Detecting the Infringement of Personally Identifiable Information of the Elderly

Rebecca Rogers [1], Edward Apeh [1], and Christopher Richardson [1]

[1]Faculty of Science and Technology (SciTech),
Bournemouth University,
Poole House, Talbot Campus,
Fern Barrow,
Poole BH12 5BB
{rrogers1, eapeh, cjrichardson}@bournemouth.ac.uk

Abstract

Socio-technical systems are generally designed to be functional and easy to use by a cross-section of society, including the elderly. The elderly, by their nature, are physically, emotionally and financially vulnerable and are therefore more susceptible to be exploited. This makes the socio-technical systems that are designed for their use, and through which their personal information flows, highly attractive to hackers and fraudsters. Much work has been done in designing socio-technical systems so they are functional and easy to use by the elderly. However, very little work has been done to secure the data that is collected, processed, stored and transmitted by these socio-technical systems. Using human factors approaches, this paper proposes a complex socio-technical system for monitoring, tracking and the early detection of the infringement of personally identifiable information of the elderly. In particular it uses personas to describe the interaction between the elderly and these complex socio-technical systems, with the goal of highlighting the problem of data loss and misuse. It also analyses and presents how the proposed system monitors, detects and reports the infringement of personally identifiable information using soft systems techniques.

Keywords: human factors; soft systems methodology; vulnerability; elderly; digital watermarks

1. Introduction

The interaction of the elderly with socio-technical systems tends to be different from other demographics within society. Over the years, to facilitate and enhance the interaction of the elderly with socio-technical systems, much work has been undertaken using human factors techniques to design and implement systems that are functional and easy for the elderly to use. Such systems have become even more crucial now that, due to rising life expectancy and declining fertility rates, the number of older people, many of whom have significant wealth and disposable income, is on the increase. In addition to this, more and more of the services regularly accessed by the elderly (including governmental and non-governmental) are now being moved onto cyber-space based socio-technical systems.

Research using Human Factors techniques in recent years has been directed towards meeting the legal, moral and economic requirements of tackling the challenge of providing more functional and accessible socio-technical systems for the elderly. The research work and findings using human factors techniques have helped to advance the design and development of socio-technical systems within all areas including healthcare, public services and retail. These developed systems have helped support elderly users in overcoming their fears of using technical systems and enabling them to accept and use technological aids and mobile devices with more confidence [1]. For example; F. Newell [2] used cognitive analysis to design and develop an email and web-browser system for the elderly for whom the internet was an 'alien territory'; M. Kalviainen [3] used the results from ethnographic research to propose solutions for new services and infrastructure for public authorities where the elderly themselves were used as active content providers working in collaboration with external businesses and S. Kurniawan and P. Zaphiris carried out usability studies on elderly Web users to evaluate the usefulness of guidelines for Web design targeted at the elderly [4].

However, very little work has been done in terms of securing the data of the elderly within these socio-technical systems. Socio-technical systems by their very nature are complex interactions between humans and complex infrastructures. A key driver of these complex interactions is trust [5]. In our brave new world where these socio-technical interactions are conducted more and more online, the trust boundaries are becoming blurred. Data which used to be collected, processed, stored and owned by single entities is now shared by disparate agencies and organisations. While this allows for collaboration and sharing of information and knowledge among entitles who otherwise would not have been able to collaborate, it leads to situations of insecurity, especially when the data is shared with an entity with no authorisation to view or use it. This is even more so when there is no overarching owner or overseer of data collection, processing, storage and sharing as is the case with modern-day socio-technical systems.

The vulnerability of this complex interaction between humans and complex infrastructure is even more heightened when it comes to the elderly. As the population of the elderly increases and as they become more reliant on agencies for their health, care and general day to day activities, more and more of their personal data is collected, stored and shared. The elderly are therefore seen as being most

vulnerable not just in terms of their physical frailty but also as an easy target for exploitation and fraud. Furthermore, not only is their data vulnerable when it is in their ownership, this vulnerability increases when it is shared or transferred across the socio-technical systems they interact with. For example, there have been several reports about the data of elderly members of society being stolen, lost or misused including incidents of Doctors sharing clinical notes via whatsapp [6], USB device with unencrypted data lost by health service provider employee [7] and a Laptop with unencrypted patient data stolen from a GP [8]. If these recent reports of elderly data misuse and abuse is anything to go by, the collection and sharing of their data is not treated with the same level of care that is required for a highly valuable and vulnerable information asset.

This paper uses human factors techniques to describe the problem of elderly personal data infringement and proposes a solution by way of digital watermarks for tracking the personally identifiable information of the elderly and early detection of the infringement of that information. The rest of this paper is structured as follows; section 2.0 describes the complex interaction between the elderly and their socio-technical systems using a rich picture. It presents the flow of information and describes in detail the elderly personas and the various cyber personas they interact with. The point of potential data losses are also highlighted and described. Section 3.0 then presents the proposed system for tracking and early detection of elderly personal information infringement using soft systems techniques. The paper concludes in section 4.0 with a conclusion which includes a summary and recommendations for future work.

2. Complex interaction between the elderly and socio-technical systems

The complex interaction of the elderly with a complex infrastructure has become easier in recent years with the development and provision of easy to use functionality and accessibility. However, trust of socio-technical systems in terms of the Fear, Uncertainty and Doubt (FUD) contagion still persist (and in some cases is on the increase) in the interaction between the elderly and socio-technical systems [6]. This lack of trust is further exacerbated by the increase in cases of reported data breaches and personal data infringement [7]. These issues, combined with the general distrust that comes from the lack of understanding of the role of technology and its functions [8], have shown that socio-technical systems do not only need to consider functionality and usability but also security in order to gain and maintain the trust of the elderly. The rich picture in Figure 1, shows the flow of personally identifiable information belonging to the elderly and highlights the potential points of data loss.

3. The flow of personally identifiable information of the elderly in socio-technical systems

Typically, the first point of contact for the elderly tends to be agencies such as, banks, health care providers, government agencies, etc. who collect and store the information within a secured information infrastructure. Such agencies are regulated by way of policies and procedures for governance, risk and compliance which they are required by law to adhere to. However, the need for information sharing for collaborative reasons, which is facilitated by modern society's infrastructure, tends to lead to sometimes unintended sharing of data. This inevitably puts the data in the hands of perpetrators of fraudulent activities. In order to represent the complex socio-technical problem, I have used a rich picture in Figure 1, to show a typical flow of an elderly individual's information as described by Checkland [12].

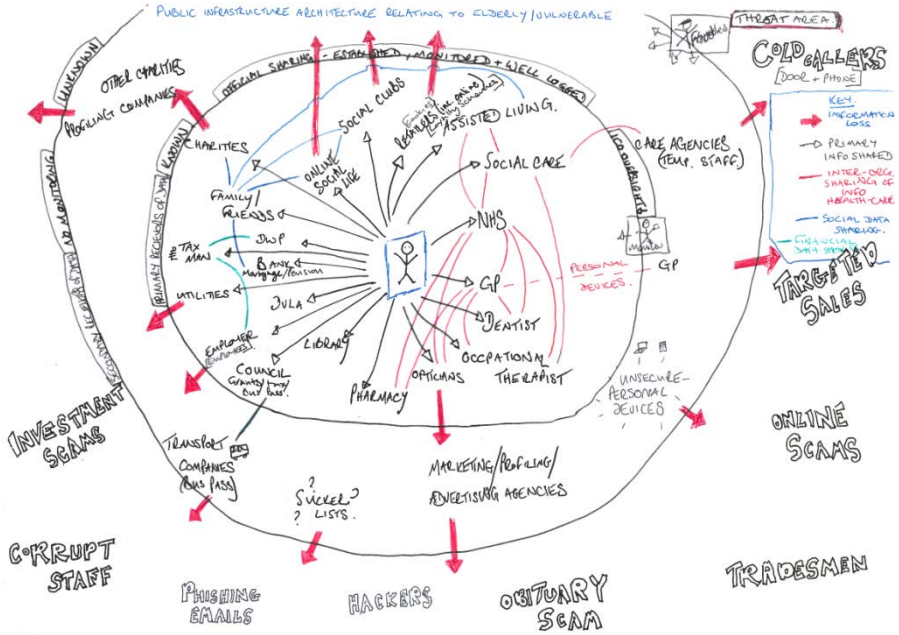

Figure 1: Rich Picture of a Typical Socio-Technical System of the Elderly

The rich picture in Figure 1, highlights the following:

- The flow of personally identifiable information from the elderly person to the primary organisations and agencies they have dealings with.
- The flow of personally identifiable information between the primary organisations and agencies which have dealings with the elderly person.
- Potential points for misuse or loss of the personally identifiable information.

- Points where information could be shared with organisations or entities which fall outside the trusted primary group.
- Threats from external fraudsters, intent on accessing the personally identifiable information and using it for criminal purposes.

Furthermore, it can be seen from the rich picture in Figure 1, that information tends to be duplicated and shared frequently within the inner circle of trusted organisations. While the data is being shared within this trusted inner circle, it is often possible to track and monitor the information, however more and more frequently it tends to find its way to individuals or groups for whom the data was not originally intended, the outer circle (or untrusted organisations). This could happen for a variety of reasons and is often a necessity due to, for example, care needs of the individual. All too frequently the information moves into the outer circle due to bad information management where individuals within these trusted organisations use personal devices and accounts to share the information. Once outside the trusted inner circle, where it is harder to track and monitor its use, it is used by unscrupulous and untrustworthy parties to target the individual, most often for some form of financial fraud.

3.1 The elderly Persona in the socio-technical system

As shown in the rich picture, the elderly personas in a socio-technical system tend to share information in a socio-technical system for various reasons with well-established and trusted entities such as family, healthcare providers and financial institutions. This personal information is then collected, processed, stored and shared as necessitated by the social needs (e.g. healthcare) of the elderly personas. There is therefore a high level of trust at this point of interaction with the socio-technical system. Appendix A provides an example of a typical elderly persona.

As the personal information moves from the first point of contact to second and third parties, the trust levels from the perspective of the elderly persona diminishes (subconsciously or otherwise) as they are no longer in control of who is accessing, processing and sharing their data.

3.2 Trusted personas within the socio-technical system

As can be seen from the Rich Picture in Figure 1, there are well established and approved channels of information flow between organisations which have dealings with the elderly. Such organisations strictly adhere to the data protection principles outlined in the data protection act which is overseen by the Information Commissioners Office. These organisations are legally obliged to protect that information they handle and store about identifiable, living people.

Under the Data Protection Act, they must [9]:

- only collect information that they need for a specific purpose;

- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as they need, and only for as long as they need it; and
- allow the subject of the information to see it on request.

Appendix B provides an example persona of a person working within a trusted organisation who strives to adhere to the rules outlined in the Data Protection Act and is overseen stringently by the Information Commissioners Office.

3.3 Un-trusted persons within the socio-technical system

It can also be seen from the Rich picture in Figure 1, that there are instances where information is shared with parties who require the information in order to undertake required tasks for the elderly but who fall outside of the known, approved and trusted group of organisations. It is this point that the risk of data loss and infringement is at its highest.

Appendix C provides an example persona of a person working within a perceived un-trusted organization who may have less control over the storage and use of its data and potentially does not have the resources to fully adhere to the Data Protection Act.

3.4 The data states of personally identifiable information of the elderly

The personally identifiable information of the elderly can be secured, monitored and tracked through the various stages of data states, i.e. data in use (process), data at rest (storage) and data in motion (transfer) [10].

Data is usually collected and used by organisations to perform a required task or for the purpose of meeting an obligation. In the case of the elderly, this could be the dispensing of drugs based on the diagnosis obtained from test results or identifying the course of physical therapy based on the information collected during a visit to a hospital after a fall.

Data security techniques such as encryption can be used to secure this data however it typically needs to be decrypted in order to be processed. If the receiver of the data has the encryption key, their systems tend to suffer performance issues in the decryption process and if the key is not available to the recipient of the data, it is virtually unusable. For example, if a ciphertext is incorporated in a socio-technical system such as a healthcare database application some of its features such as search, sort and index functions become inefficient without additional advanced keyword search schemes in place [11]. This highlights the problem of the balance between security and performance [12]. Custodians of personally identifiable information of the elderly tend to therefore be reluctant to encrypt personal data unless perceived as absolutely necessary. This also applies to other data hashing security techniques such as digital signatures as well as security mechanisms such as defense-in-depth which all affect performance by increasing latency [13].

These strong security approaches have the same effect on data at rest on which information is stored on file servers and information repositories such as exchange servers. Moreover, while security techniques like encryption can make it difficult for stolen data to be accessed, using these strong security techniques do not help in determining the point at which data has been infringed particularly in the case where information sent between trusted entities is intercepted by an untrusted entity.

Digital watermarking can however be used to monitor and track data in motion i.e. data sent over networks as well as data at rest and in use.

A digital watermark is digital data that can be embedded into all forms of data [14]. Special software is available for embedding imperceptible information via subtle changes to the data of the original digital content. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, thus facilitating data tracking and actions surrounding that data.

Because digital watermarking is a passive protection tool, i.e. it just marks data, but does not degrade it or control access to the data, it is therefore necessary that it is used in conjunction with other data protection techniques such as encryption, IPsec, digital certificates, digital signatures, etc. when the data is transmitted to un-trusted personas.

For the purpose of this paper, digital watermarks provide a mechanism for monitoring and tracking the data as it moves from within the trusted circle to its fringes. This ability of the proposed system to monitor and track the data within the trusted circle allows for the efficient operational functionality and accessibility of systems without the bottleneck that would otherwise be caused by intensive security of data such as excessive encryption among trusted personas.

This feature also allows for security protection techniques that affect the operation of socio-technical systems to be applied to the entities at the fringes of-and-beyond the trusted circle. This will mean, for example using the rich picture in Figure 1, that the encryption and security at the point of transmitting data from a primary healthcare provider within the trusted circle to a third party care provider at the fringe of the trusted circle would be stronger than the data when it is transmitted from the elderly person to the primary healthcare arena.

4. The proposed system for tracking and early detection of elderly personal information infringement using soft systems techniques

The previous section used situational awareness by way of personas to describe the problem space for the early detection of the infringement of personally identifiable information of the elderly, this section will present the proposed system using soft systems methodology.

4.1 Root definition

To assist in reducing the complexity and in the identification of the areas of concern of the proposed system for early detection of the infringement of personally identifiable information of the elderly a root definition is stated below. Hicks [15] states that a root definition should be ‘a concise verbal description of the system'. Checkland and Scholes state that it should ‘express the core purpose of a purposeful activity system and express the core or essence of the perception to be modelled [16].

‘A system to monitor, track and report on the transmission of the personal identifiable information of the elderly by means of digital watermarking and appropriate levels of data encryption in order to increase the trustworthiness of socio-technical systems amongst the elderly.’

4.2 CATWOE

Furthermore, to provide a deeper understanding of the problem space the CATWOE elements of the root definition are provided below.

C ‘customers’: The elderly person whose personally identifiable information is collected, stored and shared within the system.

A ‘actors’: The people who collect, store and share ‘C’s’ personally identifiable information and those who misuse it whether accidently or deliberately.

T ‘transformation process’: Improves the trustworthiness of a socio-technical system by applying the appropriate data hashing and digital watermarking security techniques to data that is collected, stored and transmitted between trusted parties.

W ‘worldview’: The need to improve the trustworthiness of socio-technical systems used by the elderly within society in order to align the need for security with the inherent functionality and usability provided by HCI systems.

O ‘owners’: The system owner is anyone within this proposed socio-technical system who collects, stores or transmits the personally identifiable information.

E ‘environmental constraints’: Security risks surrounding the individuals and organisations in which the proposed complex socio-technical system operates as well as access control procedures, staff training and awareness, security culture and multi-agency collaboration.

4.3 Conceptual Model

In order to provide an abstract representation of the activity within the proposed system described in the root definition in section 3.1, a conceptual model is used. According to Checkland [17], a conceptual model should include “what” activities happen in the system. Figure 2, depicts the conceptual model developed to

describe the proposed system for early detection of personally identifiable information of the elderly.

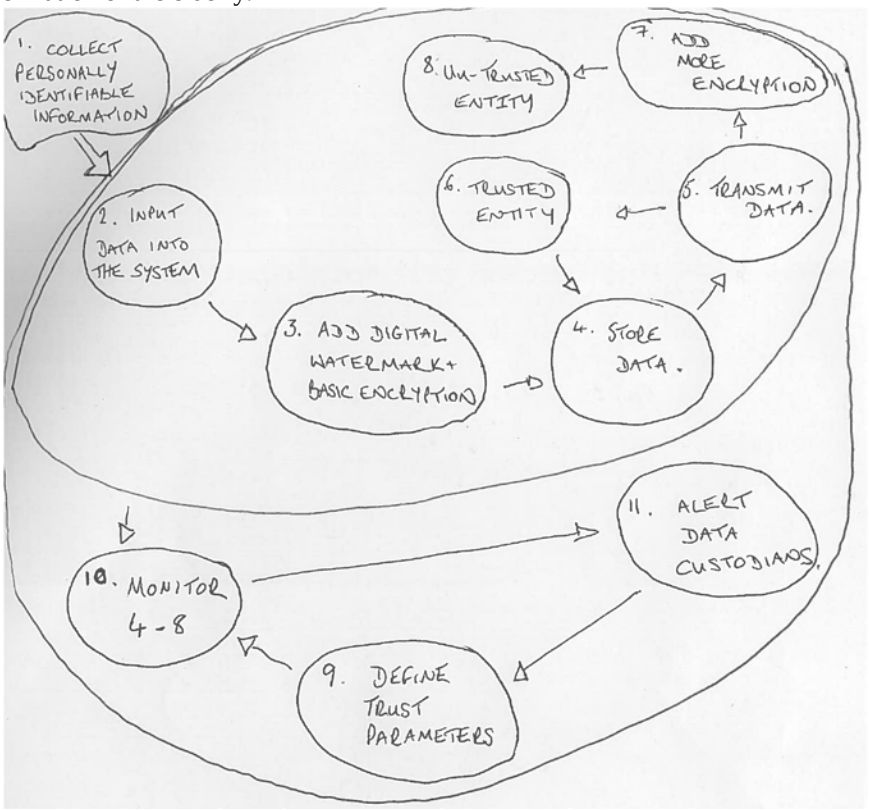

Figure 2: Conceptual model of proposed system for detecting infringement of PII of the elderly

The conceptual model highlights the data flow from its initial input into the system to its being watermarked, stored and transmitted to trusted and non-trusted entities. It also highlights the increase in strong security as the personally identifiable information is shared from trusted to non-trusted entities. The conceptual model also highlights that the system is adaptable in that the defined trust parameters can be changed and updated based on feedback from the alerts received from the data custodians if infringed by an otherwise trusted entity.

5. Conclusion

This paper, using human factors techniques has proposed as system to identify the infringement of the personally identifiable information of the elderly.

In order to do this this paper has critically reviewed the benefits of addressing socio-technical problems in particular the need to align security with the inherent functionality and usability of these systems. Also it has; analysed the usability techniques of elements of its performance around the concept of security; conducted situational awareness by way of personas to show the user experience of certain types of entities that interact with the proposed system; applied soft systems methodology to analyse real world situations for the proposed system, i.e. the complex interaction between the elderly and the socio-technical systems that host their personally identifiable information.

There is still much work to be undertaken in increasing the trustworthiness of socio-technical systems used by the elderly, in particular there is a need for awareness especially as the elderly population is on the increase. In particular work needs to be done in providing easy adaptable data and systems security techniques that provide reassurance both to all users, handlers and providers of personally identifiable information in socio-technical systems.

To further develop this concept, the next steps would be to compare the model of the proposed system described in this paper with reality. This would involve for example, overlaying what currently exists in terms of handling personally identifiable information of the elderly against what could exist in a particular organisation such as the NHS. This kind of comparison would show the gaps in the design particular the lack of systematic activities such as feedback, control and/or monitoring.

Also, undertaking a detailed analysis of all the 'actors' systems and processes as well as the data they hold and how they share and transmit that data would provide a complete picture of current practices.

In conclusion, as can be inferred by the analysis in section 2.0, increasing trustworthiness of the complex interaction between the elderly and the socio-technical systems that store their data requires more than solely having policies and procedures in place regarding secure data collection, storage and transfer. Organisations that provide and utilise the data stored in these socio-technical systems need to have the right file transfer technologies and security systems in place as well as ensuring their staff are trained [18].

References

1. Andreas Holzinger, Kizito Ssamula Mukasa, and Alexander K Nischelwitzer, "Human-Computer Interaction and Usability for Elderly," , Berlin, 2008, pp. 18-21.
2. Alan F Newell, "HCI and older people," , Leeds, 2005, pp. 29 -30.
3. Mirja Kalviainen, "Elderly as content providers in their everyday life supporting services," , Helsinki, 2012.
4. Sri Kurniawan and Panayiotis Zaphiris, "7th International ACM SIGACCESS conference on Computers and accessibility," , Newyork, 2005. [Online]. http://makinggood.ac.nz/media/1262/kurniawanzaphiris_-2005_research-derived-web-design-guidelines-for-older-p.pdf
   Ivan Flechais, Jens Riegelsberger, and M Angela Sasse, "Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-technical Systems," , 2005, pp. 33-41.
5. Stefan Carmien et al., "Socio-Technical Environments Supporting people with cognitive disabilities using public transporation," Transactions on Computer-Human Interaction, vol. 12, no. 2, pp. 233-262, 2005.
6. PWC, "2015 Information Security Breaches Survey," London, 2015.
7. John Benamati and Mark Serva, "Trust and Distrust in Online Banking," Information technology for development, vol. 13, no. 2, pp. 161-175, 2007.
8. Legislation.gov.uk, "Data Protection Act 1998," London, 1998.
9. Sabah Al-Fedaghi, "A Conceptual Foundation for Data Loss Prevention," International Journal of Digital Content Technology and its Applications, vol. 5, no. 3, 2011.
10. Jiangang Shu, Xingming Sun, Lu Zhou, and Jin Wang, "Efficient Keyword Search Scheme in Encrypted Cloud Computing Encironment," International Journal of Grid Distribution Computing, vol. 7, no. 5, pp. 65-76, 2014.
11. Ult T Mattsson, "Database Encryption - How to balance security with performance," 2004.
12. Sapna Saxena and Bhanu Kapoor, "State of the Art Parallel for RSA Public Key Based Cryptsystem," International Journal on Computational Sciences & Applications , vol. 5, no. 1, pp. 81 - 88, 2015.
13. Raju Halder, Shantanu Pal, and Agostino Cortesi, "Watermarking Techniques for Relational Databases: Survey, Classification and Comparison," Journal of Universal Computer Science, vol. 16, no. 21, pp. 3164-3190, 2010.
14. M Hicks, Probliem solving in business and management. london: Chapman and Hall, 1991.
15. Peter Checkland and Jim Scholes, Soft Systems Methodology in Action. Guildford: Biddles Ltd, 1991.
16. Peter Checkland and Jim Scholes, Soft Systems Methodology in Action, A 30 year retrospective. Chichester: John Wiley & Sons, 1999.
17. Maryati Mohd Yusof, Anastasia Papazafeiropoulou, Ray Paul, and Lampros Stergioulas, "Investigating evaluation frameworks for health informaton systems," International Journal of Medical Informatics , vol. 77, pp. 377-385, 2008.
18. Peter Checkland, Systems Thinking, Systems Practice. Avon: The Bath Press, 1988.
19. Gerry Bennett and Paul W Kingston, Elder Abuse, Concepts, theories and interventions.: Springer, 2013.

APPENDICES

Appendix A – Typical Elderly Person Persona

Muriel is seventy-nine years old and has enjoyed a lengthy, healthy retirement having worked as a secretary for twenty five years. She was married to her husband, William, for fifty years prior to his death last year. They raised two children in the home where they lived since they were married. With the help of a cleaner, gardener and weekly visits from her children, she was able to take care of herself and her home.

Muriel became less able to look after herself in her own home with her declining mobility due to hip problems and a recent fall that saw her admitted to hospital for two days. Her children became more concerned about her ability to self-manage her health. Cognitively, Muriel is not appearing to have any serious issues apart from poor memory.

Muriel is a member of her local library and enjoys visits there especially for community events. She has a small group of friends who she meets at the local village hall once a week for tea, she also keeps in touch with them via a social-media account which her son helped her set up on her laptop. Muriel has a good private pension so she regularly donates to various charities that are close to her heart.

Muriel needs to see her doctor every month to help manage her diabetes and high blood pressure. When not visiting her doctor, her prescriptions are sent directly to the pharmacist electronically and who prepare them for her and a family member or carer will collect these for her usually. Muriels children and her doctor recommended and encouraged Muriel to have daily care and as a result of speaking with social services a private care agency was employed. The care agency sends a carer to Muriels home every morning and evening to assist her with food preparation and administering her medication. Muriel has also been given emergency pendant to wear around her neck in case she suffers a fall while on her own.

Appendix B - Persona of a person working within a trusted organisation

Chris a General Practitioner for the NHS, he accesses his patients' data as and when they come into the surgery. Also, he refers patients to other healthcare services and providers both in the NHS and privately. In doing so Chris must share certain personally identifiable information.

Information that Chris has immediate access to on his system are:

- Patients age, contact details and next of kin
- Details of appointments, clinic visits etc.
- Records about health, illness, treatment and care
- Results of investigations, like laboratory tests, x-rays, etc.
- Information from other health professionals

The surgery Chris works for sends details of patients repeat prescriptions directly to the local pharmacy so drugs can be dispensed with no requirement for the patient to visit the surgery each time.

Chris often refers his patients to other areas of the healthcare system, such as physiotherapists, social workers, laboratories, hospitals and care workers, and in doing so shares much of their personally identifiable information. These other services and health care providers will also feed information back to Chris' surgery about the care and treatment they have given the patient.

The information held on Chris' system is also collected and used by the NHS to help plan and improve health care services generally.

Chris colleagues often send Chris information regarding patients who they are in the process of diagnosing, this is done in a secure manner with only limited patient data included.

Occasionally Chris works with researchers and connects patients who might be suited to working with them to assist in the advancement of medical treatments. This is only done with the patients' prior permission.

Appendix C - Persona of a person working within an un-trusted organisation

Clair works for Care, a private care agency who provides a variety of support to people in their own homes. Clair works for a variety of clients, some who employ Care directly and some whose care is commissioned by local authorities. Care is registered with the Care quality commission who regulate and inspect it.

Care holds personally identifiable information on 2,000 individuals such as name, date of birth, address and it also includes data regarding their personal care plans, medication, key safe codes. Most of this information was obtained from the social care agencies who commissioned them on behalf of the elderly people in the community in need of assistance and much of the information regarding their health issues came directly from GP's.

Clair uses a laptop as well as paper notes when visiting her clients to keep abreast of their changing health needs. Updates to client information is fed back through the social care channel to hospitals and GPs. Clair also liaises with therapists and other medical professionals regarding clients day to day care needs.