Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2007

Medical Identity Theft – Not Feeling Like Yourself?

Darren Webb
Edith Cowan University

Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/42

Medical Identity Theft – Not Feeling Like Yourself?

Darren Webb
School of Computer and Information Science
Edith Cowan University
dlwebb@student.ecu.edu.au

ABSTRACT

Hospital and general practice healthcare providers today rely heavily on the information and communication technologies they employ to provide access to patient and associated data. The continuing migration to wireless means of data transfer has afforded system users more convenient and timely access to information via the use of 802.11 based wireless network capable devices. Through the increased digital connectivity of these internet and wireless based networks, new avenues of criminal activity such as medical identity theft have been steadily increasing as malicious individuals and organisations seek to abuse the digital ubiquity of the electronic medical record. The increased need for vigilance, protective measures and tightened security policy surrounding patient data practices concerning the use of wireless devices has never been greater. This paper discusses the potential patient and organisational ramifications of medical identity theft through wireless networks and other means as well as suggesting possible risk mitigation strategies to counteract such unauthorised information access.

Keywords

Medical, Identity Theft, Wireless, Health Care Fraud

Figure 1: Fingerprint Face (Medical College of Georgia, 2005).

INTRODUCTION

Medical identity theft is an emergent criminal activity that poses significant financial, physical and emotional harm to unsuspecting victims. The financial burden of the total identity theft problem in America, identified by the Javelin/Better Business Bureau 2006 Identity Theft Report Survey, is US$56.6 billion annually (Privacy Rights Clearinghouse, 2006). Currently, limited medically specific identity theft statistics exist, due to the ambiguity of classification and differentiation from other identity criminal activities such as health insurance fraud. The perpetration methodologies for medical identity theft are as diverse as the people who commit them and as detrimental in effect as the amount or type of private patient data abused. The global adoption of electronic medical records stored on hospital computer networks, while becoming an asset for medical staff and patient treatment, has also become a prime central repository target for data thieves. Newer network technologies such as wireless device networks have also sprouted new means of remote access for malfeasant persons where security is inadequate.

IDENTITY AND MEDICAL IDENTITY THEFT

An individual's identity is something that both defines a person and allows recognition of the distinct character that is a person's being. In a technologically oriented society, people rely heavily on the reliance of recognition that comes with being able to uniquely identify themselves amongst an increasing populace. The threat of someone else assuming control of another person's identity and benefiting from the deceptive use of that identity, is becoming an increasing risk in today's society. Identity theft may be used for either self gain or other malicious activity by criminals, doctors, nurses, medical institution employees and increasingly, by highly sophisticated crime organisations (Dixon, 2006). The United States' 2006 inflation adjusted figures indicate that identity fraud is estimated to cost US$56.6 billion annually which is up from the US Federal Trade Commission's 2003 Identity Theft Survey Report Figure of $53.2 billion. Other US government and law enforcement agencies estimate the loss associated with fraud at US$170 billion each year which in 2003 equated to approximately 10% of the entire nation's annual expenditure (National Health Care Anti-Fraud Association, 2005a). In Australia, identity theft has been estimated by the Commonwealth Attorney-General's Department in 2001 at costing in excess of A$4 billion annually (Australasian Centre for Policing Research, 2007).

As financially harmful as these crimes may be, the evolution of a new type of identity theft has emerged primarily due to the wide spread adoption of electronic medical records and wireless infrastructures, that can have life threatening repercussions and leave longer lasting negative effects upon its victims. Medical identity theft occurs where a person uses another person's identity without consent, in order to obtain medical treatment services or therapeutic goods they are not authorised to receive. As in the case of identity theft, fraudulent use of another person's identity for medical purposes can be perpetrated in one of three ways, these being: by the creation of a new false identity, the assumption of an existing identity or the modification of an existing identity. People have also been known to commit identity related crimes in their former names after legally changing to a new identity (Australian Institute of Criminology, 2003).

The Australian definitions in policing often refer to identity crime, which acts as an umbrella term to encapsulate both cases of identity theft and identity fraud. There is currently no Australasian Centre for Policing Research definition protocol for that of medical identity theft or health care fraud (Australasian Centre for Policing Research, 2004). It is important to make the distinction between medical identity theft where an identity is falsely created, adopted or modified for medical services gain, and health care fraud where another person's name may or may not be abused to obtain something under false pretence often from a health insurance agency. It is for this reason that it is difficult to accurately represent medical identity theft rates and costs comparative to those of general health insurance fraud. Medical identity theft also tends to be harder to both detect and resolve than other forms of identity theft, as regular medical service transaction statements are not issued or made mandatory by government health agencies or many health insurance providers. Resolution of a detected medical record alteration can often take years to rectify, leading to long-term frustration for individuals who are sometimes too sick to validate their identity personally. Dependent upon the dissemination of the patient's electronic medical record before detection of the error, the ability of the patient to correctly identify themselves post identity theft, and the willingness or capability of the medical and insurance agencies to cater for that request, the likelihood of total resolution is remote (Dixon, 2006).

Everyone from a baby to the elderly can be vulnerable to the practices of medical identity theft. Deceased people make particularly effective targets as, unless there is someone else who investigates the deceased person's record on their behalf, crimes committed by this form of identity theft which is termed Ghosting, can take a long time to be uncovered. Due to the interconnectivity of health agencies, ghosting is less prevalent now but still occurs where routine record checks do not determine if a death certificate has been issued in the deceased victim's name (The Free Dictionary, n.d.).

THREATS

Medical network administrators need to be aware of the varied array of attack vectors and strategies available to data thieves in order to effectively secure confidential patient data. The ideology that malicious users only ever attack from outside the network is one that is sure to see more networks become compromised from internal network avenues. Insiders often have the greatest operational knowledge of how processes occur and either know or can learn what data security measures are in place to find the best ways to bypass them (Valli, 2006).

Threat agents vary in accordance with patient record storage systems, the security elements employed to protect them and the access given to the information contained within the database. Due to the need to use internet based channels for communication between medical providers, the global accessibility and anonymity for hackers to remotely and covertly attack internet connected hospital and other medical network systems is greatly increased. A single remote data breach of any medical database can often result in the theft of thousands of patient electronic medical records at any one time, compared to singular paper based patient records which have

to be accessed directly from the site of use. This increased effectiveness makes medical data theft via digital networks a much more appealing and profitable option to cyber criminals. As far as the specific information targeted by identity thieves, there is no set criterion other than the information that they require to achieve their purpose of committing transactions in the victim's name. (Canadian Internet Policy and Public Interest Clinic, 2007).

As with most computer networks, data theft of personal or organisational restricted client (or patient) record data items can be perpetrated through a wide assortment of technology approaches and devices. These can include attacks via wired or wireless networks, portable digital storage hardware such as bluetooth or IrDA (Infrared Data Association) capable devices, USB thumbdrives and even email services, which have all in the past been used to perpetrate data theft attacks. Methods of medical identity theft perpetration range from the simplistic theft of a device containing data, to the elaborate creation of medical practices where identity thieves portray themselves as doctors and other health care professionals in order to secure patient medicare card details (Dixon, 2006). Despite the many varied means of data extraction for medical identity theft, this paper focuses on the risks posed by wireless networks in medical environments.

Wireless Networks

The wireless revolution of computer networks has seen a dramatic change in the introduction of 802.11 wireless networks for use in a wide range of service organisations including hospitals and medical practices where patient records are typically stored. While the use of wireless local area networks (WLANs) are of practical nature to medical environments in that they provide improved mobility, scalability and cost savings to adopting institutions, there are further risks associated with patient record security. These security issues can be classified as being of either technical or managerial derivation. A problem facing the successful technical implementation of secure wireless networks within medical environments can relate to the prevalence of sometimes insufficiently configured wireless networks, where security focus or knowledge is limited. Managerial issues, such as poor policy implementation and enforcement, can however pose a greater risk to wireless networks than technical issues, as they involve the human element of securing the network which contains patient data (Owens, et al, 2001).

Wireless networks are still subjected to the standard vulnerabilities of wired networks such as Denial of Service (DoS) attacks, Spoofing attacks, Man In the Middle (MITM) attacks and various malware employed attacks, but are also exposed by its remotely accessible nature to de-authentication type attacks through the use of rogue access points (SearchSecurity.com, 2007). The broadcast nature of wireless networks makes the protection of data more of a security issue for sensitive information holders such as medical institutions.

Typically due to legal requirements, the vast majority of medical wireless infrastructures are protected from unauthorised access by security protocols such as Wi-Fi Protected Access (WPA) based on the draft 802.11i standard and the security enhanced WPA2 variant, based on finalised 802.11i. WPA2 is particularly secure as it employs AES (Advanced Encryption Standard) as well as catering for Radius authentication. Predecessor security measures such as Wired Equivalent Privacy (WEP) have proven insecure and will typically only deter casual network snooping. Although better than totally unencrypted or open networks, this encryption format will not stop a determined wireless hacker (Ciampa, 2005). Unfortunately many wireless device manufacturers still ship wireless devices with security settings either completely disabled or at a minimal level, such as easily broken Wireless Equivalency Privacy (WEP) by default, in order to simplify setup procedures (Symantec, 2002). Due to the serious and widely publicised weaknesses of WEP, medically business oriented WEP users in America are deemed to be in breach of adequate security compliance using this data security measure alone. As well as the obvious security concerns of a confidential data breach, the HIPAA (Health Insurance Portability and Accountability Act) penalties for violations range from US$100 per person/per incident for minor improper disclosures to US$250,000 and a 10 year prison sentence for intentional disclosures. Statutory penalties such as these however, may be of minimal concern considering the potential for class action lawsuits if significant medical information breaches were brought to trial (HIPAAdvisory, 2006).

Medical institutions are unsurprisingly secretive of wireless network breaches that have occurred to their system as a result of inadequate security implementation or management. Steve Lewack the Director of Technology Services at the Columbus Regional Medical Center in Columbus, Georgia stated in 2005 that their wireless network monitoring security systems had stopped approximately 120 attempted breaches in a one month period. This was also estimated to be double the number of attempts of a few months earlier (USA Today, 2005). In light of this, hospitals and other wireless adopting medical institutions should also consider the necessity for wireless deployment where a wired and hence more remotely secure network would suffice.

The remote access possibilities of wireless medical networks could also serve as a point of access for malware by potential identity thieves, who can use trojan attacks with rootkit functionalities to gain access to personal

information and passwords from infected systems. In the 2006 Australian Computer Crime and Security Survey, key findings indicated that since the 2004 survey there has been a substantial increase in the number of trojan attacks which are believed to be for the purpose of facilitating identity theft crimes. Trojan attacks are often targeted at the customers or clients of specific organisations rather than having a larger infection range as in the case of viruses and worms. A decline in indiscriminate worm and virus attacks identified that the motivation change of attackers was due to the desire for illicit financial gain through the identity theft of online access credentials (AusCERT, 2006).

With American wireless market penetration growing from 9% in 2000 (Gartner, 2002) and expecting to reach 84.8% of businesses adopting the technology by the end of 2009 (Gartner, 2006a), the potential for further insecurity in the deployment of wireless networks is growing. This penetration rate is also related to the increased inclusion of wireless enabled devices in mobile PCs being shipped, from 10% of all laptops in 2000 to 68% in 2007 (Gartner, 2002). In the same vein, the decreasing cost of wireless equipment has increased the deployment possibility of wireless networks and at the same time, allowed the technology to become more obtainable to hackers who wish to use the freely internet accessible wireless hacking programs to penetrate signal available wireless networks. For an external hacker, the equipment required for accessing a network can be as minimal as a wireless enabled laptop and a covert location within the broadcast range of the access point.

CONSEQUENCES

Patients who have medical records created in their name for the purposes of treatment, have a right to privacy regarding the protection and access to that information. While there are clearly many functional benefits to be gained from the digitalisation of medical records, the patient must be satisfied with the privacy measures employed to allay these concerns and protect the future doctor-patient relationship (Doctors Reform Society of Australia, 2005).

The private content of a medical record, either electronic or paper based, presents itself as a high value target to those with motive to seek potential gain from the theft of such information. Typically most medical identity theft is targeted at the acquisition of information for financial reward where further risk for patients presents consequences ranging from low impact data alterations to fatal medical treatment administration. Medical identity malfeasance can lead to serious medical, health insurance and employment issues for victims who fall prey to such attacks by either individuals or organisational groups. These instances of fraudulent activity can also indirectly affect the wider community.

Medically related consequences

The data contained in an electronic medical record is of a highly private nature to an individual. This data can include information on the patient's diagnostic history of diseases, medication and treatment histories, genetic and psychological profiles, sexual orientation and activity, employment and income, as well as subjective notes relating to personality made by doctors and nurses. If patients were to lose confidence in the security of medical record systems, this could potentially lead to patient discomfort in truthfully disclosing sensitive information if they believed there was a chance the information could be leaked to unauthorised parties. This privacy issue could then place the patient at risk of not being correctly diagnosed and treated and endanger the doctor-patient relationship (Choi, et al, 2006).

The physical repercussions of malicious abuse of a person's identity for medically related gain, can include use of another person's identity to obtain access to prescription medications and treatment services including surgical procedures. Erroneous alteration of patient medically critical data such as disease conditions, allergies, medications and even blood type all have life threatening impacts if used to base diagnosis or provide treatment from this information. While these risks often originate externally from maliciously modified information, adverse patient consequences can also, although rarely, be attributed to physician abuse of patient identities and records. An example of this is the June 2002 US federal conviction of three physicians and a hospital administrator from Chicago who over a 10 year period had performed over 750 invasive and unnecessary heart catheterizations and angioplasties. The victims primarily homeless people, substance abusers and elderly men and women, were offered food, cash and cigarettes as incentives in order that the doctors could claim on the procedural benefits (National Health Care Anti-Fraud Association, 2005b).

In other individually oriented cases, victims only discovered their plight when invoices for medical services rendered in their name arrived in the mail. For example, a man in Colorado USA, whose name, address and social security number had been stolen, received a letter from a debt collector demanding the US$44,000 he owed to a hospital for surgery he never had. The man, who had no private health insurance, then had to endure a lengthy process to clear his name, which after two years had still not been resolved. As well as this damaging his credit rating, he may possibly never know if his medical record has been completely cleared of erroneous

information. This typifies the victim patient adversities in clearing their name and getting the correct recognition and medical treatment in the future (Dixon, 2006). While victims of financial identity theft are able to gain access to and correct errors on their credit statements and other financial documents, victims of medical identity theft are not able to achieve such resolution. For such victims there is currently no standard procedure for addressing medical record abuse or alteration as they often do not have direct access to their own medical record or regular statements by which to identify anomalies.

Once medical identity theft has occurred, the compromised record can then be further used to access more identity information leading to further crime. Medications obtained in this way are sometimes stolen for personal use or often sold off in larger quantities as in the case of organised crime syndicates. Victims often don't discover their medical records or benefits have been abused until well after the crime has occurred. The advice given to medical identity theft victims is generally also targeted at the more commonly known financial identity theft which involves an exclusively different set of protocols for resolving the victim's issues (Dixon, 2006).

Long term problems can also be created for the accuracy of medical research statistics, where patient records have been incorrectly modified in hospital databases which are often used as a source of de-identified data thereby reflecting inaccuracies. Medical health care providers can also fall victim to identity theft allowing thieves to falsify patient records and forge prescriptions at will (Dixon, 2006).

With the promised introduction of the Australian Government's Health and Social Services Access Card due for release from 2008, further security issues could arise regarding the medical identity theft risks to card holders. The card is scheduled to amalgamate 17 existing cards and be used for the administration and payment of health and social services for all eligible Australians (Queensland University of Technology, 2006). But what is yet to be seen is, if Australian criminal elements will now target this new patient identification item as has been the case with the health insurance card in the United States of America.

It is currently widely viewed that from an operational perspective, the digitisation of medical records is a boon for users of this data medium, as well as enabling improved healthcare and reducing fraud and medical errors which will ultimately lead to saving lives. This however doesn't take into account the challenging reality of threat posed by the perpetrators of medical identity theft and the severe emotional damage that can have significant consequences on a victim's well-being (Dixon, 2006).

Health insurance related consequences

The lack of awareness of this type of crime is also an inhibiting factor in the detection and recovery of stolen benefits. There is often a large time lag between the theft of data and the patient realisation that malfeasance has taken place. Despite the victims affected directly by medical identity theft attacks, the ultimate result, due to costs associated with higher insurance premiums, is that the general cost of medical care increases for everyone in order for services to be maintained (National Health Care Anti-Fraud Association, 2005c). This increased theft prevalence of individuals' health insurance benefits, may then leave patients financially liable for medical services that are no longer covered due to malicious use of their finite claim entitlements. Other effects can be a loss of life insurance cover due to incorrect diseases recorded in patient medical records. The people who commit medical identity theft can also be medical professionals who know how the system works and are adept at making sure the crime is hard to detect by victims. There have also been reported cases of individuals stealing the medical identities of others in order to dodge medical bills (Dixon, 2006).

Employment related consequences

Disregarding the ethicality of employers having access to job applicant medical records on which to base employment suitability, medical record abuse by identity thieves could create loss of job opportunity situations. Employer discrimination could then be based upon false information after an applicant's background medical check revealed a disease that they don't actually have or a more severe condition of a disease they do have (National Health Care Anti-Fraud Association, 2005d). A non-patient of a Boston psychiatrist found after applying for employment, that his medical record had been modified showing that he had numerous psychiatric sessions by the Boston specialist for a false diagnosis of severe depression (Dixon, 2006). This type of event shows the wide reaching effect that the abuse of an individual's private medical details can severely affect other facets of the individual's life.

Community related consequences

The community consequences of medical identity theft are hard to accurately portray, as the identification of theft related to healthcare is both intermeshed with health insurance fraud, and the fact that many instances of medically related identity theft go unreported and undetected. As well as the obvious increases in health

insurance premiums, medical fraud annually strips billions of dollars from state and federal government public services that could otherwise be available to treat more patients (Identity Theft 911, 2006).

Reports from the World Privacy Group, a San Diego-based research group, now indicate a shift in the priorities of thieves. Stolen health records can now fetch between US$50 to US$60 on the black market, in comparison with the previously high target information source of stolen curriculum vitae's which now only raise a paltry seven cents (Business Week, 2007). The impact of this type of crime is also hard to quantify for policing and other law enforcement agencies, who spend considerable amounts of time and resources dealing with the investigation and prosecution of identity thieves (IDTheft.gov, 2007).

INADEQUATE AUSTRALIAN LEGISLATION

In Australia there is currently limited legislation specifically related to medical identity theft. The Australian Federal Privacy Act 1998, Subsection 95A, titled "Guidelines for National Privacy Principles about health information" outlines little change in reference to the National Privacy Principles' data security guidelines. The general nature of these data guidelines only recognise the protection and later destruction of de-identified data by organisations and is largely devoid of electronic storage and communication specific guidelines for medically related patient information (The Office of the Privacy Commissioner, 2000).

Internationally the medical information standards have been updated by the International Organization for Standards (2006) in the form of ISO/DIS 27799 which is only currently a draft international standard as at June 2006. Based upon the previous year 2000 ISO 17799 code for information security management, the more medically related information security minimum requirements of ISO/DIS 27799 addresses the specialised management of medical information security. This is to ensure that the information security tenants of confidentiality, integrity and availability are applied to all aspects of electronic health information (Fraser, 2006).

The Health Insurance Portability and Accountability Act (HIPAA)'s administrative simplification provisions enacted by the United States Congress in 1996, developed legal foundations for electronic transfer of medical information that acts to provide both security and privacy for patient records. Additionally the use of CFR 45 (Code of Federal Regulations number 45) which outlines a set of standards for the protection of sensitive electronic personal health information, is far more specific than that effected in the Australian health environment (DotSec, 2006).

PREVENTATIVE MEASURES

There are many preventative measures that can be initiated by individuals and organisations to mitigate against medical identity theft occurrences, even though it is not possible to prevent all determined malicious individuals from gaining access to private data. Despite a patient's medical data being primarily stored in medical institution databases, patients can still take simple measures in guarding their personal medical data. These steps include:

- Treat health insurance cards and details with credit card-like security
- Immediately report lost or stolen cards to medical and/or insurance agencies
- Request and check health benefit statements regularly for erroneous items
- Be suspicious of healthcare agencies offering "free or heavily discounted healthcare" promotional services

(The Ohio State University, 2007).

Organisations that handle restricted access medical patient information should also employ additional security practices to ensure patient data is less vulnerable to opportunistic identity thieves. Some of the ways security could be improved is to:

- Educate patients and staff about medical identity theft
- Improve physician security practices by ensuring correct patient identification before consulting
- Use recognition technology to improve patient identity accuracy
- Analyse patient claims more thoroughly and monitor claim trends
- Improve healthcare provider internal security through: record encryption, log auditing, security policies and further securing data access (Gartner, 2006b)

- Encrypt email containing patient data
- Conduct criminal background checks on all employees
- Maintain physical facility security
- Avoid the discussion of patient related information in public areas where others may eavesdrop (Radiology Today, 2006)
- Maintain a history of disclosures record to identify all parties that the information has been disclosed to in order to later help track breaches (National Security Institute, Inc, 2006).

The data breach preventative policies of hospitals and other medically related service institutions need to be kept up-to-date to reflect the growing risks and concerns regarding medical identity theft. This is critical because once a data leak has been detected and the damage has already been done, it is virtually impossible to identify to whom the data has been further disseminated and if there is any form of riposte. Health care providers at Kaiser Permanente, a health care network of 30 medical centres and 431 medical offices, now check driver's licences as standard practice in addition to the program's health card. This new medical identity theft reduction measure was only introduced after staff reported to investigative researchers that approximately a dozen patients per week attempt to impersonate others for their benefits. Reasons for the staff disclosure to the researchers, was primarily due to concerns they had over the true patient consequences of false entries in medical records (Dixon, 2006). Although the staff in this case became aware of the patient identity anomalies before an offence could occur, the more complex schemes of medical identity theft often go undetected. As in many information security critical applications, the increased security measures are typically performed in a reactive manner after an identity abuse has been detected.

Hospitals and medical institutions need to realise that reporting of data breaches is becoming a legal requirement in many locations, where withholding information regarding security breaches is an infringement of notification laws. In America as of October 2006, there were two laws under consideration in Congress, namely the Identity Theft Protection Act (S1408) and the Federal Agency Data Breach Notification Act (HR5838) which are aimed at making reporting of data breaches a mandatory practice for organisations (Journal of AHIMA, 2006).

The recent popularity of web based social interaction practices, where publicly accessible forums such as chat rooms, wikis or blog sites that are used to share information among users, has expanded to global proportions. The advent of the Web 2.0 social networking trend, which is intended to create richer web application interactions, facilitate user sharing and collaborations, could be covertly used by malicious individuals to procure more critical private information about future victims (Microsoft, 2006). People posting personal details to these mediums could thereby expose themselves to greater medical identity theft risk, by divulging private information that could inadvertently be used to perpetrate identity crimes against the information discloser. It is for this reason that users of these mediums need to be aware of potential risks and take preventative measures.

CONCLUSION

The theft of an identity for malicious purposes is a threat that must not be underestimated. The potential for individual harm is far greater than that of other crimes where victims are not specifically targeted. Medically related identity theft is an even more significant risk to people whose medical data is illegally accessed, altered or disseminated, as the consequences can be life threatening. Currently there appears to be a limited awareness of the risks and increasing prevalence of medical identity theft due to the inability to statistically categorise its occurrences and recognise its protracted covert existence. Over time, as medical institution patient records become increasingly electronically based, this form of identity fraud may become easier to commit and may already be occurring more than anyone has documented to date due to its difficulty of detection (Dixon, 2006).

Where medical data storage security provisions are inadequate and breaches occur, medical identity theft can destroy the integrity of the accuracy concerning electronic medical records, leaving financially liable and increased medically at-risk patients in its wake. Once breached, the private medical data disseminated and re-disseminated via computer networks or abused by identity thieves, can do irreparable financial, medical and emotional damage to victims. This in turn can depreciate the critical value and trust component of the doctor-patient relationship, as well as the integrity of the patient's own medical record, where medical institutions have themselves become victims of their own technological security inadequacies. There is currently no standardised healthcare industry process for addressing the concerns of medical identity theft victims, who after having their identities compromised then have the long term challenge of verifying their true existence.

REFERENCES

AusCERT (2006) 2006 Australian Computer Crime and Security Survey, URL http://www.auscert.org.au/images/ACCSS2006.pdf, Accessed 28 April 2007.

Australasian Centre for Policing Research (2004) Standardisation of Definitions of Identity Crime Terms, URL http://www.acpr.gov.au/pdf/Standdefinit.pdf, Accessed 27 April 2007.

Australasian Centre for Policing Research (2007) Identity Crime Research and Coordination, URL http://www.acpr.gov.au/research_idcrime.as, Accessed 27 April 2007.

Australian Institute of Criminology (2003) Serious Fraud In Australia and New Zealand, 26, URL http://www.aic.gov.au/publications/rpp/48/RPP48.pdf, Accessed 24 April 2007.

BusinessWeek (2007) Diagnosis: Identity Theft, URL http://www.businessweek.com/magazine/content/07_02/b4016041.htm, Accessed 12 May 2007.

Canadian Internet Policy and Public Interest Clinic (2007) Techniques of Identity Theft, URL www.cippic.ca/en/bulletin/Techniques.pdf, Accessed 14 May 2007.

Choi, Y., Capitan, K., Krause, J. and Streeper, M. (2006) Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules, *J Med Sys (2006)* 30(1): 57–64, URL http://www.springerlink.com/content/035317748wrk775t/fulltext.pdf, Accessed 18 April 2007.

Ciampa, M. (2005) Protecting Advanced Communications, *Security+ Guide To Network Security Fundamentals, Second Edition.* 7, 252-253, Course Technology, Boston, Massachusetts.

Dixon, P. (2006) *Medical Identity Theft: The Information Crime That Can Kill You,* World Privacy Forum, URL http://www.worldprivacyforum.org/medicalidentitytheft.html, Accessed 28 March 2007.

Doctors Reform Society of Australia (2005) Doctors Fear For Patients Privacy With Electronic Records, URL http://www.drs.org.au/media/2005/media010605.htm, Accessed 5 May 2007.

DotSec (2006) Holistic, or full of holes? PCI, HIPAA and experiences in implementing secure computing systems, Presentation Abstract, URL http://www.dotsec.com/Links%20-%20health.html, Accessed 26 April 2007.

Fraser, R. (2006) ISO 27799: Security management in health using ISO/IEC 17799. *Canadian Institute for Health Information (CIHI) Partnership Conference. June 2006,* URL http://sl.infoway-inforoute.ca/downloads/Ross_Fraser_-_ISO_27799.pdf, Accessed 5 May 2007.

Gartner (2002) Gartner Dataquest Says Worldwide Wireless LAN Shipments to Grow 73 Percent in 2002, URL http://www.gartner.com/5_about/press_releases/2002_09/pr20020919a.jsp, Accessed 4 May 2007.

Gartner (2006a) Gartner Wireless & Mobile Summit 2006, URL http://www.gartner.com/2_events/conferences/attributes/attr_138156_93.pdf, Accessed 4 May 2007.

Gartner (2006b) Gartner Voice - Medical Identity Theft, URL http://www.gartner.com/it/products/podcasting/asset_163121_2575.jsp, Accessed 20 April 2007.

HIPAAdvisory (2006) Wireless Networks, HIPAA & WiFi: Regulatory Tangles for Wireless Health Care Networks Analyzed, URL http://www.hipaadvisory.com/tech/wireless.htm, Accessed 14 May 2007.

Identity Theft 911 (2006) Medical Identity Theft Case Pursued in Florida, URL http://www.identitytheft911.org/alerts/alert.ext?sp=631, Accessed 10 May 2007.

IDTheft.gov (2007) Combating Identity Theft - A Strategic Plan. Law Enforcement – Prosecuting and Punishing Identity Thieves, *The President's Identity Theft Task Force,* URL http://www.idtheft.gov/reports/StrategicPlan.pdf, Accessed 5 May 2007.

International Organization for Standards (2006) ISO Update, *Supplement to ISO Focus, June 2006*, URL http://www.iso.ch/iso/en/commcentre/isofocus/isoupdate/pdf/june06.pdf, Accessed 5 May 2007.

Journal of AHIMA (2006) Data Theft and State Law - When Data Breaches Occur, 34 States Require Organizations to Speak Up. November–December 2006, 77/10, URL http://www.privacyrights.org/ar/Wernick_Dec06.pdf, Accessed 6 May 2007.

Medical College of Georgia (2005) Fingerprint Face [Picture], URL http://www.mcg.edu/ipi/Resources.htm,

Accessed 5 May 2007.

Microsoft (2006) Blog behaviour: Safety advice for kids, URL http://www.microsoft.com/canada/home/internetandsecurity/2.4.49_blogbehavioursafetyadviceforkids.aspx, Accessed 17 May 2007.

National Health Care Anti-Fraud Association (2005a) *Health Care Fraud – A Serious and Costly Reality For All Americans*, URL http://www.hcinsight.com/docs/papers/NHCAA%20White%20Paper%20on%20Fraud.pdf, Accessed 26 April 2007.

National Health Care Anti-Fraud Association (2005b) Physical Risk to Patients, *Health Care Fraud – A Serious and Costly Reality For All Americans*, URL http://www.hcinsight.com/docs/papers/NHCAA%20White%20Paper%20on%20Fraud.pdf, Accessed 26 April 2007.

National Health Care Anti-Fraud Association (2005c) That Some Health Insurance Claims Are Fraudulent is Beyond Dispute, *Health Care Fraud – A Serious and Costly Reality For All Americans*, URL http://www.hcinsight.com/docs/papers/NHCAA%20White%20Paper%20on%20Fraud.pdf, Accessed 26 April 2007.

National Health Care Anti-Fraud Association (2005d) Falsification of Patient's Diagnoses and/or Treatment Histories, *Health Care Fraud – A Serious and Costly Reality For All Americans,* URL http://www.hcinsight.com/docs/papers/NHCAA%20White%20Paper%20on%20Fraud.pdf, Accessed 26 April 2007.

National Security Institute, Inc (2006) Protect Yourself from Medical ID Theft, *Security Sense,* Vol 9, No. 11, Sept 2006, URL http://www.enr.state.nc.us/its/SecuritySense/7sep06.html, Accessed 16 May 2007.

Owens, T., Tachakra, S., Banitas, K. and Istepanian, R. (2001) Securing a Medical Wireless LAN System, URL http://www.packetnexus.com/docs/EMBC%20security%20paper.pdf, Accessed 24 April 2007.

Privacy Rights Clearinghouse (2006) How Many Identity Theft Victims Are There? What IS the Impact on Victims?, URL http://www.privacyrights.org/ar/idtheftsurveys.htm#BBB, Accessed 24 April 2007.

Queensland University of Technology (2006) The Proposed Health and Social Services Access Card, *e-Health Research Group.* URL http://www.e-health.qut.edu.au/about/healthcard.jsp, Accessed 24 April 2007.

Radiology Today (2006) Fighting Fraud & Identity Theft in Radiology, URL http://www.radiologytoday.net/archive/rt11202006p40.shtml, Accessed 12 May 2007.

SearchSecurity.com (2007) *Wireless attacks, A to Z,* URL http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1167611,00.html, Accessed 24 April 2007.

Symantec (2002) Wireless LAN Security - Enabling and Protecting the Enterprise, URL http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf, Accessed 3 May 2007.

The Free Dictionary (n.d.) *Ghosting (Identity Theft),* URL http://encyclopedia.thefreedictionary.com/Ghosting+(identify+theft), Accessed 12 May 2007.

The Office of the Privacy Commissioner (2000) National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000), URL http://www.privacy.gov.au/publications/npps01.html#d, Accessed 10 May 2007.

The Ohio State University (2007) Medical ID Theft: Is Someone Getting Treatment in Your Name? *Human Resources.* URL http://hr.osu.edu/hrpubs/resourcespr07.pdf, Accessed 4 May 2007.

USA Today (2005) Identity thieves can lurk at Wi-Fi spots, *Tech,* URL http://www.usatoday.com/tech/news/2005-02-06-evil-twin-usat_x.htm, Accessed 15 May 2007.

Valli, C. (2006) The Insider Threat to Medical Records: Has the Network Age Changed Anything?, URL http://ww1.ucmss.com/books/LFS/CSREA2006/SAM8148.pdf, Accessed 14 April 2007.

COPYRIGHT

Darren Webb © 2007. The author assigns Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the

World Wide Web. The author also grants a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the author.