Information Governance and Patient Data Protection within Primary Health Care

Smith M, Buchanan W, Thuemmler C, and Hazelhoff Roelfzema, Nicole
School of Computing, Edinburgh Napier University, UK

I. Abstract

The introduction of Information Governance throughout the NHS in Great Britain from 2004 onwards, saw Primary Care Medicine subject to a regulatory regime aligning current practice with codes, ethics, legislation and standards. However the Information Commissioners Office, as regulator of Healthcare Data Controllers, has issued statutory Undertakings to stem the tide of continued leakage of sensitive health data. Drawing on research from America, the issue of IT Security Risk is presented as problematic given the limitations of surveys indentifying industry trends and is viewed beyond the traditional Threat Value Asset Matrix towards a framework incorporating the reasonable man – taking all due care and diligence as is reasonably practicable in the circumstances. Following the identification of major problems across 10% of English general practices in complying with both Confidentiality and Data Protection Assurance, and Information Security Assurance, a national survey of GP Practices was undertaken to investigate security incidents and risk. Contemporaneous to this, information on reported untoward security incidents was obtained from the regulator and all Health Boards across Scotland. Together, these results identified actual risk to securing patient data and concerns voiced from within the sector. This may be of relevance to practitioners, managers as well as policy makers particularly where changes to the structure of the NHS are proposed.

Categories and Subject Descriptors
K.6.5 [Security and Protection]

General Terms
Management, Security, Theory

Keywords
Risk Management, Risk Assessment, Risk Control, Information Privacy, Information Security, Compliance, Healthcare, IT Management

II. Data Leakage as a problem area

The forward to the Information Governance Program Plan 2008-2011 provides a succinct review of the aims of government policy as the NHS moves toward integrated IT Systems and an electronic Health Record (Scottish Government, 2008). Information processing must occur to the benefit of patients in a secure and confidential environment which meets all regulatory, quality, legal and ethical obligations. This must meet the Confidentiality-Integrity-Availability (CIA) triad- data must remain confidential, its integrity must be ensured and it must be both accurate and available to those authorised to receive it (Kolkowska, Hedstrom, & Karlsson, 2009). In the US the move to a fully integrated e-Health system has been estimated to improve efficiency and reduce costs, saving some $81bn (Appari & Johnson, 2009). The coalition government recently announced a paradigm shift in the provision of Health Care in the UK with proposals to remove Primary Care Trusts in England and giving full fiscal independence to general practices (Department of Health, 2010d).

Given the sensitive nature of personal health data and the sheer size of the NHS, the largest employer in Europe with 1.3 million staff (NHS Careers, 2010), it is hardly surprising the media are replete with examples of data leakage. These include reports of one in ten hospitals having insecure IT Systems (BJHCIM, 2010a), loss of a USB stick containing patient data found in a car park (BJHCIM, 2010 b), an average loss of around 835 patient records every day within the NHS (Doyle, 2010), IT Professionals Failing in IT Security (BJHCIM , 2010 c), and even spending six weeks locating a memory card missing from the medical photographers office at the Sick Kids Hospital in Edinburgh (Morris, 2010).

Within the UK the Office of the Information Commissioner (Information Commissioner, 2010) is charged by parliament with regulating the processing of data. The Data Protection Act 1998 defines identifiable personal data (IPD), as sensitive where this contains health, or details of union activity, political preferences, religious inclinations or sexual proclivities (Crown, 1998). This is consistent with its predecessor the 1984 Act (Crown, 1984). As such sensitive data should be subject to a stricter processing regime.

Despite the benefits of an integrated e-Health strategy, the Information Commissioner reported the Healthcare sector accounts for some of the largest number of complaints. Indeed, of all the undertakings entered into to ensure compliance in the last few years, the majority were issued to the Health Sector (Information Commissioner, 2010). Table 1 provides a breakdown of these undertakings.

Most notable amongst these undertakings is the large number of data leakages arising from hospitals rather than GP Practices. Of the undertakings issued, two were to GP's (Office Information Commissioner, 2009). From an analysis of all the undertakings, it appears basic physical security systems were absent (devices secured to desks) or basic measures to prevent unauthorised access were missing (password protected encrypted data). The volume and type of data affected ranged from patient details through to staff records.

III. The problem of Assessing Risk to Data

Several fundamental flaws have been highlighted in current IT Security Risk assessment methods (Parker D., 2006) (Mattord H. , 2007). These are based around an economic analysis of Threat Vulnerability Asset (TVA) in order to determine

the optimal security investment (Gordon & Loeb, 2002). Firstly assets are identified and an asset value associated to it. Secondly for every asset potential threats are identified. At this stage an estimate of the probability of the threat occurring is made as well as an estimate of the loss incurred if the threat materialises. The third stage is to estimate the annualised loss expectancy (ALE). This is the cumulative value of all threats affecting the asset.

However, reports of occurrence of a risk may not be based upon large populations but on inconsistent reporting over differing populations and in altogether different industrial sectors with diverse opinions on threat to their assets (Price Waterhouse Coopers, 2010). Underlying all of this is the problem of reluctance to report. With no consistent statutory notification scheme the datasets may be skewed.

A survey of IT Security practitioners in 2006, albeit rather small, provided some indication that many managers estimate en element of the ALE calculation (Mattord H., 2007). Interestingly 74% indicated compliance with regulations drove the risk assessment approach. The Sarbanes-Oxley Act of 2002 (SOX), The Gramm-Leach-Bliley Act (GLBA) and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) were most influential in the compliance environment. Over half of the respondents indicated they were reliant upon compulsory regulation to a large degree.

The alternative approach espoused by Mattord and others is due diligence, compliance and business enablement. This is taking all steps as is reasonably practicable (a precept normally associated with common law based jurisdictions) to meet the standards defined in voluntary codes, codes approved by regulators or legislation.

IV. Risk and Regulation in the American Healthcare Sector

Within the Healthcare sector, compliance with the HIPAA regulations, coming into effect in April 2005, has produced some interesting results. In a 2006 survey, only 25% of hospitals across the USA were found to comply with the security regulations. This prompted research in 2008 and 2009 at the prestigious Dartmouth College, into the extent to which hospitals met the requirements of the Privacy, Security and Transaction Rules (Appari, Anthony, & Johnson, 2008). The methodology used in these studies was to review a database of hospital information including perceived compliance from senior managers. A second database was used to identify IT Leaders demonstrating good practice. Both databases were combined to produce IT Leaders within the Healthcare field and nationally gathered information on the Hospitals themselves. The status of the hospital determined whether further regulation applied such as Sarbanes Oxley Act which requires the implementation of COBIT.

The more recent 2009 study attempted to identify the effect of institutional and market forces on compliance. Thus external pressure from regulation (coercive), copying competitive rivals (mimetic) and industry best practice from external consultants (norms) influence compliance levels (Appari, Anthony, & Johnson, 2009). Whilst both studies identified characteristics of hospitals with high levels of HIPAA compliance the major flaw in the research was the data set used dated from 2003 and therefore did not portray an accurate picture of current compliance.

V. Risk and Regulation in the British Healthcare Sector

The Department of Health has worked closely with the Royal College of General Practitioners to establish standards governing the processing of patient data (Department of Health & Royal College of General Practitioners, 2005). Generally, the NHS approach to IT Security in Primary Care has been to encase this as a small element within a wider Information Governance Framework (NHS Connecting for Health, 2009). The raison d'être of the framework was to provide a mechanism whereby Regulations (statute law including the Data Protection Act 1998, statutory instruments, orders, case law), Standards (Professional and Ethical) and Good Practice (NHS Executive letters, directions and guidance notes) could be enforced throughout the largest employer in Western Europe. In Primary Care there are a number of elements which GP's must satisfy in order to demonstrate good governance (Department of Health, 2007) (Department of Health, 2010 a). These criteria fall within the scope of three major areas: Information Governance Management, Confidentiality and Data Protection Assurance, and Information Security Assurance.

Practices were obliged to complete their Information Governance self-assessment before 31st March 2010. Every practice must attain a predetermined number of key requirements to achieve an overall green rating of 70% in each area. An analysis of 10% of the publically available results for England, some 800 practices revealed the nature of the risks to Patient data. Nearly 40% of practices failed to meet the government set standards for Information Security Assurance. In terms of Confidentiality and Data Protection compliance, some 55% failed to attain a green rating. In April, the Information Commissioner was granted the powers to impose fines of up to £500,000 for data security breaches. Facing the potential of crippling fines and poor governance results in England are Scottish Practices any better?

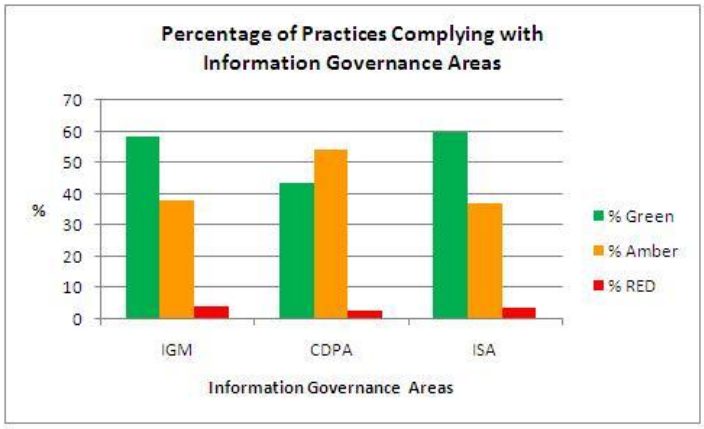

Figure 1 Information Governance compliance in England

Source: Analysis of results 2009-10 from 10% of GP practices in England (Department of Health, 2010 c)

VI. The 2010 Scottish Survey

An online questionnaire was issued to all Health Boards (1,082 practices) in Scotland with two refusing to participate. This reduced the population to 837 practices. Contemporaneous to this, requests under the Freedom of Information Act were similarly issued to all Health Boards requiring details of all reported IT Security incidents during the last few years. The majority of respondents to the survey were practice managers. Thus managers in 84 (10.05%) of the sample population of 837 practices responded.

1) IT Security in Scottish practices: Main Findings

Eighty percent of practices retain their own databases of patient data. Interestingly, 21% of practice managers indicated they were not registered as data controllers. It is recommended practice managers check with the online list of registered data controllers to confirm they are currently registered. As this is a strict statutory liability offence, it was expected all practices were already registered. This may be simply due to the senior partner registering the practice rather than the practice manager.

The Information Commissioner, in the latest Annual Report to Parliament, drew attention to Health Boards and PCT had experienced theft of laptops and PC's. Therefore it was deemed important to investigate whether devices which could be easily stolen were encrypted. Nearly 2/3rd of practice managers indicated encrypted laptops were used in the practice. A similar figure used fully encrypted desktop systems within their practice.

Whilst most health boards have mandated the use of fully encrypted USB devices it should be noted less than three percent of practice managers indicated USB devices were used to transfer patient records. It is recommended that practice managers ensure where they do use USB devices these are fully encrypted.

It is reassuring to read the most common forms of transferring patient records are via secure systems (NHS email, courier, GPEX). There is virtually no use of USB devices or CD/DVD's to transfer data. In light of this it is unlikely a repeat of the HMRC debacle where entire data sets of millions of records on DVD went missing.

Data is shared with secondary care professionals. Few practices transfer the entire electronic patient record. Most sharing occurs via secure methods, the SCI gateway being most popular. NHS email is predominately used. However ¾ transfer details with secondary care professionals via telephone. Almost two thirds use faxes to transfer details.

In terms of awareness of relevant codes and legislation there was a higher awareness of confidentiality, Data Protection and Freedom of Information legislation than other codes. Over half (59%) of practices indicated they were aware of Good Practice Guidelines for GP's. A similar number were aware of the NHS Information Security Policy (60%) and Records Management NHS Code of Practice (64.4%).

Most practices were aware of how they could contact the Information Governance lead within their practices for advice and guidance. However 40% did not know how to contact the IT Security Officer (ITSO) within the Primary Care Trust. The ITSO within the PCT is able to provide a degree of computer security expertise to practices.

2) Results-Security Incidents

Reassuringly the bulk of practices (nearly ¾) indicated they have not suffered an IT Security incident effecting the security or confidentiality of patient data. A small percentage (16.5%) indicated they did experience an incident. When investigated further the vast majority (90%) suffered less than five incidents. According to the categories defined in the NHS IT Security manual, these were Minor (affecting an isolated individual). Where an incident occurred this was reported to the senior partner in almost all cases. No incident resulted in financial damage.

An analysis of the security incident identified the most common being unauthorised individuals accessing data. Only one practice each respectively, defined a security incident they suffered as arising as a result of either a virus infecting machines, failure to dispose of paper or electronic records correctly, or failure to ensure backup data was adequate or passwords being shared between users. All practices which indicated they suffered a security incident implemented a plan to resolve security weaknesses within one month.

3) Results- Risk Assessment

Nearly half (48%) of practices performed a risk assessment. Nearly a third did not know if a risk assessment had taken place. Where a risk assessment was performed a fifth used a senior partner, a quarter the IG lead. The PCT IT Security Officer was used by one practice as was the information asset administrator. No practice used an IT Consultant.

Only one practice indicated they used CRAMM as the risk analysis method. No use was made of either ITSEC or SAFE. The remainder indicated the risk analysis method used was unknown. Interestingly, no practice sought advice or guidance on IT Security from reviewing the BS7799 standards or NHS Security Manual controls matrix. A quarter indicated they referred to the Risk Analysis and Risk Management volume of the NHS Security Manual. Most used other sources of guidance. The bulk of practices (75%) would like more training or support with IT Security and information governance.

4) Results- Greatest Risk to Systems and Data

Practice Managers perceived the greatest risk to securing their IT Systems and patient data came from insecure exchanges of data with secondary care professionals or clerical staff being unaware or their roles and responsibilities. Over half of practices perceived some of the lowest risks to arise from insider abuse, unauthorised access to systems, or loss of data via portable devices (USB, PDA or phone).

It was indicated by the majority of practices were most confident with exchanging data with other Scottish GP's, hospitals or labs. Least confidence was expressed where data was exchanged with pharmacies, researchers or secondary care professionals.

5) Results-Current Threats to Security of Systems

Practice Managers felt there were a number of threats to the security of IT Systems and patient data. These could be classified as Security, Transfers and Training. In terms of Security, the sharing of passwords between staff, staff failing to logout of systems leaving an unattended logged in system,

and maintaining lists of multiple passwords to many systems were the most common perceived security threat. A single login may alleviate this problem whilst providing a reliable audit trail. Transfers of data via fax were seen as a major threat as errors can easily lead to data being sent to the wrong person. Training was an issue covering a range of threats reported by a few practices each. This includes better training to ensure staff conversations could not be overheard, raising the awareness of Data Protection responsibilities amongst staff and training to ensure staff do not leave paper based records lying in the open where they could be viewed or stolen.

6) Results- Main Challenges

The main challenges facing General Practice in the next two years were varied. Primarily this was how increasingly integrated systems could be secured to ensure only appropriate personnel gained access to data without any leakage. A corollary of this was the need for training. However underlying these was the perennial problem of funding. Managers felt a wider share of the PCT or Health Board funds should be devoted to IT in GP surgeries.

Importantly several indicated the sheer volume of data coming into practices and the many systems GP's now had to access could easily lead to important data being missed. GP's had to action their Docman mail, their EMIS tasks, Lab results, SCI-Gateway referral box, to find all the information for each day.

7) Results- Improvements to enhance IT use in the Practice

Hardware, Support and System Design are key areas where improvements could enhance the use of IT within practices. It was almost universally reported hardware issues was the prominent area for improvement. Either machines were old, outdated and slow or the external communication links used by practices were inadequate. Again the issue of funding was crucial to this. As independent contractors GP's do not procure hardware assets or software applications often making do with what has been provided by the Health Board. A key improvement would be to review IT budgets and purchasing regimes.

Better support for practices encompassing both IT hardware and training was widely regarded as a key enhancement. Training in new applications is often not factored into hosted organization's budget as highly as it ought to. Implementation of the increasingly e-Health driven agenda does not take account of workforce skill mix issues on the ground in primary care. More widespread training for non Vision users was also requested.

8) Results- Enhancements PCT could initiate

Enhancements to the system produced some worthy areas for improvement. A large number of practices requested a single unified logon even suggesting finger print or smart card access would reduce the wide variety of passwords. To quote a practice manager, "Currently I have 12 login's and passwords to remember and change every month - too many".

Other suggested system improvements included requests for better GP2GP transfers for Vision. Specific screens for administrative staff to enter details without displaying clinical information about patients but would allow clerical staff to input administrative information, telephone calls, or appointment messages. Web based facilities for patients to book appointments and request repeat scripts were suggested. The facility for user feedback into systems design to facilitate rapid improvements and the use of standardized data extraction software was also suggested.

Related to this is improved design of integrated systems. This would enable better communications with hospitals, easier to transfer patient records from one practice to another, labs linking directly into the patient record, and the ability to use systems whilst at home to complete outstanding paperwork or access records whilst on home visits.

Whilst a wish list of improvements to enhance the systems is useful, practice managers considered the PCT could better protect patient data. Some suggestions were to ensure all communications between sites and departments were encrypted; provide a more secure mechanism for sending faxes to reduce the risk of human error; to provide a more effective education and training regime and improving access to the system. This latter element could be used to provide access for locums to practices on the day they are needed.

Some comments in this area are interesting. One practice manager suggested the emphasis be moved from "protecting data to systems that can SHARE data safely for the benefit of patients. We give too much emphasis to PROTECTING and not nearly enough on better ways to SHARE data. This is why we see failures in care throughout the UK". In order to reduce workload and enhance security one practice thought it best if the PCT ensure all research data is gathered centrally and pass it to researchers.

9) Untoward Security Incidents Reported to Health Boards

Like the concerns raised by the Information Commissioner, a clear risk is presented by theft or loss of equipment containing data. However, a number of incidents were reported involving staff sharing logon's. Breach of existing policies accounts for another large number of reported incidents. Given the lack of complete data, only eight boards provided useable responses, it was not possible to correlate the responses with organisation status to determine whether hospitals or GP Surgeries were the most likely to present data risks.

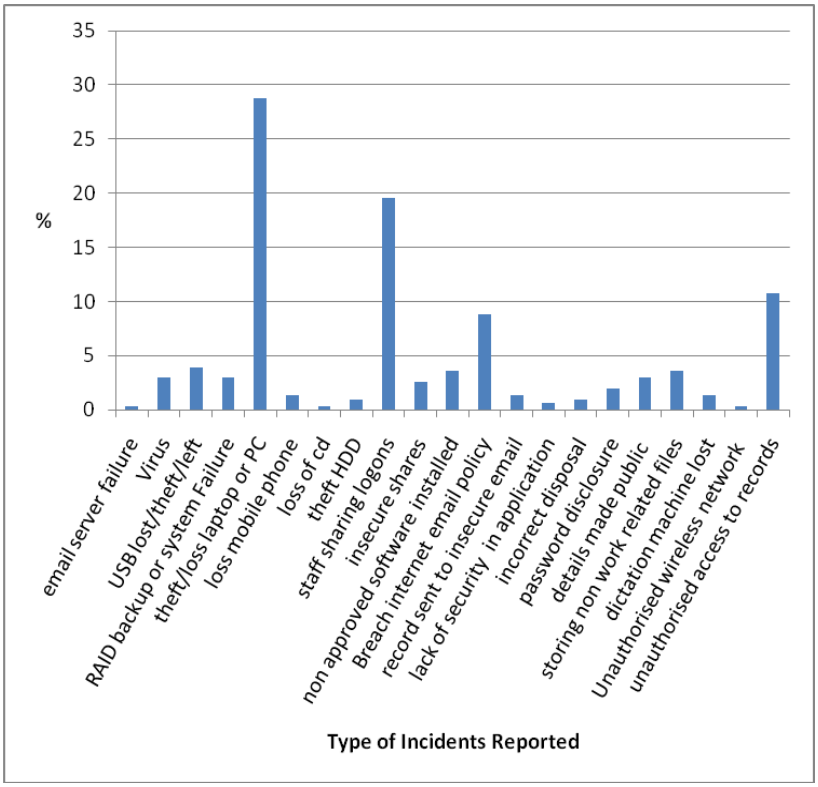

Figure 2 Details of Reported Incidents (Obtained by FOI)

I. Conclusions

The results may be useful to policy makers and Primary Care Staff alike as it provides some guidance for the disbursal of scare funds in a tight spending round to provide cost effective methods of ensuring compliance, protecting sensitive health data and avoiding hefty fines. The English IG results provide some background in which reasoned decisions can be made: over 50% failing to meet green standard in Confidentiality, Data Protection and nearly, 40% failing in Security. This is despite over two decades of legislation in the field and seven versions of information governance. There were examples of good practice. These include the introduction of encrypted laptops throughout the Board area (NHS Grampian), contacting effected individuals after incidents (NHS Lothian even won an award), banning USB devices (NHS Forth Valley).

The results provide an insight into the current industry view of risk. The low level of risk analysis and limited use of standard IT Security Risk Analysis Methods, demonstrate a movement away from risk as the sole measurement of success. The IG framework places little emphasis on risk assessment (two out of several criteria refer to this), this itself supports Mattord and Parkers view. Regulatory compliance should be the goal. It is interesting both authors refer to due diligence.

Whilst there will always be the ever present threat of theft or loss of equipment it is paramount data on all devices be encrypted and password protected. The possibility of an immense fine of £500,000 for data security breaches may prompt better compliance. The threat of such a sanction may redress the current drift to ensure the reaction is a higher level of regulatory compliance. However, only better awareness and training can ensure all data held within Primary Care is encrypted and password protected. Before the PCT tier is removed from the NHS Structure in England consideration should be applied to ensuring how the governance standards can be attained and patient data secured amongst independent contractors who currently face difficulties in compliance. Perhaps we should take heed of Ross Anderson, professor at the Cambridge University Computing Laboratory who when commenting upon plans to allow thousands, inside and outside the NHS, access to the summary care record: "We do need to automate medical records-but we need to do it right." (Anderson, 2010)

II. References and Bibliography

Anderson, R. (2010). Do summary care records have the potential to do more harm than good? Yes. British Medical Journal , 340, c3020.

Appari, A., & Johnson, E. (2009). Information Security and Privacy Research in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management .

Appari, A., Anthony, D., & Johnson, E. (2009). HIPAA Compliance: An Examination of Institutional and Market Forces.

Appari, A., Anthony, D., & Johnson, E. (2008). Which Hospitals are Complying with HIPAA: An Empirical Investigations of US Hospitals.

BJHCIM . (2010 c, June 28). IT Security Professionals still failing in mobile security. Retrieved August 3, 2010, from BJHCIM News: http://www.bjhcim.co.uk/news/2010/n1006041.htm

BJHCIM. (2010 a, July 13). One in ten trusts have insecure IT Systems. Retrieved August 3, 2010, from BJHCIM: http://www.bjhcim.co.uk/news/2010/n1007005.htm

BJHCIM. (2010 b, May 6). USB Stick data loss by Scottish hospital could be a pivotal case for ICO. Retrieved August 3, 2010, from British Journal of Healthcare Computing and Information Management: http://www.bjhcim.co.uk/news/2010/n1005016.htm

Bridgehead Software. (2010). The Data Management Health Check Survey 2010. Ashtead, London: Bridgehead.

Clearswift. (2010). Data Leakage: The Stealth Threat to Business. Redwood City, CA: Clearswift.

Crown. (1984). The Data Protection Act 1984.

Crown. (1998). The Data Protection Act 1998.

Department of Health & Royal College of General Practitioners. (2005). Good Practice Guidelines for general practitioners electronic patient records (version 3.1). Department of Health .

Department of Health. (2010 d). Excellence and Quality: Liberating the NHS. London: Crown.

Department of Health. (2010 a, August 12). Information Governance Toolkit Knowledgebase. Retrieved August 12, 2010, from Information Governance Framework: https://www.igt.connectingforhealth.nhs.uk/KnowledgeBase.aspx?tk=403496785370438&lnv=5&cb=16%3a29%3a24&sViewOrgType=4&sDesc=General+Practice

Department of Health. (2007). Information Security Management: NHS Code of Practice. London: Department of Health.

Department of Health. (2010 c, March 31). Organisation Assessment Report. Retrieved August 12, 2010, from Information Governance Toolkit: https://www.igt.connectingforhealth.nhs.uk/ReportsOrganisationChooser.aspx?tk=403499140314365&lnv=6&cb=22%3a31%3a19&reptypeid=1

Doyle, J. (2010, June 25). NHS loses 800 patients' private files everyday. Retrieved August 3, 2010, from Daily Mail: http://www.dailymail.co.uk/news/article-1289629/NHS-loses-800-patients-private-files-day.html

Gordon, L., & Loeb, M. (2008). Information Security and Risk Management. Communications of the ACM , 51 (4), 64-68.

Gordon, L., & Loeb, M. (2002). The economics of information security investment. ACM Transactions on Information and System Security , 5 (4), 438-457.

ICO Undertakings. (2010, August 12). ICO Press Releases 2008-2010. Retrieved August 2010, 2010, from Information Commissioners Office: http://www.ico.gov.uk/news/press_releases.aspx

Information Commissioner. (2010). Information Commissioner's Annual Report 2009/10. London: The Stationary Office.

Kolkowska, E., Hedstrom, K., & Karlsson, F. (2009). Information Security Goals in a Swedish Hospital. In G. Dhillon (Ed.), Proceedings of the 8th Annual Security Conference Discourses in Security Assurance and Privacy, (pp. 16,1-11). Las Vegas.

Mattord, H. (2007). Rethinking Risk based Information Security. Information Security Curriculum Development 07. Kenneshaw, Georgia, USA.

McGraw, D., Dempsey, J., Harris, L., & Goldman, J. (2009). Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange. Health Affairs , 28 (2), 416-427.

Morris, A. (2010, May 3). NHS Chiefs waste six weeks hunting for memory card. Retrieved August 3, 2010, from Edinbrugh Evening News: http://edinburghnews.scotsman.com/healthofthenhs/NHS-chiefs-waste-six-weeks.6268440.jp

NHS Careers. (2010, August 3). NHS Careers. Retrieved August 3, 2010, from NHS: http://www.nhscareers.nhs.uk/details/Default.aspx?Id=796

NHS Connecting for Health. (2009). Information Governance Toolkit v7 :Getting Started for General Practice. London: Department of Health.

Office Information Commissioner. (2009). undertaking Dr P Thomas.

Parker, D. (2006, May). Making the case for replacing risk based security. The ISSA Journal .

Price Waterhouse Coopers. (2010). Information Security Breaches Survey 2010. London: Price Waterhouse Coopers.

Scottish Government. (2008, August 28). e-Health Strategy 2008-2011. Retrieved August 1, 2010, from NHS Scotland e-Health: link:http://www.scotland.gov.uk/Publications/2008/08/27103130/0

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. International Conference on Availability, Reliability and Security, (pp. 258-261). Krackow, Poland.

Table 1:

Date	Board	Undertaking
14 08 2010	Birmingham Children's Hospital NHS Trust	1.Theft of two laptops containing 17 patients details
15 06 2010	NHS Stoke on Trent	1.2,000 record missing from paper file system
22 01 2010	Southampton University Hospital Trust	1.Theft of laptop containing 33,000 patient details
13 11 2009	Great Yarmouth and Waveney NHS Primary Care Trust	1.Theft of two desktop PC's containing 1,000 details of patients and staff
11 11 2009	Maidstone and Tunbridge wells NHS Trust	1.Theft of unencrypted laptop containing 33 patient details and others over a period form 2003-2006.
14 09 2009	NHS Grampian	1.Email distribution of an individual's records 2.loss of 200 patient/staff records 3.theft laptop 1500 patient records
08 09 2009	NHS Education Scotland	1.Theft of laptop containing details of 6377 individuals
28 08 2009	NHS Lothian	1. Temporary loss of 25 records 2. Loss USB Stick 137 patient details
14 08 2009	East Cheshire NHS Trust	1.Patient register containing details of 60 patients found in a garden 2. Open skip used to destroy records
12 08 2009	Gripping Valley Practice	1.Practice Server found in car park with patient and employee details
29 07 2009	Imperial College Healthcare NHS Trust	1.Theft of 6 laptops containing 6,000 patient details
15 07 2009	Surrey and Sussex Healthcare NHS Trust	1.Loss of ward handover sheet with 23 patient details 2.Theft of two laptops containing 80 patient details
15 07 2009	Chelsea and Westminster NHS Hospitals Trust	1.Theft of memory stick containing 143 patient details
15 07 2009	Hampshire Partnership NHS Trust	1.Theft of a laptop containing 349 patients and 258 staff
15 07 2009	Royal Free Hampstead NHS Trust	1.Loss of disk containing 20,000 records
15 07 2009	Epsom and ST Hellier University Hospitals NHS Trust	Insecure storage of patient data
04 06 2009	Salford Royal NHS Foundation Trust	1.Theft of laptop 3500 patient details
30 04 2009	North West London Hospital	1.Theft of 2 laptops holding 181 patient details 2. Theft PC 180 patient details
07 04 2009	Stockport NHS Foundation Trust	1.Theft of laptop containing 1588 patient details
07 04 2009	St Georges Healthcare NHS Trust	1.Laptop Computers stolen containing 22,000 patients
23 03 2009	Camden Primary Care Trust	1.Loss of redundant computers containing details of 2,500 patients
05 02 2009	Brent Teaching Primary Care Trust	1.Theft of two laptops containing 389 patient details
22 01 2009	Abertawe Bro Morgannwyg University NHS Trust	1.Theft of laptop containing 5,000 patient details
22 01 2009	Tees, Esk and Wear Valleys NHS Foundation Trust	1.Loss of USB stick, later handed to press, containing personal and staff details.
20 01 2009	Southampton City Primary Care Trust	1.Loss of 168 employee payslips
26 11 2008	NHS Lanarkshire	1.Personal data found in former hospital grounds
26 11 2008	NHS Tayside	1.Personal data found in former hospital grounds
22 10 2008	Kings College London	1.Theft of mac and several laptops containing 45 patient details. 2.Theft resulting in loss of 150 dental patients records