe is Safe Enough?

Fischhoff et al. (1978) noted, " Acceptable risk for a new technology is defined as that level of safety associated with ongoing activities having similar benefits to society." Stakeholders like consumers and providers will compare Telecare/Telemedicine services to traditional care. Thus, once the system is in place it is important to evaluate the perception of the system for different stakeholders. Even if the system is completely secure, but the provider does not feel that it is, they are unlikely to suggest it to a consumer. At the same time if the

consumer feels the system is either insecure or intrusive they are unlikely to use it. Telemedicine systems in particular should be evaluated for perceptions, since they are perceived as intrusive and ineffective (Percival et al., 2006) since caregiving is usually assumed to be a human experience. For consumers suffering with dementia, Whitehouse et al. (2002) note, “Will computers diagnose dementia based on a pattern of inefficiencies in their use? More importantly, will computers be able to adapt to their aging users, presenting in ways that account for their cognitive abilities? (p. 4)” Due to the poor perception of computer aided assistive living technologies it is important to measure the same for different stakeholders.

CHAPTER 3. METHODOLOGY

This study aims to access the research conducted in security in telemedicine in general and Telecare in particular. The study will identify the key areas that were studied and the respective pros and cons of the solutions being proposed. The study also aims to identify security measures that need immediate attention due to lack of research or the significance of the threat. Several journals were searched with the following keywords:

1. Telemedicine and Security
2. Telemedicine and Safety
3. Telemedicine and Privacy
4. Telecare and Security
5. Telecare and Safety
6. Telecare and Privacy

The following journals were searched. Some of the journals were not searched individually but were searched through a database called *PubMed*:

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

In all 66 articles were found. Eight articles, found with the search phrase 'Telemedicine and Safety', were excluded since they were not pertinent to this research. Articles used in the literature review were excluded. In the end 58 articles were collected and coded according to the following scheme for meta-analysis:

1. Article Title
2. Research Questions
3. Security Issues
4. Types of Security issues e.g. Privacy, Physical Safety
5. Threat Model
6. Metrics (yes/no). If yes, what metrics?

7. Significance of Problem
8. Solution Proposed (or Results)
9. Solution tested (yes/no). If yes what were the results?
10. Limitation

This is a qualitative study that aims to do a meta-analysis of the reviewed articles. Once the articles were coded, the study would bring to light the areas of security that were not addressed adequately and their importance. The study also attempts to look at the proposed solutions and bring to light their limitations. Finally, the most important focus of the study is on identifying the problems in the methodology of research pertaining to security issues in Telemedicine and Telecare.

CHAPTER 4. DATA

In this section we present each individually coded article. Each new article starts after a page break to maintain readability.

4.1. Paper 1

1. Article Title

   Columbia University's Informatics for Diabetes Education and Telemedicine (IDEATel) Project: Technical Implementation
2. Research Questions
   a. Evaluate feasibility, acceptability, effectiveness and cost effectiveness of telemedicine.
3. Security Issues
   a. Secure web-based messaging
   b. In particular, the security issue was how to keep the service efficient and user friendly while at the same time providing adequate security
4. Types of Security issues e.g. Privacy, Physical Safety
   a. Data Security
5. Threat Model
   a. No
6. Metrics (yes/no). If yes, what metrics?
   a. No
7. Significance of Problem
   a. Security is important since the data in question is primarily medical data. Patients would be more comfortable using the web messaging if they were assured of the secrecy of the information divulged.
8. Solution Proposed (or Results)
   a. SSL is used for secure channel
   b. HL7 standards
   c. Password protected VPN for authentication
   d. Four authorization levels for different levels of access
   e. Audit trails are maintained
   f. Physical security is taken into account

9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. A threat model was not proposed. The setup was tested for operations, not for security. This limits the trust that one can put in the system. However, the use of standard security practices like using SSL does provide some confidence.

4.2. Paper 2

1. Article Title
    a. The High-Performance Computing and Communications Program, the National Information Infrastructure, and Health Care
2. Research Questions
    a. No research questions, this is a review article
3. Security Issues
    a. Data privacy of medical records
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Data privacy is important to provide confidence to the consumers that their information would not be divulged.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. NA

4.3. Paper 3

1. Article Title
    a. The use of telecare for people with chronic obstructive pulmonary disease: implications for management
2. Research Questions
    a. Evaluation of telecare services for Chronic Obstructive Pulmonary Disease (COPD) patients.
3. Security Issues
    a. Increased perception of safety and security due to telecare.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Safety
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. NA
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. While the study reports an increase in the perception of safety in the patients, it does not quantify it or supports with any data.

4.4. Paper 4

1. Article Title
    a. The legal and risk management conundrum of telemedicine
2. Research Questions
    a. An assessment of risk in telemedicine services
3. Security Issues
    a. Security, Confidentiality, Risk, Legal
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Security, Confidentiality, Risk, Legal
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Problem has not been defined
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. Security, confidentiality and risk are identified as areas of concern. However what that means is not stated. No problem has been defined nor any solutions provided.

4.5. Paper 5

1. Article Title
    a. Mobile Phone Text Messaging for Pharmaceutical care in a hospital in China
2. Research Questions
    a. Evaluating the effectives of a SMS based information systems that informs the patients about their medication.
3. Security Issues
    a. Adverse effect of medication
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Safety
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. The problem is that there is lack of information about the adverse effects of the drugs that a patient might. There are also safety issues with under medication, over medication and untimely medication.
8. Solution Proposed (or Results)
    a. A SMS based solution is proposed.
9. Solution tested (yes/no). If yes what were the results?
    a. The solution is tested via a quantitative study and the results are found to be satisfactory. Most participants find the solution to be effective.
10. Limitation
    a. The results might not be generalizable for all kinds of diseases especially Alzheimer. Amongst the sample, there was a dearth of the elderly and since they are known to not adapt to technology as

quickly the solution might also not work for all age groups.

4.6. Paper 6

1. Article Title
    a. Designing mobile dietary management support technologies for people with diabetes.
2. Research Questions
    a. Evaluating the effectiveness of a digital solution for helping patients suffering with diabetes
3. Security Issues
    a. No security issues are identified
4. Types of Security issues e.g. Privacy, Physical Safety
    a. None
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. No security issues are talked about. However since medical data like blood glucose is transferred and stored, HIPAA compliance should have been a issue.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. No security issues have been identified. This is worrisome since medical data and patient information is transferred over networks and stored in digital media; thus standard security issues like data security and privacy should have been a concern.

4.7. Paper 7

1. Article Title
    a. Home telecare technologies for the elderly
2. Research Questions
    a. An analysis of the different home telecare technologies for different diseases. What are the different factors that would drive the development and dissemination of these technologies?
3. Security Issues
    a. Data Security
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Computer Security and Data confidentiality
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. A specific problem has not been identified
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. No specific problem has been proposed. The paper only talks about data security and computer security but fails to mention network security and physical safety and security.

4.8. Paper 8

1. Article Title
    a. Identity Management factors in e-health and telemedicine applications
2. Research Questions
    a. An evaluation of standardization of security in telecare services.
3. Security Issues
    a. Reliable identification through secure channels that are standardized and thus used by all allowing communication between unknown entities.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Standardization and Policy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. The problem stated is very important. There need to devices that ensure the security of the data and the individual. To ensure that we use technologies like Iris scans. These technologies need to be standardized to mitigate concerns about safety. There is also the issue of privacy of medical data and the ethics involving the revelation of this data for care purposes. If the patient is unsure about security they might not provide accurate data. If the provider is unsure they might choose not to use the technology or not use it to the full extent, leading to poor care and underutilized systems. Compromise of health IT systems can cause financial damage in terms of lawsuits and reputation loss.
8. Solution Proposed (or Results)
    a. Adherence to ISO/IEC 20000 standards.

9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The only limitation seems to the overbearing importance given to RFID and biometrics. These technologies have significant drawbacks which have not been discussed e.g. management of databases of biometric identifiers etc.

4.9. Paper 9

1. Article Title
    a. Design of a trial of Internet-based self-management for diabetes
2. Research Questions
    a. Evaluation of feasibility, acceptability and effectiveness of a web based management system for diabetes patients.
3. Security Issues
    a. Data would be stored on remote servers thus it has to be protected. Participants should be trained to use the systems in a safe manner.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security and Confidentiality
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Safety of the data is important just because its is personally identifiable medical data.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. The security requirements are not well defined. The kind of data being stored is not given, thus there is no way to identify what level of security would be required to protect it reasonably. Also the stress is only on security once the data is being stored, there is no mention of security of the data in transit or the integrity of the data.

4.10. Paper 10

1. Article Title
    a. A systematic review of the benefits of home Telecare for frail elderly people and those with long-term conditions
2. Research Questions
    a. A meta analysis of studies of home Telecare systems for the elderly and those with long term diseases
3. Security Issues
    a. Effectiveness of safety features like fall monitoring.
    b. Effectiveness of security features regarding data security
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Safety
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Evaluation of physical safety measures is very important since the patient would not have on site caregivers to assist them in case of an emergency. In case the safety measures do not work (preventive and mitigating) the patient would be left stranded in case of an emergency.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. The safety and security concerns are limited to physical security

4.11. Paper 11

1. Article Title
    a. Standards for data collection and monitoring in a telemedicine research network
2. Research Questions
    a. Standardization of policies in privacy, security, confidentiality, technical standards, telecommunication, computer infrastructure, change management and training to allow for inter-operatibility.
3. Security Issues
    a. Standardization of policies in privacy, security, confidentiality.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Policy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Standardization of security practices is important to impart trust in the users, since it allows them to evaluate how secure a particular service is.
    b. Standardization also allows inter-opertability that in turn allows wider dissemination of a technology
8. Solution Proposed (or Results)
    a. Development of a National Health Information Infrastructure
    b. Introduction of universal patient identifiers and health provider identifiers.
    c. Development of standards based Telemedicine Research Networks.
9. Solution tested (yes/no). If yes what were the results?
    a. No.

10. Limitation
    a. The paper does not discuss the hurdles in the development of universal patient identifiers.
    b. It does not talk about the roadblocks in development of standards, especially in security where two different aspects of security might contradictory or security itself would be contradictory with usability.

4.12. Paper 12

1. Article Title
    a. Management of medicines information for patient safety
2. Research Questions
    a. How to ensure patient safety in the management of medicines?
3. Security Issues
    a. Security of data as it is shared across different medical communities
    b. Safety of the patient from adverse drug reactions.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security, Physical Safety
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Security of the data in question is important since it is personally identifiable medical data.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. No.
10. Limitation
    a. Without a threat model and without a solution simply stating that security is important for medical data does not really add anything to the existing body of knowledge.

4.13. Paper 13

1. Article Title
    a. Information and communication technology in supporting people with serious chronic illness living at home – an intervention study
2. Research Questions
    a. Evaluation of the improvement of quality of life in patients suffering from chronic illness while using text based virtual rooms to communicate with health care providers.
3. Security Issues
    a. The lack of feeling of safety and security in patients suffering from chronic illness.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Perception of Safety
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Perception of safety and security can have significant effect on the quality of life of the patients. If the patients feel insecure they are likely to be less happy and confident about living independently.
8. Solution Proposed (or Results)
    a. A channel of communication with the care provider using text messaging.
9. Solution tested (yes/no). If yes what were the results?
    a. Yes. The text messaging allows the patient to feel more secure. They feel that they have access to help.
10. Limitation
    a. This solution might not be universally acceptable especially amongst older adults. As a qualitative study the results cannot be

generalized. Also this solution only addresses the perception of safety and security not actual safety and security.

4.14. Paper 14

1. Article Title
    a. Telemedicine systems and telecommunications
2. Research Questions
    a. What are the elements of a successful telemedicine implementation?
3. Security Issues
    a. Security of medical information being transferred and stored and maintaining privacy of patient.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data security and Privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data security and privacy is important from the point of view of adhering to legal requirements like HIPAA and also to provide the users trust that their information is safe.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. A threat model is not proposed. The definition of security is limited to technology; there is not discussion of physical security or the perception of security amongst the users.

4.15. Paper 15

1. Article Title
    a. Information governance standards for managing e-health information
2. Research Questions
    a. Evaluation of data quality of electronic health information
3. Security Issues
    a. Security of medical information being transferred and stored and maintaining privacy of patient.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Security, Privacy, Confidentiality, most importantly data integrity
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data security and privacy is important from the point of view of adhering to legal requirements like HIPAA and also to provide the users trust that their information is safe.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. There is no solution proposed to allow for construction of adequate policies. There is no discussion of why these policies do not exist.

4.16. Paper 16

1. Article Title
    a. Challenges for implementing wireless hand-held technology in health care: views from selected Queensland nurses.
2. Research Questions
    a. What factors are roadblocks in implementing wireless technology in healthcare?
3. Security Issues
    a. Security and Confidentiality of Data
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Security and Confidentiality of Data
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data security and confidentiality is important from the point of view of adhering to legal requirements like HIPAA and also to provide the users trust that their information is safe.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. None
10. Limitation
    a. Importance of data security and confidentiality in health care is well known and as such does not add to the body of knowledge. The results are limited in the sense that there is no grading within the individual challenges. The participants identified 15 themes as challenges, it would have been interesting to see a relative grading of the importance of these challenges.

4.17. Paper 17

1. Article Title
    a. An intelligent emergency response system: preliminary development and testing of automated fall detection
2. Research Questions
    a. Evaluating the effectiveness of a fall detection system that provides information about whether a there is an emergency and the patient needs help?
3. Security Issues
    a. Elderly patients who live independently at home can have an accident like a fall. Can a technology-based solution be used to identify when such fall occurs and inform caregivers that the patient might need help?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Safety
5. Threat Model
    a. Falls that might cause hip fractures and other sort of physical injuries to a patient.
6. Metrics (yes/no). If yes, what metrics?
    a. Yes. Percentages.
7. Significance of Problem
    a. One of the issues with the elderly patients living independently is that they might get into an accident and caregivers would not be aware that they need help. This reduces the quality of life of the patient. The fall can cause both physical and psychological damage.
8. Solution Proposed (or Results)
    a. A vision based system that identifies if a fall has occurred.
9. Solution tested (yes/no). If yes what were the results?
    a. Yes. 315 trials were done and the system identified falls 77% of the

time and missed 23%. There were 5% cases of false alarms.

10. Limitation
    a. The study did not play with the threshold value of the fall. It is possible that if the system were manipulated to catch the fall more number of times it would lead to an increase in the number of false alarms.
    b. It is also a subjective issue whether 77% success ratio would be acceptable in a real life scenario.

4.18. Paper 18

1. Article Title
    a. Network basics for telemedicine
2. Research Questions
    a. Identifying the various factors and the trade offs that define performance in digital technologies that are being for telemedicine communications.
3. Security Issues
    a. What are the solutions to ensure privacy and confidentiality of this data.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy and Confidentiality
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Since data packets travel through a public network there is a need for security.
8. Solution Proposed (or Results)
    a. VPN (Virtual Private Networks)
    b. AES (Advanced Encryption Standard)
    c. PKI (Public Key infrastructure)
    d. Firewalls
    e. Network Address Translators (NAT)
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The relative pros and cons of the technologies and the problems with the implementation have not being discussed. While the

problem of security vs. usability is touched upon it could have been developed further since that is probably the most important factor as the telemedicine is used a lot of times for people who do not adopt technology very quickly.

4.19. Paper 19

1. Article Title
    a. Virtual microscopy and public-key cryptography for Internet telepathology
2. Research Questions
    a. Can telepathology be used to give accurate diagnosis in a secure manner?
3. Security Issues
    a. Since the images are going to be sent over a public network, how to maintain the integrity and confidentiality of the data?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy and Confidentiality
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Images required by telepathology provide data that is medical in nature and thus requires the same kind of protection that any other medical information does.
8. Solution Proposed (or Results)
    a. Public Key Cryptography
9. Solution tested (yes/no). If yes what were the results?
    a. Yes
10. Limitation
    a. Public Key cryptography is not a very efficient method for big amounts of data. Images are usually big data. There should be a more efficient way of doing this like using Public keys to exchange symmetric keys that are later used to encrypt the images.

4.20. Paper 20

1. Article Title
    a. The Austrian Academic Computer Network and its usefulness for teleradiology
2. Research Questions
    a. Feasibility of image transfer for teleradiological consultations.
3. Security Issues
    a. Not defined
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Not Defined
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Problem is not defined.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. NA

4.21. Paper 21

1. Article Title
    a. Telemedicine in Australia. Recent developments
2. Research Questions
    a. Review and evaluation of development in telemedicine.
3. Security Issues
    a. Privacy and security issues of transferring medical data.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy and confidentiality
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Problem is not defined.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. NA

4.22. Paper 22

1. Article Title
    a. Telegenetic medicine: improved access to services in an underserved area
2. Research Questions
    a. Evaluation of telegenetic services for children.
3. Security Issues
    a. Privacy of the patient.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy and perception of privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. Yes. Percentage.
7. Significance of Problem
    a. Perception of privacy is important since if the patient or their guardians feel unsure about privacy they would choose not to use telegenetics that are helpful especially in remote areas.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. While the guardians were satisfied with the privacy of their wards, it is unsure why they came to this conclusion. Thus it is not necessary that the results can be generalized.

4.23. Paper 23

1. Article Title
    a. Improved access to subspecialist diabetes care by telemedicine: cost savings and care measures in the first two years of the FITE diabetes project.
2. Research Questions
    a. Evaluation of telemedicine services for diabetes care in remote areas.
3. Security Issues
    a. Privacy of patient information
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Privacy of patient information is important to build trust in providers and patients that leads to better care and for legal purposes.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. There is limited detail on how the perception of privacy was measured.

4.24. Paper 24

1. Article Title
    a. Emerging trends in ocular telemedicine: the diabetic retinopathy model
2. Research Questions
    a. Evaluation of telemedicine services for diabetes to check if telemedicine provides clinical care of the same standard as provided by traditional care.
3. Security Issues
    a. Privacy of patient information
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Patient information needs to be HIPAA compliant to meet standards of traditional care.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. HIPAA is only for electronic data, there are other security issues with the service that were not looked into.

4.25. Paper 25

1. Article Title
    a. Telemedicine in Australia. 2: The Health Communication Network (HCN)
2. Research Questions
    a. A review of the Health Communication Network (HCN) in Australia.
3. Security Issues
    a. Privacy of patient information
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy Policy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Privacy of patient information is a big concern. If the patients do not trust the technology they are less likely to use it.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. NA

4.26. Paper 26

1. Article Title
    a. High-quality television links for home-based support for the elderly
2. Research Questions
    a. An evaluation of the qualitative aspects of a television based telecare service for the elderly
3. Security Issues
    a. The perception of privacy for the provider and patient. Security of data in transit and storage and need for training for the people who deal with this data.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy, Data Security and training
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Privacy of patient information is a big concern. If the patients do not trust the technology they are less likely to use it. There is also a need to look at the training for the personnel who deal with patient data.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. There is no discussion on why less invasive technologies might not be an equally good option.

4.27. Paper 27

1. Article Title
    a. TECHTALK: Security of Internet-based Telemedicine Systems
2. Research Questions
    a. A review of security in telemedicine systems
3. Security Issues
    a. A review of security issues in telemedicine from technological perspective to physical security
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Security, Access Control, private networks, firewalls, authentication, encryption, time stamping.
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Security is one of the major issues in acceptance of telemedicine technologies. Poor security leads to poor trust in the system. So the system is either underutilized or not given complete and accurate information leading to poor quality of care and thus even further lack of trust.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. There is no comparison of the different solutions for security and the pros and cons of each.

4.28. Paper 28

1. Article Title
    a. Security Framework for Pervasive healthcare architectures utilizing MPEG-21 IPMP Components
2. Research Questions
    a. Evaluation of MPEG-21 as a means of secure data communication
3. Security Issues
    a. Can MPEG-21 be used to provide data integrity, confidentiality and privacy for the patient?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data integrity, Confidentiality and privacy. Key Distribution.
5. Threat Model
    a. Yes
        i. Non authorized access to patients medical data
        ii. Intentional alteration of patients medical data
        iii. Disclosure of medical data to third parties
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Security is one of the major issues in acceptance of telemedicine technologies. Poor security leads to poor trust in the system. So the system is either underutilized or not given complete and accurate information leading to poor quality of care and thus even further lack of trust.
8. Solution Proposed (or Results)
    a. An architecture based on MPEG-21 standard using Intellectual Property Right Management (IPMP).
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation

a. There is no discussion of MPEG-21 not being compliant to HL7 standards for medical data.

4.29. Paper 29

1. Article Title
    a. Real time and secure wireless health monitoring
2. Research Questions
    a. A framework for a wireless system for monitoring and transmission of healthcare information in a secure manner.
3. Security Issues
    a. Security of wireless systems for transmission of medical data
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Key distribution, Authentication, Confidentiality, Integrity, Security Protocols
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Security is one of the major issues in acceptance of telemedicine technologies. Wireless security issues can be more and varied from wired systems.
8. Solution Proposed (or Results)
    a. A wireless 3-tierd health monitoring system using wireless networks like Zigbee
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The solution proposed has not even been theoretically tested. For example a security protocol is proposed but it has not even been subjected to logic-based tests like BAN logic.

4.30. Paper 30

1. Article Title
    a. Basic Application-Related Patient Identifiers: What Solution for a European Country?
2. Research Questions
    a. Can patient identifiers be developed using hash functions and social security numbers?
3. Security Issues
    a. Security of patient identifiers based on social security numbers
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy and Anonymity.
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Developing patient identifiers has been very hard. If patient identifiers are either social security numbers or a derived number, it is possible to link patient data to other information like social, economic or employment.
8. Solution Proposed (or Results)
    a. Converting social security numbers into patient identifiers using hash functions.
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. There would still be information leakage if patient identifiers were based on social security numbers. For example if social security number is known an adversary can find whether a patient was ever admitted to a hospital by looking at the hospitals records.

4.31. Paper 31

1. Article Title
    a. A Tamper Resistant and Portable Healthcare Folder
2. Research Questions
    a. Developing a framework for electronic medical health records that would give the patient more control over sharing of their medial data using smart cards and USBs.
3. Security Issues
    a. The dissemination of the patient information should be in control of the patient to satisfy privacy requirements and build trust
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy.
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. If the patients do not have control over the sharing of their medical information, they are less likely to be trustful of the systems and be unwilling to provide complete and accurate information and thus there would be more chance of poor care.
8. Solution Proposed (or Results)
    a. Secure portable token (SPT) that is a microcontroller chip in charge of security mechanisms with an eternal memory in charge of storage of the patient information.
9. Solution tested (yes/no). If yes what were the results?
    a. A study to test the solution has been proposed. But it is more about the acceptance of technology rather than the reliability of it.
10. Limitation
    a. Duplication of patient data is still a problem from the centralized dB.

4.32. Paper 32

1. Article Title
    a. An integral care telemedicine system for HIV/AIDS
2. Research Questions
    a. How can telemedicine be used to improve self care in HIV/AIDs patients?
3. Security Issues
    a. Security of data for HIV patients including anonymization, since HIV/AIDs is sometimes considered a stigma and sometimes patients would not want it to be known that they suffer from the disease.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Anonymization, Authentication, Access Control
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. It is important to protect patient information for HIV patients especially as it is still considered a stigma.
8. Solution Proposed (or Results)
    a. VPN
    b. Encryption
    c. Password based login systems
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. There is not much detail on the security mechanisms. There are pros and cons of using each mechanism. There is no justification why certain solutions were used over others.

4.33. Paper 33

1. Article Title
    a. Taking the call-bell home: a qualitative evaluation of Tele-HomeCare for children
2. Research Questions
    a. Evaluating the effect of Tele Home care (THC) on children for early discharge from traditional care facilities.
3. Security Issues
    a. Effect of THC on the sense of security for the patients and their primary care givers.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Perception of Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. It is important the system builds a sense of trust and security in the patient and the family otherwise they would be unwilling to take an early discharge which is not only cost effective but also helps the patient recover earlier since they are in familiar surroundings.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. Perception of security should be based on actual security. There is no discussion of why the system is reliable and worthy of the trust that the patients put in it.

4.34. Paper 34

1. Article Title
    a. Telemonitoring of patients at home: a software agent approach
2. Research Questions
    a. Preserving the privacy and quality of life of the patient while providing them more autonomy.
3. Security Issues
    a. Design and evaluation of a software based telemonitoring and alarm system.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Perception of Security, Privacy, Physical Security.
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. There is a growing demand for a system that would allow patients to live at home. There are two major deterrents to this. One this the perception of safety and quality of care going down.
8. Solution Proposed (or Results)
    a. Yes
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The security question has not been very well described. There is little discussion about the sensors for physical safety and security.

4.35. Paper 35

1. Article Title
    a. Safety and Privacy in RFID and Applications in Telemedicine
2. Research Questions
    a. What are the security and privacy implications of using RFIDs in telemedicine applications?
3. Security Issues
    a. What are the security and privacy implications of using RFIDs in telemedicine applications?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Security and Privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Unless security and privacy issues can be addressed use of RFID would be limited since most countries have laws that need to be satisfied regarding patient's right to privacy and security of medical data. Security issues are very significant in RFIDs that are vulnerable to many attacks like denial of service, eavesdropping etc.
8. Solution Proposed (or Results)
    a. Yes
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The attacks and the solutions could have been better understood if a threat model was given. No solution is good for all threat models. There might be a greater possibility of denial of service attack in a

certain environment while in another application the key attack might be eavesdropping.

4.36. Paper 36

1. Article Title
    a. Digital Watermarking in Telemedicine Applications – Towards Enhanced Data Security and Accessibility
2. Research Questions
    a. Developing architecture to use watermarking to improve security of telemedicine applications.
3. Security Issues
    a. Security of data in transit.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. There is a need to secure medical data and improve authorized accessibility.
8. Solution Proposed (or Results)
    a. Yes. Watermarking.
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. There is no discussion of scenarios where watermarking would fail. Also the system is not tested. This systems uses two preexisting architectures, there must have been some inconsistencies when you try to combine them. It is usually better to build a solution from scratch, than use something preexisting which might be incompatible or have gaps with the other preexisting solution, because it is these gaps that are used by attackers to get into the

system. A common example is rootkits.

4.37. Paper 37

1. Article Title
    a. The North Norwegian Health Net
2. Research Questions
    a. Developing a secure national computer based health care network to improve the quality and accessibility to health care providers.
3. Security Issues
    a. Security and integrity of the data that is being stored or transmitted over the network.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security and integrity
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. There is a need to secure medical data and improve authorized accessibility especially in a country like Norway that is sparsely populated and there are regions that are not well connected to traditional health care services.
8. Solution Proposed (or Results)
    a. Yes. A national interconnected network that would have all health care services interconnected including telemedicine services. It uses encryption for authentication.
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The details about the security measures are few.

4.38. Paper 38

1. Article Title
    a. Changes in the job situation due to telemedicine
2. Research Questions
    a. How is it different for a healthcare professional to work with telemedicine than working with traditional healthcare.
3. Security Issues
    a. Does the healthcare provider have a better sense of professional security?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Perception of Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. If the caregiver finds the system to be secure there would be a better chance of them accepting a change to telemedicine. For example they might feel that telemedicine would cause them to lose their jobs and they would feel threatened by technology.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The paper states that the caregivers had a better sense of professional security but does not discuss how this conclusion is reached. None of the questions asked seem to address this issue.

4.39. Paper 39

1. Article Title
    a. International medical education between Hawaii and Thailand over Internet2
2. Research Questions
    a. Evaluation of videoconferencing over Internet2.
3. Security Issues
    a. Firewall waivers were required for every IP connection.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Access Control.
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. If waivers are required for every connection it would be hard to make the service available to different personnel on a variety of systems.
8. Solution Proposed (or Results)
    a. Yes. Virtual Local Area Network.
9. Solution tested (yes/no). If yes what were the results?
    a. Yes
10. Limitation
    a. The definition of the problem and the solution are not really clear. It is also not clear how security over internet2 is different fro security over Internet.

4.40. Paper 40

1. Article Title
    a. Current developments in Canadian privacy and information law: implications for telehealth
2. Research Questions
    a. Implications of laws regarding patients private information
3. Security Issues
    a. How to protect patient's right to privacy while maintaining access for legitimate access?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. It is important to protect patient's medical data or identifiable information because the patient might not want that information to be known and it also gives them more trust in the system. However too much legislation can put too many restrictions on patient data leading to a lower quality of care.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The change in laws change the application of telemedicine but the change in telemedicine also changes the laws. The paper only looks at one side of the equation.

4.41. Paper 41

1. Article Title
    a. An evaluation of an intelligent home monitoring system.
2. Research Questions
    a. Does the quality of life increase for the patient if they use an intelligent monitoring system along with traditional care.
3. Security Issues
    a. Does the system respond if the client has an accident?
    b. Is the system too intrusive?
    c. Is the system respectful of patient's right to privacy?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy, Physical Safety and Security.
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. It is usually very expensive for patients to get 24-hour care as it is very expensive. 24-hour care is also wasting manpower since for a significant section of the time the patient would be sleeping. This is where monitoring systems step in. They are cheap and can replace human caregivers in periods of low activity. They also compliment the human caregivers during the daytime.
8. Solution Proposed (or Results)
    a. The system was found to give few false positives and had only two false negatives that were the result of the patient responding before the system could identify the situation. The patients also did not find the system to be intrusive.
9. Solution tested (yes/no). If yes what were the results?
    a. Yes.

10. Limitation
    a. While the paper talks about both safety and security the system seems to address only safety and not security.

4.42. Paper 42

1. Article Title
    a. Telephone advice nursing – callers experiences
2. Research Questions
    a. Evaluating the perception of a medical call centre service
3. Security Issues
    a. Does the patient feel more secure after contacting the call centre?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Perception of Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. A number of the times the patient calls in when they are feeling insecure. It is important that the patient feels secure with the knowledge they gain from the caregiver.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The authors should have probably defined what they mean by security. According to the comments security can be confused with kindness.

4.43. Paper 43

1. Article Title
    a. Guidelines for teleradiology practice: results of the Tyrolean teleradiology pilot project
2. Research Questions
    a. Evaluate the effectiveness of a teleradiology solution
3. Security Issues
    a. How to secure that is being transmitted?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data has to be secure to maintain integrity and confidentiality to allow for good quality of care and patient privacy respectively.
8. Solution Proposed (or Results)
    a. Yes. Smart Cards and Biometric Identification
9. Solution tested (yes/no). If yes what were the results?
    a. Yes.
10. Limitation
    a. The authors should have defined a threat model. Smart cards and biometric identification cannot be the answer to all the threats that electronic data especially over the network can be vulnerable to.

4.44. Paper 44

1. Article Title
    a. The potential impact of home Telecare on clinical practice
2. Research Questions
    a. How do Telecare services change the nature of clinical practice?
3. Security Issues
    a. How to secure data that is being transmitted and ensure that it is being used ethically?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security
5. Threat Model
    a. None
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data has to be secure to maintain integrity and confidentiality to allow for good quality of care and patient privacy respectively.
8. Solution Proposed (or Results)
    a. Encryption
    b. SSL
    c. Secure Electronic Transaction (SET)
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. Security is not just technology. There are always other issues like training of staff that uses the system.

4.45. Paper 45

1. Article Title
    a. Network and data security design for telemedicine applications
2. Research Questions
    a. How to secure data generated by telemedicine services in an efficient and economic manner?
3. Security Issues
    a. There is a need to protect the confidentiality and integrity of the data generated and used in telemedicine services
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Security protocols, Data Confidentiality and Integrity
5. Threat Model
    a. Yes
        i. Message origin authentication
        ii. Secure Access management
        iii. Content integrity
        iv. Content confidentiality
6. Metrics (yes/no). If yes, what metrics?
    a. None
7. Significance of Problem
    a. Data has to be secure to maintain integrity and confidentiality to allow for good quality of care and patient privacy respectively.
8. Solution Proposed (or Results)
    a. Encryption
    b. Public key cryptography
    c. Symmetric key cryptography
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. Some of the solutions proposed in the paper might have been good

when the paper was written but are dated now. There is no proof given for the security of the key exchange protocol described in the paper.

4.46. Paper 46

1. Article Title
    a. Shaping the future: Needs and expectations of Telehealth Professionals
2. Research Questions
    a. Evaluating the perceptions and expectations of healthcare providers regarding Telecare.
3. Security Issues
    a. The perception of security and privacy issues due to telehealth amongst healthcare providers
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Privacy, Perception of Security
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. Sometimes telehealth services are perceived to be insecure that reduces the trust that the caregivers have in those services leading to underutilization and poor quality of care. Caregivers also need to be aware of the privacy and security risks that arise because of the novel technology.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The paper does not mention the kind of security and privacy issues in telehealth that would be different from traditional health care.

4.47. Paper 47

1. Article Title
    a. Making Grandma's Data Secure: A Security Architecture for Home Telemedicine
2. Research Questions
    a. How to develop a security solution that is user friendly but reliable?
3. Security Issues
    a. What are the problems in trying to find one size fit all security solution?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security, Authorization, Access Control, Physical Security, Auditing.
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Security solutions should not be generalized but targeted. It leads to better utilization of resources and also allows the system to be tailored so that it is more user friendly.
8. Solution Proposed (or Results)
    a. Password based login system
    b. Public Key Infrastructure
    c. Time based tokens
    d. IP filtering
    e. Virtual Private Network (VPN)
    f. Symmetric key cryptography
    g. Asymmetric key cryptography
    h. Firewalls
    i. Dedicated connections

9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The paper states the idea that security should be user friendly but some of the solutions proposed like a password based login system are not really user friendly, there could have been a discussion of alternatives like a pneumonic based login system.

4.48. Paper 48

1. Article Title
    a. Challenges to the implementation of Telemedicine
2. Research Questions
    a. What are the major obstacles in the dissemination of Telemedicine as an effective means of care-giving?
3. Security Issues
    a. What are the challenges in ensuring patient's right to privacy in Telemedicine?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security and Privacy
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Telemedicine is different from traditional care-giving. The use of technology introduces new risks in ensuring patient's right to privacy. Unless we address these risks telemedicine would probably not be very popular amongst patients or providers who might be held legally liable.
8. Solution Proposed (or Results)
    a. Password based login system
    b. Encryption
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The notion that encryption and passwords are enough for security is naïve. Telemedicine like IT needs proper security analysis.

4.49. Paper 49

1. Article Title
    a. Home Telecare and its discontents
2. Research Questions
    a. What are the major obstacles in the dissemination of Telecare as an effective means of care-giving?
3. Security Issues
    a. It is not easy to identify truly secure solutions in the market.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Confidentiality
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. It is not easy to gain knowledge about securing your systems especially for people in telemedicine who are more on the healthcare side rather than on the security side.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The paper does not explain why it is hard to find our about secure solutions for example it could have talked about the lack of standards in security.

4.50. Paper 50

1. Article Title
    a. Evolving Telemedicine/ehealth technology
2. Research Questions
    a. What are the emerging technologies that support telemedicine and what are the problems associated with them
3. Security Issues
    a. What are the challenges regarding security in Telemedicine due to introduction of new technology like telemedicine
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security and Privacy
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Security is a big issue in telemedicine and as technologies change the vulnerabilities change thus there is a constant need to revaluate the security solutions and their effectiveness.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. The paper talks primarily about WEP when it talks of wireless security. But its replacement WPA was already out when the paper was written. There was little discussion on other problems with wireless security like easy to mount DoS attacks.

4.51. Paper 51

1. Article Title
    a. Organizing Safety: Conditions for successful information assurance programs.
2. Research Questions
    a. What are the determinants that allow a successful implementation of information assurance programs compliant with HIPAA
3. Security Issues
    a. Organization with aggressive information assurance programs get breached because they tend to unwisely dedicate resources.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Training, Confidentiality, Integrity and Availability
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. The failure of information assurance program is disheartening. Failure might lead to less investment in information security since the stakeholder would assume that the risk levels remain the same with or without these programs. There is a need to revamp these programs by understanding why they fail.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. While the paper states the reasons for failure, they do not provide specific evidence to support their claim in terms of case studies or prior research.

4.52. Paper 52

1. Article Title
    a. A Web based Telemedicine system for diabetic Retinopathy Screening using digital Fundus photography
2. Research Questions
    a. Is telemedicine based retinopathy screening reliable?
3. Security Issues
    a. Secure transfer of data and images.
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Confidentiality and Integrity
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. Data integrity needs to be ensured for more reliable service while data confidentiality needs to be maintained to ensure patient's right to privacy.
8. Solution Proposed (or Results)
    a. SSL
    b. HTTPS
    c. Password based login system
9. Solution tested (yes/no). If yes what were the results?
    a. No, solution was not tested for security.
10. Limitation
    a. SSL and password based login systems is a myopic view of security.

4.53. Paper 53

1. Article Title
    a. Nationwide Telecare for Diabetes: A pilot implementation of the HOLON architecture
2. Research Questions
    a. Evaluation of a HOLON based implementation of a Telecare project.
3. Security Issues
    a. Secure transfer and storage of medical data
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Authorization, Authentication and Confidentiality
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Conversion of medical data from paper based format to electronic exposes it to new kinds of risk. These risks need to be addressed for legal compliance like HIPAA and to ensure patient trust.
8. Solution Proposed (or Results)
    a. SSL
    b. HTTPS
    c. Password based login system
9. Solution tested (yes/no). If yes what were the results?
    a. No, solution was not tested for security.
10. Limitation
    a. SSL and password based login systems is a myopic view of security.

4.54. Paper 54

1. Article Title
    a. Online Eye Care in Prisons in Western Australia
2. Research Questions
    a. Can similar quality of care be provided to the prison patient by using an online system rather than traditional on site visits?
3. Security Issues
    a. How to reduce the risk suffered when prisoners are transported from prisons to the doctor?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Security
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. Specialists are required to treat the patients in prisons many a times, however transportation induces the risk of escape from prison, this risk can be mitigated if the specialist can use data and images sent to them via telemedicine systems to make a diagnosis.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The solution is limited to eye care as of now. Prisoners would still need to be transported for other specialist doctors.

4.55. Paper 55

1. Article Title
    a. Teleradiology: results of a questionnaire of German Radiologists
2. Research Questions
    a. Evaluation of perception and awareness of teleradiology amongst German radiologists.
3. Security Issues
    a. How well do radiologists understand the data security issues with using Teleradiology?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security, Perception of Security
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. Yes. Percentages
7. Significance of Problem
    a. New technology introduces new risk to data. It is important that the doctors are aware of these risks so that they can take steps to mitigate them.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. The findings have not been reported in an articulate manner. Since the questionnaire has not been provided it is unclear if the participants understood the security risks or the tools used to mitigate them. There are no percentages reported to state how many people thought stronger security was required.

4.56. Paper 56

1. Article Title
    a. The legal and ethical aspects of telemedicine. 2: Data protection, security and European Law
2. Research Questions
    a. Electronic medical records are vulnerable to many more risks than the corresponding paper records. It is important to make entities responsible for protecting these records by making them legally liable.
3. Security Issues
    a. Who is legally liable for protecting medical data in electronic format?
    b. How can laws be used to mitigate threats to electronic medical records?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Data Security, Legal Liability
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. New technology introduces new risk to data. It is important that the stakeholders involved take steps to protect this data. One of the incentives for them to do this would be to make them legally liable.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. NA

4.57. Paper 57

1. Article Title
    a. Prison Telemedicine and Telehealth: Utilization in the United States: State and Federal Perceptions of Benefits and Barriers
2. Research Questions
    a. What is the level of usage of Telemedicine and telehealth services in corrections facilities across United States?
    b. What are the perceived benefits of these services?
    c. What are the barriers against the dissemination of these services?
3. Security Issues
    a. What are the security benefits of telemedicine and telehealth services?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Physical Security and Safety
5. Threat Model
    a. NA
6. Metrics (yes/no). If yes, what metrics?
    a. NA
7. Significance of Problem
    a. Telemedicine services provide a cost effective and more secure way of correctional facilities to deal with their patients. It is important to understand what exactly the perceived benefits and disadvantages are.
8. Solution Proposed (or Results)
    a. NA
9. Solution tested (yes/no). If yes what were the results?
    a. NA
10. Limitation
    a. It would be interesting if the prisoners were interviewed about their perceptions as well.

4.58. Paper 58

1. Article Title
    a. Meeting the challenges- the role of medical informatics in an ageing society
2. Research Questions
    a. How can medical informatics used to develop new and adapt existing assisted living environments for the elderly?
3. Security Issues
    a. What are the security implications of the new assisted living technologies?
4. Types of Security issues e.g. Privacy, Physical Safety
    a. Safety, Security, Accessibility and Availability
5. Threat Model
    a. No
6. Metrics (yes/no). If yes, what metrics?
    a. No
7. Significance of Problem
    a. New technology brings new risks and security vulnerabilities. It is important that they are mitigated to acceptable before these technologies are deployed in the market.
8. Solution Proposed (or Results)
    a. None
9. Solution tested (yes/no). If yes what were the results?
    a. No
10. Limitation
    a. There is no discussion of how security issues in smart homes are different from security in traditional care.

CHAPTER 5. DISCUSSION AND CONCLUSION

5.1. Discussion

In all, a total of 58 articles were found in 14 journals. There was no constraint on the date of publication. Some of these journals were publishing since 1994 or even before. 58 articles over 14 journals is a mean of about 4 articles for every journal. Spread over a decade, that is less than one article per year per journal. Journal of Telemedicine and Telecare published 14 articles in a single issue published in March 2009. Comparing those numbers gives an idea of how much the field of security is neglected in Telemedicine and Telecare. Figure 1 is a distribution of the number of articles by journal. If one takes into account journals that are exclusively marked for Telemedicine and Telecare, we have five journals and a total of 46 articles between them. That still means around nine articles per journal and around one article per year per journal (assuming a time span of a decade, however the time span is closer to two decades). This still means that security research is not given priority amongst Telemedicine and Telecare researchers.

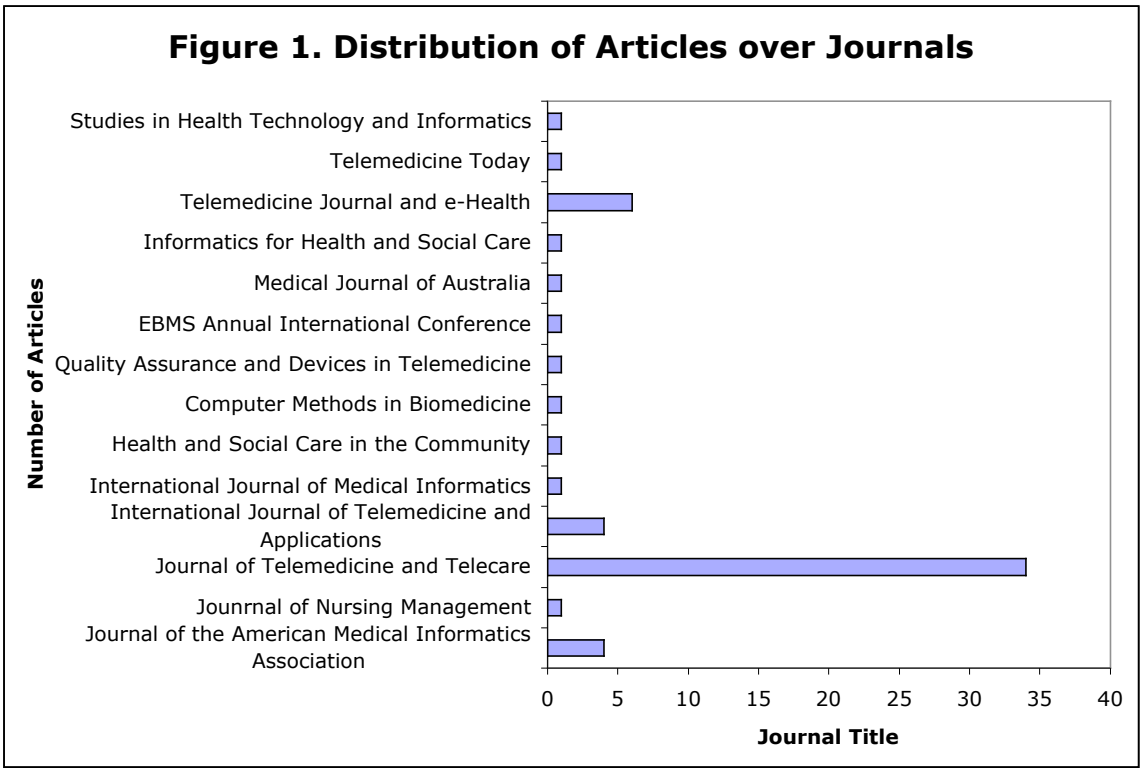

Figure 1: Distribution of Articles across Journals

If we look at the distribution of articles over the year, Figure 2, the graph seems to be left skewed and the number of articles seems to have increased in recent years. This definitely seems like a positive trend as it suggests that more researchers are looking at the security aspects of Telemedicine and Telecare services. However, the increase in the number of articles on security in Telemedicine might simply be a result of the increase the number of articles on Telemedicine.

Only six of the 58 articles studied were quantitative in nature, 13 were qualitative, and the rest were theory. This suggests that researchers are still struggling to come up with a hypothesis that they can test through quantitative or

quantitative methods. At the same time the papers that do use qualitative or quantitative methodology do not report some of the required details. Fifteen percent of the papers did not report the population size. This is however better than overall figures of Telemedicine which is 26% (Whitten et al., 2007). Fifty percent of the articles did not represent age range. Given that one of the barriers is supposed to be the reluctance of the elderly to adapt to technology this is an important statistic. Only 25% of the papers reported both the upper and the lower limit of the age range. Eighty percent of the papers did not report the age mean or median. Only one article reported a median and that made for 8% of the articles that reported either mean or median. Median is more resistant to outliers and thus should have been the statistic of choice.

For only 47% of the articles security was the primary issue. For 35% of the articles, security was a secondary issue. If a researcher considers security to be the primary issue, then at least one of the research questions should address security. When security is a secondary issue, security issues are not one of the research questions but it is discussed. For 17% of the articles security was mentioned merely as an afterthought.

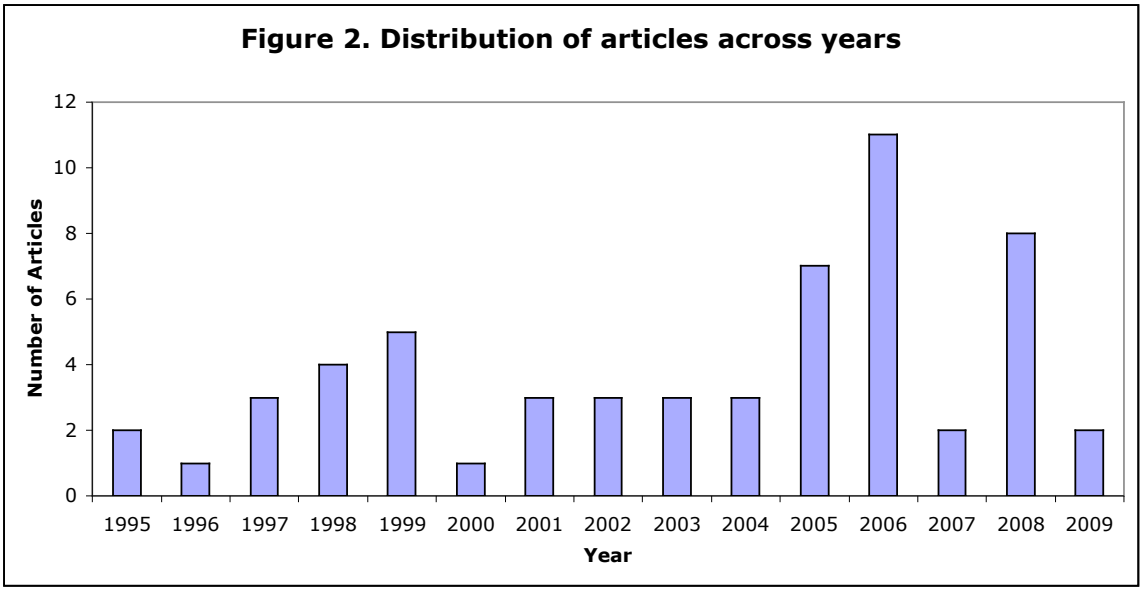

Figure 2: Distribution of Articles across years

The studies were conducted in different parts of the world. Figure 3. shows the distribution of studies across nations. The graph shows that 38% of the research on security is being done in the United States whose overall contribution to telemedicine research is 34% (Witten et al., 2007). On the other hand 42% of the research in security is being conducted in Europe. Europe accounts for 24% of the research in telemedicine overall (Whitten et al., 2007). These numbers seems to indicate that European researchers are taking security issues more seriously than their American counterparts. Of the 20 articles based in the US, only six mentioned HIPAA, even though all 20 of the articles dealt with information covered by this Act.

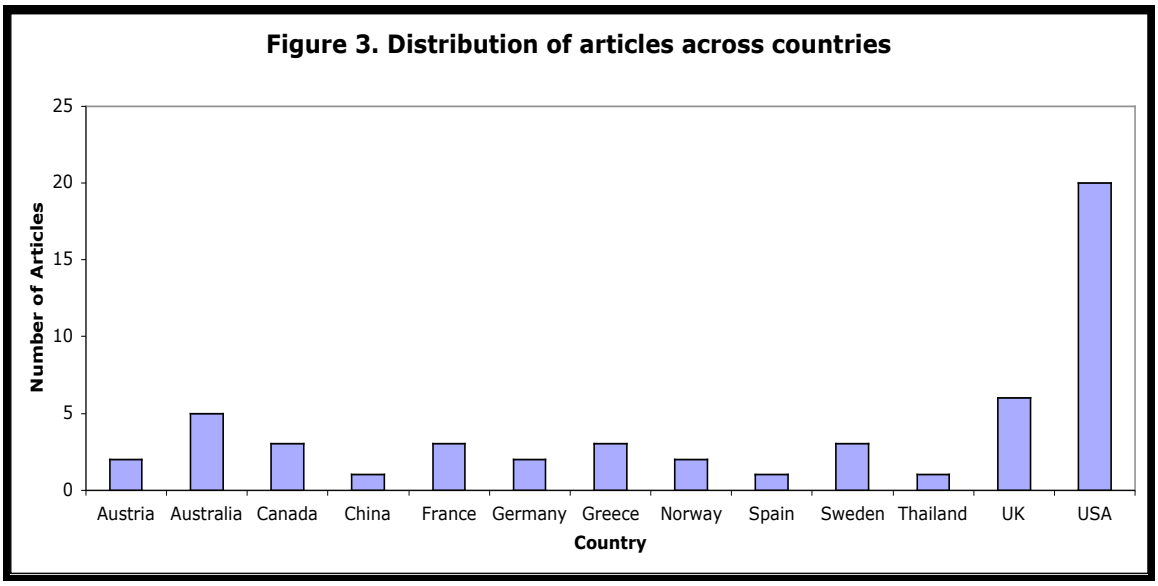

Figure 3: Distribution of Articles across countries

Seventy-six percent of the articles defined a security problem. 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. The importance of threat modeling cannot be over stressed (Schneier, 1996). No security solution can be all encompassing protecting the system against everything. Thus the articles need to report a threat model so that the reader would know what the solution is going to protect against.

There was a varied distribution when it came to kind of consumers these papers were addressing as well. Most of the research seems to be concentrated around the elderly and individuals suffering from diabetes. For both these groups security is an important issue. For example, in the cases of the elderly, timely intervention in the event of a fall is important (Lee et al., 2005). There is an increasing occurrence of Alzheimer in the elderly (Whitehouse, 2002). Thus they

should not be made to wear devices that make them stand out or they might become targets of crime (Lormel, 2001). Twelve and a half percent of the studies did not report the kind of consumers they were catering to. This seems to be an important oversight. Security solutions cannot be generalized. Different consumers will require different sensors and different services according to their condition thus, they would also require different levels/types of security. For example, physical safety is important for the elderly, but for individuals suffering from HIV/AIDS, privacy may be a bigger concern.

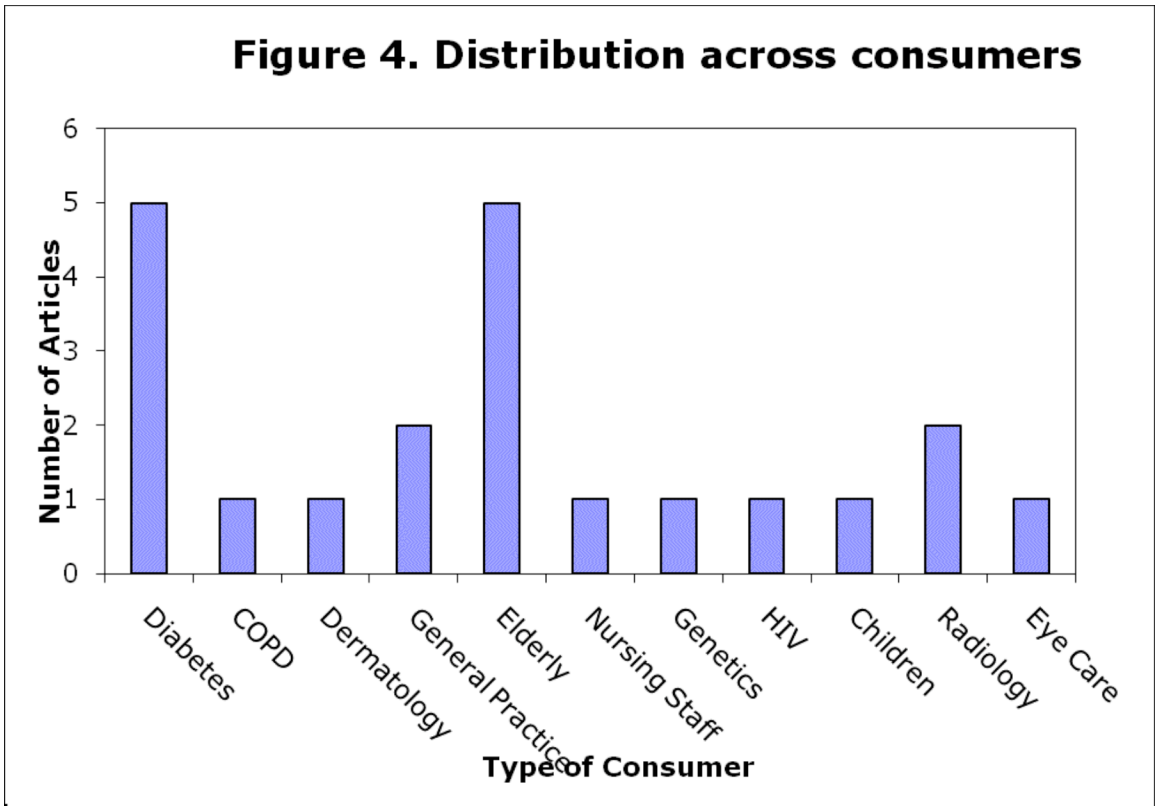

Figure 4: Distribution of Articles across Consumers

Two of the articles dealt with the use of Telemedicine/Telecare in prisons (Larsen et al., 2004; Yogesan et al., 2001). They give an interesting insight into how Telemedicine services can be used to solve existing security issues instead of being a security issue by themselves. One of the studies is conducted in Australia (Yogesan et al., 2001), while the other is conducted in USA (Larsen et al., 2004). Both these countries have large land area where transporting prisoners requiring medical attention over these large areas may lead to security problems. For example, the prisoners might escape while they are being transported to or from the prison to a medical facility. This can be mitigated to an extent by the use of telemedicine services. Now the prisoners can be diagnosed via data transmitted over the network. The healthcare provider can suggest an onsite visit in more serious cases.

Different articles catered to different security issues. Figure 5. gives a distribution of the number of articles for each security issue. The clear winners are Privacy and Data Security/Integrity. This suggests that the researchers in Telemedicine are not very familiar with the field of Information Security. Security issues should not be treated in isolation. Privacy is hard to maintain without addressing Authentication and Authorization. Merely three articles address training of personnel. This is an important area that needs to be addressed. One of the reasons of failure 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, but also the patients and other personnel that interact with the system directly or indirectly need to be trained.

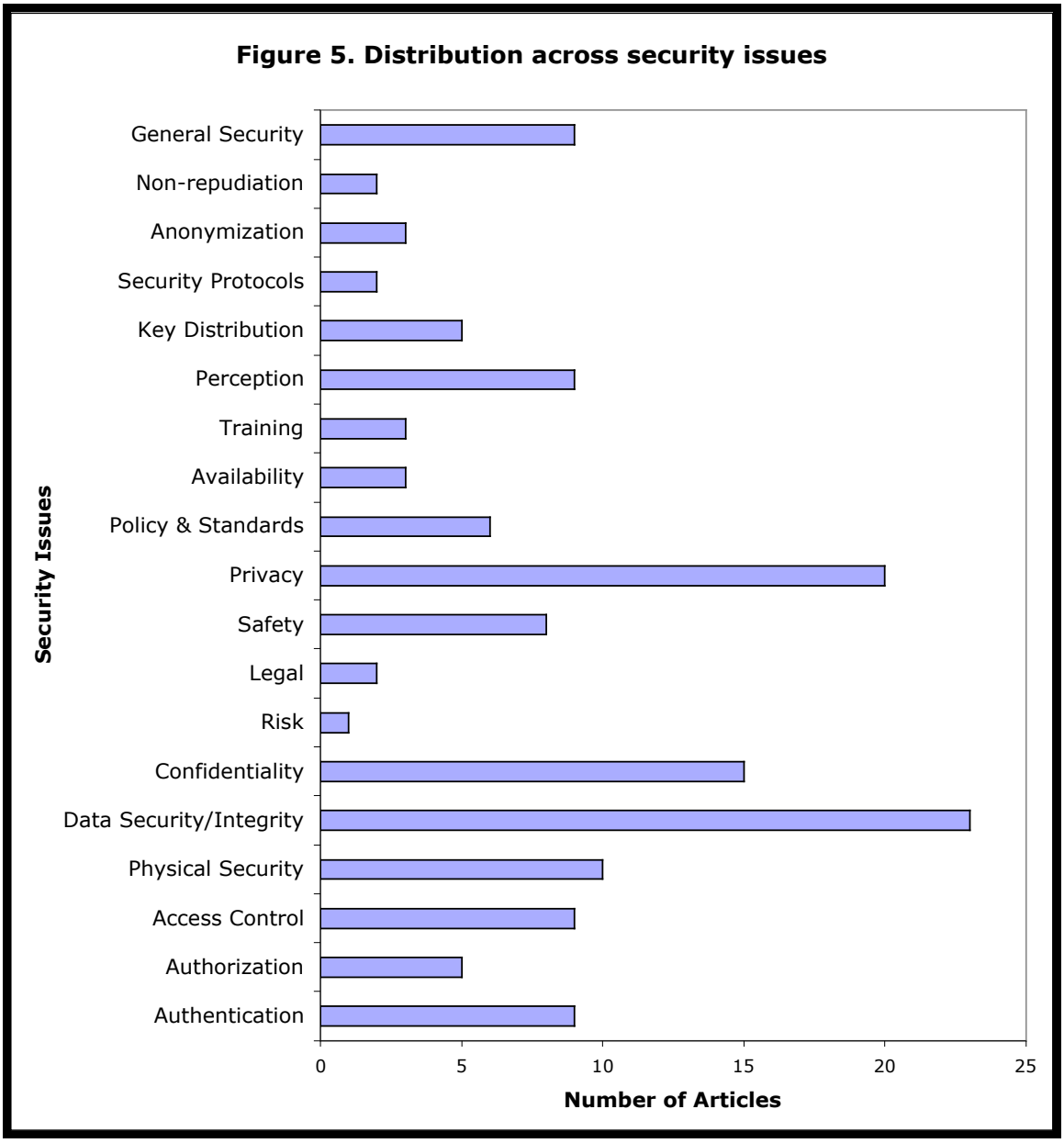

Figure 5: Distribution of Articles across Security Issues

A change in technology from traditional care giving to Telemedicine means that the attack vector also changes. All personnel need to be aware of

what these attacks might be. Most systems are vulnerable because the users do not use them correctly. It is important to train personnel to prevent other kinds of attacks like social engineering (Mitnick et al., 2002), if data security is to be ensured and privacy maintained which are the top two concerns of Telemedicine researchers.

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 (Broens et al., 2007). This is definitely an area to look into. Legal issues in telemedicine and telecare 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. However there is more reason to protect data. Stanberry (1998) notes, “leaking of information is not the only danger that teleconsultants face. There could be catastrophic consequences for the clinical care of a patient where the unauthorized interception of telemedicine transmissions gave rise to modifications that produced inaccurate or incomplete data. (p. 19)” Concurrently network related issues like packet dropping and jitter can also lower the quality of medical data being transmitted. The question of legal liability still stands. The only two papers (Stanberry, 1998; Wallace et al., 1999) that discuss legal liability were published in 1998 and 1999 and were conducted in UK, which suggests that this area is ignored by most researchers in the recent times in most countries.

To some extent, the question of legal liability can be dealt by policies and standards and by making sure that healthcare providers adhere to them. But research in this area is also disappointing. Only five articles addressed policy and standards. Policy and standards help in building confidence amongst the consumers and providers regarding the reliability and safety of the service. Savastano et al. (2008) note that certain biometric sensors might be seen to cause infectious, in case of touch based sensors, or can be seen to cause safety concerns in case of iris sensors that reflect light in the eye. Standardization would reduce the fear of using these technologies. Certain other technologies like RFID might raise privacy concerns. If a well-established standard is used, it would alleviate worries. Standardization also implies developers would repeatedly implement the same framework. This allows to borrow from previous implementations and improve on them.

Yellowlees et al (2006) also talk about standards, but their focus is on how standardization helps in quicker dissemination of technology. Cavallerano et al. (2005) talk about HIPAA compliance. Alexander (1996) talks about developing a nationwide privacy policy for health care data in Australia. None of the papers talks about HL7 even though 3 of the studies have been conducted in USA and UK, where HL7 is the standard for storing medical data. This oversight suggests that there is a lack of awareness about standards in the Telemedicine research community.

However no standards are better than bad standards. Makris et al (1997) use DES for encryption. This paper was published in 1997, however, the

algorithm was already broken in 1993 (Biham et al., 1993). Markis et al. (1997) also describe two authentication protocols. They do not provide a proof of security of either of the protocols. Neither of the protocols is referenced so it can be assumed that the authors constructed both the protocols themselves. However constructing 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 14 years after its publication even though the protocol had been proven secure using BAN logic (Needham et al., 1978; Lowe, 1995). The researchers used an insecure algorithm to encrypt and an unproven security protocols to communicate. This suggests that many researchers in Telemedicine are not familiar with research in security.

Another area that seems to be neglected is research on availability. Only three papers discuss availability (Collmann et al., 2004; Koch, 2006; Savastano et al., 2008). None of the papers discuss the importance of availability or the implications of lack of it. They do not mention any measures that can be used to ensure availability. This is an important issue, since it guarantees the reliability of the service.

Another important property is Non-repudiation. It implies that a person cannot deny responsibility for a certain transaction. This is important to maintain audit trails, since a personnel implicated by an audit should not be able to repudiate responsibility. Only two papers mention this property (Ferrante, 2005; Makris et al., 1997). Ferrante (2005) states that non-repudiation is necessary to

comply with HIPAA, while Markis et al (1997) state that non-repudiation is a basic property of open systems.

Some of the other areas also need more attention. For example key distribution is addressed only in five papers. This is an important issue since most systems need to distribute keys for encryption. Only two papers address anonymization. Overall, none of the security issues were adequately addressed. In general there seemed to be dearth of research in this field. The available research was lacking in providing a solution and a few articles that did, did not test them.

5.2. Conclusion

This study suggests that research in security in Telemedicine and Telecare services needs to be given more attention. Several papers (Huston 2005; Savastano et al., 2008) suggested that lack of security in these services would lead to poorer quality of care, lack of confidence in the services for both providers and consumers and cause legal liability. Earlier research (Huston, 1999a; Huston 1999b) also suggested that security is not the primary focus Telemedicine research community. But this needs to change if Telemedicine/Telecare services are to become widely acceptable (Broens et al., 2007).

LIST OF REFERENCES

LIST OF REFERENCES

Aas, I. H. M. (2008). Changes in the job situation due to telemedicine. *Journal of Telemedicine and Telecare, 8,* 41-47.

Absher, C. (2009). What does Assisted Living really cost? Retrieved on February 4, 2009 from HTTP://WWW.CAREPATHWAYS.COM/CTO9.CFM.

Alexander, M. (1996). Telemedicine in Australia. 2: The Health Communication Network. *Journal of Telemedicine and Telecare, 2,* 1-6.

Anciaux, N., Berthelot, M., Braconnier, L., Bouganim, L., Blache, M., Gardarin, G., et al. (2008). A Tamper-Resistant and portable Healthcare Folder. *International Journal of Telemedicine and Applications, 2008.*

Armstrong, N., Powell, J., Hearnshaw, H., & Dale, J. (2007). Design of a trial of Internet-based self-management for diabetes. *Journal of Telemedicine and Telecare, 13(1),* 1-2.

Arsand, E., Tufano, J. T., Ralston, J. D., & Hijortdahl, P. (2008). Designing mobile dietary management support technologies for people with diabetes. *Journal of Telemedicine and Telecare, 14,* 329-332.

Barlow, J., Singh, D., Bayer, S., & Curry, R. (2007). A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions. *Journal of Telemedicine and Telecare, 13,* 172-179.

Berg M. (1999). Patient Care information systems and health care work: a socialtechnical approach. *International Journal of Medical Information, 55,* 87-101.

Biham, E., & Shamir, A. (1993). *Differential Cryptanalysis of Data Encryption Standard.* London: Springer-Verlag.

Bolte, R., Walz, M., Lehmann, K. J., Hothom, T., Brill, C., Hothom, L., et al. (1998). Teleradiology: results of a questionnaire of German radiologists. *Journal of Telemedicine and Telecare, 4(1),* 69-71.

Botsis, T., Demiris, G., Pedersen, S., & Hartvigsen, G. (2008). Home telecare technologies for the elderly. *Journal of Telemedicine and Telecare, 14,* 333-337.

Broens, T., Veld, R., Vollenbroek-Hutten, M., Hermens, H., Halteren, A., & Nieuwenhuis, L. (2007). Determinants of Successful Telemedicine implementations: a literature study. *Journal of Telemedicine and Telecare, 13,* 303-309.

Buono, S., & Citta, S. (2007). Tele-assistance in intellectual disability. *Journal of Telemedicine and Telecare, 13*, 241-245.

Caceres, C., Gomez, E. J., Garcia, F., Gatell, J. M., & Pozo, F. (2006). An integral care telemedicine system for HIV/AIDS patients. *International Journal of Medical Informatics, 75,* 638-642.

Cavallerano, J., & Aiello, L., M. (2005). Emerging trends in ocular telemedicine: the diabetic retinopathy model. *Journal of Telemedicine and Telecare, 11,* 163-166.

Celler, B. G., Lovell, N. H., & Chan, D. K. Y. (1999). The potential impact of home telecare on clinical practice. *Medical Journal of Australia, 171,* 518-521.

Collman, J., Coleman, J., Sostrom, K., & Wright, W. (2004). Organizing Safety: Conditions for Successful Information Assurance Programs. *Telemedicine Journal and e-Health, 10(3),* 311-320.

Crowe, B. L., & McDonald G. (1997). Telemedicine in Australia. Recent Developments. *Journal of Telemedicine and Telecare, 3,* 188-193.

Dagtas, S., Pekhteryev, G., Cam, H., & Challa, N. (2008). Real-Time and Secure Wireless Health Monitoring. *International Journal of Telemedicine and Applications, 2008.*

Demiris, G., Edison, K., & Schopp, L. H. (2004). Shaping the future: Needs and Expectations of Telehealth professionals. *Telehealth Journal and e-Health, 10(2),* 60-63.

Dutch ministry of Health Welfare and Sport (VWS) (2004). *Health Care in an Ageing Society: A Challenge for all European Countries.* Retrieved February 3rd, 2009 from HTTP://WWW.MINVWS.NL/IMAGES/2508976C.DOC_TCM20-107926.PDF

Emerson, E. (2004). Cluster housing for adults with intellectual disabilities. *Journal of Intellectual & Developmental Disability, 29*(3), 187-197.

Erkert, T. (1997). High quality television links for home based support for the elderly. *Journal of Telemedicine and Telecare, 3(1),* 26-28.

Felce, D., Perry, J., Romeo, R., Robertson, J., Meek, A., Emerson, E., & Knapp, M. (2008). Outcomes and costs of community living: Semi-independent living and fully staffed group homes. *American Journal on Mental Retardation 113*(2), 87-101.

Ferreante, F. E. (2005). Evolving Telemedicine/eHealth Technology. *Telemedicine and e-Health, 11(3),* 370-383.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? Attitudes toward technological risks and benefits. *Policy Sciences, 9,* 127-152.

Fragopoulos A., Gialelis, J., & Serpanos, D. (2009). Security Framework for Pervasive Healthcare Architectures Utilizing MPEG-21 IPMP Components. *International Journal of Telemedicine and Applications, 2009.*

Gemmill, J. (2005). Network basics for telemedicine. *Journal of Telemedicine and Telecare, 11,* 71-76.

Giacomuzzi, S. M., Springer, P., Stoger, A., Dessl, A., Bucchberger, W., Bocher, G., et al. (1998). The Austrian Acedemic Computer Network and its usefulness for teleradiology. *Journal of Telemedicine and Telecare, 4(1),* 41-42.

Giakoumaki, A., Perakis, K., Tagaris, A., & Koutsouris, D. (2006). Digital Watermarking in Telemedicine Applications - Towards Enhanced Data Security and Accessibility. Proceedings from EMBS' 06: *The 28th IEEE EMBS Annual International Conference.* New York, USA: IEEE.

Gururajan, R., Moloney, C., & Soar, J. (2005). Challenges for implementing wireless hand-held technology in health care: views from selected Queensland nurses. *Journal of Telemedicine and Telecare, 11(2),* 37-38.

Haigh, K. Z. & Yanco, H. A. (2002). Automation as Caregiver: Survey of issues and Technologies. Proceedings of the AAAI-02 Workshop: *Automation as caregiver, 39-53*. Menlo Park, CA: AAAI Press.

Harnett, B. (2006). Telemedicine systems and telecommunications. *Journal of Telemedicine and Telecare, 12,* 4-15.

Harris, G. (1999). Home Telecare and its discontents. *Telemedicine Today, 7(4),* 27-35.

Hawes, C. (2002). *Elder abuse in residential long-term care facilities: What is known about prevalence, causes and prevention.* Retrieved February 19, 2009 from HTTP://FINANCE.SENATE.GOV/HEARINGS/TESTIMONY/061802CHTEST.PDF

Horton, K. (2008). The use of telecare for people with chronic obctructive pulmonary disease: Implication for management. *Journal of Nursing Management, 16,* 173-180.

Huston, J. L. (1999a). Managing telehealthcare information. *Journal of Healthcare Informatics Management, 13(4),* 49-58.

Huston, J. L. (1999b). Telemedical record documentation: a preliminary survey. *Journal of Telemedicine and Telecare, 5(1),* 6-8.

Huston, J. L. (2005). Information governance standards for managing e-health information. *Journal of Telemedicine and Telecare, 11(2),* 56-58.

Jones, P. C., Silverman, B. G., Athanasoulis, M., Drucker, D., Goldberg, H., Marsh, J., et. al. (1998). Nationwide Telecare for Diabetics: A Pilot Implementation of the HOLON Architecture. *Proceedings of the AMIA symposium,* 346-350.

Koch, S. (2006). Meeting the challenges – the role of Medical Informatics in an Ageing Society. *Studies in Health Technologies Informatics, 124,* 25-31.

Larson, D., Stamm, B. H., Davis, K., & Magaletta, P. R. (2004). Prison Telemedicine and Telehealth Utilization in the United States: State and Federal Perceptions of the Benefits and Barriers. *Telemedicine Journal and e-Health, 10(2),* 81-89.

Lee, T., & Mihailidis, A. (2005). An intelligent emergency response system: preliminary development and testing of automated fall detection. *Journal of Telemedicine and Telecare, 11,* 194-198.

Lindberg, D. A. B., & Humphreys, B. L. (1995). The High-Performance Computing and Communications Program, the National Information Infrastructure, and Health Care. *Journal of the American Medical Informatics Association, 2,* 156-159.

Linke, S., Harrison, R., & Wallace, P. (2005). A Web-based intervention used in general practice for people with excessive alcohol consumption. *Journal of Telemedicine and Telecare, 11(1),* 39-41.

Loera, J. A. (2008). Generational Differences in Acceptance of Technology. *Telemedicine and e-Health, 14(10),* 1087-1090.

Lormel, D. M. (2001). Testimony of Dennis M. Lormel. Retrieved on March 30, 2009 from HTTP://WWW.QUACKWATCH.ORG/01QUACKERYRELATEDTOPICS/HEARING/FBI.HTML

Lowe, G. (1995). An attack on the Needham-Schroeder Public Key Authentication Protocol. Retrieved on March 30, 2009 from HTTP://WEB.COMLAB.OX.AC.UK/PEOPLE/GAVIN.LOWE/SECURITY/PAPERS/NSPKP.PS

Malasanos, T., Patel, B., Klein, J., & Burlingame, J. (2005). School nurse, family and provider connectivity in the FITE diabetes project. *Journal of Telemedicine and Telecare, 11(1),* 76-78.

Manes, S. (2007). Dim Vista. Retrieved on February 10, 2009 from HTTP://WWW.FORBES.COM/FORBES/2007/0226/050.HTML

Markris, L., Argiriou, N., & Strintzis, M. G. (1997). Network and data security design for telemedicine applications. *Medical Informatics, 22(2),* 133-142.

Malasanos, T. H., Burlingame, J. B., Youngblade, L., Patel, B., D. & Muir, A. B. (2005). Improved access to subspecialist diabetes care by telemedicine: cost savings and care measures in the first two years of the FITE diabetes project. *Journal of Telemedicine and Telecare, 11(1),* 74-76.

Mao, Y., Zhang, Y., & Zhai, S. (2008). Mobile phone text messaging for pharmaceutical care in a hospital in China. *Journal of Telemedicine and Telecare, 14,* 410-414.

Mitnick K., & Simon W. (2002). *The art of deception: Controlling the human element of Security.* Jon Wiley & Sons.

Needham, R., & Schroeder, M. (1978). Using encryption for authentication in large computer networks. *Communications of the ACM, 21(12),* 993-999.

Nerenberg, L. (2002). Caregiver stress and Elder Abuse. Retrieved on February 11, 2009 from HTTP://WWW.NCEA.AOA.GOV/NCEAROOT/MAIN_SITE/PDF/FAMILY/CAREGIVER.PDF

Nilsson, C., Ohman, M., & Soderberg, S. (2006). Information and communication technology in supporting people with serious chronic illness living at home - an intervention study. *Journal of Telemedicine and Telecare, 12,* 198-202.

Pappa, D., Telonis, P., & Stergioulas, L. K. (2006). Management of medicines information for patient safety. *Journal of Telemedicine and Telecare, 12(1),* 34-36.

Pervical J., & Hanson J. Big Brother or Brave New World? Telecare and its implications for older people's independence and social inclusion. *Critical Social Policy, 26(4),* 888-909.

Pettersen, S., Uldal, S. B., Baardsgard, A., Amundsen, M., Myrvang, R., Nordvag, D., et al. (1999). The North Norwegian Health Net. *Journal of Telemedicine and Telecare, 5(1),* 34-36.

Poulsen, K. (2008). Hackers assault epilepsy patient via computer. Retrieved on February 10, 2009 from HTTP://WWW.WIRED.COM/POLITICS/SECURITY/NEWS/2008/03/EPILEPSY

Quantin, C., Allaert, F., Avillach, P., Fassa, M., Riandey, B., Trouessin, G., et al. (2008). Building Application-Related Patient Identifiers: What Solution for a European Country? *International Journal of Telemedicine and Applications, 2008.*

Rialle, V., Lamy, J., Noury, N., & Bajolle, L. (2003). Telemonitoring of patients at home: a software agent approach. *Computer Methods and Programs in Biomedicine, 72,* 257-268.

Sanders, J. H., & Bashshur, R. L. (1995). Challenges to the implementation of Telemedicine. *Telemedicine Journal, 1(2), 115-123.*

Savastano, M., Hovsto, A., Pharow, P., & Blobel, B. (2008). Identity-management factors in e-health and telemedicine applications. *Journal of Telemedicine and Telecare,14,* 386-388.

Schneier, B. (1996). Why Cryptography is harder than it looks. Retrieved on March 30, 2009 from HTTP://INSECURE.ORG/STF/WHYCRYPTO.HTML

Schneier, B. (2005). Insider threat statistics. Retrieved on February 10, 2009 from HTTP://WWW.SCHNEIER.COM/BLOG/ARCHIVES/2005/12/INSIDER_THREAT.HTML

Sinyee (2008). Intel processors transistor count. Retrieved on February 10, 2009 from HTTP://WWW.SWIVEL.COM/DATA_SETS/SHOW/1011714.

Sixsmith, A. J. (2000). An evaluation of an intelligent home monitoring system. *Journal of Telemedicine and Telecare, 6,* 63-72.

Soegner, P., Rettenbacher, Th., Smekal, A., & Nedden, D. (2003). Guidelines for teleradiology practice: results of the Tyrolean teleradiology pilot project. *Journal of Telemedicine and Telecare, 9(1),* 48-50.

Stalker, H. J., Wilson, R., McCune, H., Gonzalez, J., Moffett, M., & Zori, R. T. (2006). Telegenetic medicine: improved access to services in an underserved area. *Journal of Telemedicine and Telecare, 12,* 182-185.

Stanberry, B. (1998). The legal and ethical aspects of telemedicine. 2: Data protection, security and European Law. *Journal of Telemedicine and Telecare, 4,* 18-24.

Stancliffe, R. J. Lakin, K. C. Doljanac, R. Byun, S., Taub, S. & Chiri, G. (2007). Loneliness and living arrangements. *Intellectual and Developmental Disabilities. 45*(6), 380-390.

Stell, A., Sinnott, R., & Ajayi O. (2006). Secure Federated Data Retrieval in Clinical Trials. *Telehealth Conference.*

Starren J., Hripcsak, G., Sengupta, S., Abbruscato, C. R., Knudson, P. E., Weinstock, R. S., et al. (2002). Columbia University's Informatics for Diabetes Education and Telemedicine (IDEATel) Project: Technical Implementation. *Journal of the American Medical Informatics Association, 9(1),* 25-36.

Starren J., Sengupta, S., Hripcsak, G., Ring, G., Klerer, R., & Shea, S. (2001). Making Grandma's data secure: A Security Architecture for Home Telemedicine. *Proceeding of American Medical Informatics Association Annual Symposium,* 657-661.

Strauss, J. S., Felten, C. L., Okada, D. H., & Marchevsky, A. M. (1999). Virtual Micrpscopy and public-key cryptography for Internet telepathology. *Journal of Telemedicine and Telecare, 5,* 105-110.

Swartz, D. (1998). TECHTALK: Security of Internet-based telemedicine systems. Retrieved on February 2, 2009 from HTTP://WWW2.TELEMEDTODAY.COM/ARTICLES/TECHTALK.SHTML

Tanriverdi H., & Iacono C. (1998). Knowledge barriers to diffusion of telemedicine. Proceeding from ICIS '98: International Conference on Information Systems. Atlanta, GA: Association for Information Services, 1998;39-50.

Thompson, K. (1984). Reflections on trusting trust. *Communications of the ACM, 27(8),* 761-763.

Tigerstrom, B. (2000). Current developments in Canadian privacy and information law: implications for telehealth. *Journal of Telemedicine and Telecare, 6(2),* 83-85.

US Department of Health and Human Services (2006). *Prevalence of Selected Chronic Conditions.* Retrieved February 3, 2009 from HTTP://WWW.HHS.GOV.

Vincent, D. S., Berg, B. W., Hudson, D. A., & Chitpatima, S. T. (2003). International medical education between Hawaii and Thailand over Internet2. *Journal of Telemedicine and Telecare, 9(2),* 71-72.

Wahlberg, A. C., & Wredling, R. (2001). Telephone advice nursing – callers' experiences. *Journal of Telemedicine and Telecare, 7,* 272-276.

Wallace, S., Sibson, L., Stanberry, S., Waters, D., Goodall, P., Jones, R., et al. (1999). The legal and risk management conundrum of Telemedicine. *Journal of Telemedicine and Telecare, 5(1),* 8-9.

Wei, J. C., Valentino, D. J., Bell, D. S., & Baker, R. S. (2006). A Web-based Telemedicine System for Diabetic Retionpathy Screening Using Digital Fundus Photography. *Telemedicine and e-Health, 12(1),* 50-57.

Whitehouse, P., Marling, C., & Harving R. (2002). Can a computer be a caregiver? Proceedings of the AAAI-02 Workshop: *Automation as caregiver, 103-107*. Menlo Park, CA: AAAI Press.

Whitten, P., Johannessen, L., Soernsen, T., Gammon, D., & Mackert, M. (2007). A systematic review of research methodology in telemedicine studies. *Journal of Telemedicine and Telecare, 13,* 230-235.

Xiao, Y., Shen, X., Sun, B., & Cai, L. (2006). Security and Privacy in RFID and Applications in Telemedicine. *IEEE Communications Magazine, 44(4),* 64-72.

Yellowlees, P., & Harry, D. (2006). Standards for data collection and monitoring in a telemedicine research network. *Journal of Telemedicine and Telecare, 12(2),* 72-76.

Yogesan, K., Henderson, C., Barry, C. J., & Constable, I. J. (2001). Online Eye care in prisons in Western Australia. *Journal of Telemedicine and Telecare, 7(2),* 63-64.

Young, N. L., Barden, W., McKeever, P., Dick, P. T., & The Tele-HomeCare Team (2006). Taking the call-bell home: a qualitative evaluation of Tele-HomeCare for Children. *Health and Social Care in the Community, 14(3),* 231-241.