INFORMATICS IN PRIMARY CARE

Research article

Privacy protection for personal health information and shared care records

Roderick L B Neame

Health Information Consulting Ltd, Homestall House Low Barn, Homestall Lane, Faversham, Kent ME13 8UT, UK

Cite this article: Neame RLB. Privacy protection for personal health information and shared care records. *Inform Prim Care*. 2014;21(2):84–91.

http://dx.doi.org/10.14236/jhi.v21i2.55

Author address for correspondence:
Roderick L B Neame
Director, Health Information Consulting Ltd
Homestall House Low Barn
Homestall Lane, Faversham
Kent ME13 8UT, UK
Email: roddyneame@health-informatics.co

Accepted February 2014

ABSTRACT

Background The protection of personal information privacy has become one of the most pressing security concerns for record keepers: this will become more onerous with the introduction of the European General Data Protection Regulation (GDPR) in mid-2014. Many institutions, both large and small, have yet to implement the essential infrastructure for data privacy protection and patient consent and control when accessing and sharing data; even more have failed to instil a privacy and security awareness mindset and culture amongst their staff. Increased regulation, together with better compliance monitoring, has led to the imposition of increasingly significant monetary penalties for failure to protect privacy: these too are set to become more onerous under the GDPR, increasing to a maximum of 2% of annual turnover.

Objective There is growing pressure in clinical environments to deliver shared patient care and to support this with integrated information. This demands that more information passes between institutions and care providers without breaching patient privacy or autonomy. This can be achieved with relatively minor enhancements of existing infrastructures and does not require extensive investment in inter-operating electronic records: indeed such investments to date have been shown not to materially improve data sharing.[1]

Requirements for privacy There is an ethical duty as well as a legal obligation on the part of care providers (and record keepers) to keep patient information confidential and to share it only with the authorisation of the patient. To achieve this information storage and retrieval, communication systems must be appropriately configured. There are many components of this, which are discussed in this paper. Patients may consult clinicians anywhere and at any time: therefore, their data must be available for recipient-driven retrieval (i.e. like the World Wide Web) under patient control and kept private: a method for delivering this is outlined.

Keywords: Electronic medical records, information privacy, medical record sharing, shared care

What this paper adds Many record keepers strictly limit sharing of information with colleagues on the grounds of privacy concern, and the members of staff expose private data to risks simply because they do not understand those risks. Even where those privacy concerns are not the issue, record keepers may still be unable to share information because of the difficulty of obtaining access to it, and of retrieving files that are compatible with the recipient's reader systems. This paper summarises the key issues that must be addressed in configuring a system that properly protects privacy. It outlines how data can be readily shared without the need for costly investment in inter-operating systems. In addition, it indicates how patients can be put in control of access to their own records—if they so choose.

HEALTH INFORMATION AND PRIVACY

Personalised information is generally private. The ethical principle of respect for personal autonomy holds that an individual should be in control of their own person, as well as their own information, and the law supports this through several different bodies of legislation. The health information privacy 'problem' arises because every medical record typically contains elements of context (names, addresses, dates, places, clinics, and so on) routinely embedded in the stored clinical data (content). There is a demand for that information because it is of value not just to care providers, but also to others—such as financiers, employers, and solicitors—and even more so where the patient concerned is a celebrity. Historically, where records were kept on paper, storing context with the content was essential to ensure that the record stayed associated with the correct patient and was stored in the same folder as their other records: there was no other tag for checking that the records in a specific folder actually were associated with that patient. However, that is no longer necessary with electronic records systems.

It is widely accepted that the patient does not own the physical substance of their medical records: ownership is vested in the doctor, clinic, or institution that created the records. However, their ownership is effectively limited to little more than a custodial role as the owner cannot sell, edit, or destroy content in the medical records, and must make them available to the patient and his nominated agents and care providers, although there may be some limited right on the part of the custodian to restrict what the patient and his agents can access. The owner does not even have the right to share the records, whilst they remain identifiable, with third parties except with the consent of the patient.[2] Therefore, control over what can be done with the records, whilst they remain identifiable, is effectively vested in the patient, and the records must otherwise be kept private and confidential.

In a previous issue of IPC, Harrison and Booth[3] explored how individuals might become guardians of their own data and digital identities, including alternate identities; they outline their virtual home concept in which individuals have an online 'space' where they can store data, or links to data held elsewhere, and which could act as their authentication and privacy agent. In a more recent issue of IPC (2008), Neame[4] addressing the same theme outlined a schema for managing health care (patient and professional) identification/authentication services using tokens (e.g. smart cards) for authorisation of record access. This paper draws on ideas put forward in both those articles, as well as relevant work by Schoenberg and Safran,[5] whose interest was in finding a means for exchanging patient information with privacy and using the Internet (discussed below).

KEEPING RECORDS PRIVATE

Whilst electronic records were still in an early stage of their development, Anderson[6] as long ago as 1996 set out a series of nine privacy policy principles (Figure 1) relating to their management and sharing. The framework applies only to personally identifiable information, and remains generally sound today: however, failure to implement the principles is widespread.

1. Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the access control list from accessing the record in any way.
2. A clinician may open a record with herself and the patient on the access control list. Where a patient has been referred, she may open a record with herself, the patient, and the referring clinician(s) on the access control list.
3. One of the clinicians on the access control list must be marked as being responsible. Only she may alter the access control list, and she may only add other health care professionals to it.
4. The responsible clinician must notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. His consent must also be obtained, except in an emergency of in the case of statutory exemptions.
5. No-one shall have the ability to delete clinical information until the appropriate time period has expired.
6. All accesses to clinical records shall be marked on the record with the subject's name, as well as the date and time. An audit trail must also be kept of all deletions.
7. Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.
8. There shall be effective measures to prevent the aggregation of personal health information. In particular, patients must receive special notification if any person whom it is proposed to add to their access control list already has access to personal health information on a large number of people.
9. Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be subject to evaluation by independent experts.

Figure 1 Anderson's nine principles[6]

PRIVACY BREACHES ARISE PRINCIPALLY FROM FIVE SOURCES

1. Inadequate identification and authentication of individuals, allowing significant numbers of authorised system users to pose as someone else (using privileges belonging to another person).[7]
2. Ready accessibility of electronically stored information where unrestricted record access and read/write privileges are available to vastly more users than just those with a need to know and with the authorisation of the patient concerned; inadequate logging of user activity and monitoring of logs for abuses.
3. Inappropriate disclosure,[8] for example, where data have been exported from the institution (on paper, on memory media, in mobile devices/laptops, in communications, and so on) without authorisation, and/or whilst inadequately secured, and/or passed to a recipient where privacy protection measures are inadequate. Also disclosures made without patient authorisation.
4. Reporting requirements, some statutory and deriving from primary legislation, others arising out of departmental directives, and all requiring disclosures of personal information provided in confidence.
5. Poor security, failing to protect the system against external hackers, and malware; permitting users to access instant messaging[9] services and system 'back doors' (e.g. implemented for remote management), which permit external access to the system often bypassing security controls.

The demand for shared information for shared care is very strong and growing, and overly restrictive approaches to information exchange are not fit for the purpose and infringe patient rights (Panel 1).[10] Around half of the security breaches arise as a result of authorised users abusing their privileges,[11,12] and therefore no amount of blocking external access will solve the problem. On the other hand externally driven attacks are becoming increasingly common, with around 100,000 new malware variants appearing every day, and powerful hacker toolkits being readily available to buy or rent on the Web.

DISCUSSION

Personal health information has a value: unfortunately, its value is recognised not just within the health care sector, but also outside, and around one-third to one-half of all reported security breaches arise in the health care sector.[13,14] There is a significant financial incentive to acquire private health information for purposes such as decisions about employment and finance, and exerting improper influence. The issues associated with abuse of personal health information have led to public expectations of professional ethical behaviour dating back to Hippocrates more than two millennia ago, as well as modern legislation.

Amongst the most effective measures for privacy protection are the education of users, and the careful formulation of a contract between them and the record keeper, setting down user privileges and making abuses easy to litigate. In many instances, users are given information system access privileges, but not made explicitly aware of their responsibilities or limits, nor of the penalties for abuses. All authorised users must be identifiable, and authenticated, for example, by use of a smart token; and they must be held accountable for all actions undertaken on their account. Given that around half of the breaches arise as a result of authorised user actions, this is a vital area to address: some breaches are deliberate, but others are a result of poor IT practice and lack of basic IT education.[15]

Whilst there are legal bases for prosecutions in common law (breach of fiduciary duty), as well as in statute (under data protection, privacy, and human rights law), obtaining a conviction may not be easy, and the penalties they impose may be uncertain and inappropriate. Unfortunately, the impact of the EU Privacy directive (95/46/EC) (Panel 2)[16] has been limited, but this will be greatly strengthened by the introduction in mid-2014 of the General Data Protection Regulation (GDPR) (Panel 2).[17] At present, it is often better to set down penalties in an employment contract where enforcement is simpler. More significant in many instances are the penalties that can be imposed by professional associations for unprofessional/unethical behaviour, including expulsion from the association, which may affect the right to practice: this promotes the importance of self-regulation, although still requiring monitoring.

The not uncommon practice of 'borrowing' an identification/userID from someone else, or using 'common' UserIDs, such as the same one for all staff of a clinic or ward, or having 'floating' UserIDs for a given role (e.g. 'DutySurgicalRegistrar') are all incompatible with proper user identification and authentication: the actual user at a given time may not be known for certain. The security system must require that users are positively authenticated by some unique physical security element, such as a unique token, and/or a biometric identifier (e.g. fingerprint/iris/facial scan). Where a request for access emanates from an external IP address, and/or the user is unidentified, access should be restricted solely to 'public' data—although those 'public data' can readily be re-designed for sharing with privacy (see below).

Internal data processing is often overlooked as a source of privacy breach, but the routine practice of including personal identifiers with data being processed for internal management and claims purposes breaches privacy. Unless both clinical and personal information are required at the same time and place, they should be separated, and the data processed under an alternate code, such as the system-generated record or event identifier. Internal IT management is another potential source of breach: by the nature of their work, IT staff generally have access to all stored data, as well as to the security system that protects them. Having a procedure for active monitoring and oversight of all staff with access to sensitive data is vital, as is ensuring that they delete data that are no longer required in a way that prevents their subsequent recovery.

Confidential data in transit are always at risk from eavesdropping, since the communication channels are for the most part 'public'. Data are equally at risk when stored on portable media that can be removed from institutional control and are not secured (e.g. on notebooks and memory sticks), since misplacement of the device can lead to major disclosures. Therefore, encryption of data capable of being exported is essential where personal identifiers are included, and the use of asymmetric encryption, such as using a public key infrastructure,[18] is strongly recommended. Some or all of the technical and data processing services may be outsourced to contractors: just like the regular user contract, the outsourcing contract needs to address data protection and privacy issues, and include penalties for breach.[19,20] Passing data to a third party whose privacy protection and security measures are inadequate is a clear breach of the law on the part of the sender, whether or not it is an offence on the part of the recipient.

Ensuring that the system is not abused requires both preventive and detective security elements. Prevention is discussed above—but what about detection? In detective terms, there are options to implement keystroke logging so that it is possible to state definitively who did and saw what, and when. Patterns of access to records can be monitored and audited, and the system can be rolled back to any point in time to establish what information was available and viewed in making a specific decision.

CHECKLIST OF PRIVACY INFRASTRUCTURE REQUIREMENTS

A system for ensuring information privacy in electronic records systems must include

1. **Identification:** users must be uniquely identified, and their identities authenticated for issuance of a UserID, affording them privileges for the use of the system.
2. **User contract, privileges, and penalties:** users must have a clear understanding of their system privileges and responsibilities set out in the form of a binding user contract, including penalties for abuses. The contract acts as a guide to users to self-regulate their actions and, together with the user logs, can be the basis for proceedings for abuses.
3. **Prevention by access control:** the system should be configured to prevent users accessing records and functions, for which they have no authorisation, for example, through the use of application access rights and individual file access tables. Where this is not technically possible, activity monitoring should be comprehensive.
4. **Detection by logs and audit:** every action by every user must be tracked using a data logging system, which records UserID, dates, times, terminal identity, and keystrokes. This makes it possible to reconstruct exactly what that user saw and did, as well as to analyse the data logs to audit for activity patterns that are unusual and could suggest impropriety. Frequent routine monitoring of logs is essential.
5. **Export and outsourcing control:** where data are in a form that may be exported from the security controls of the system, that export must be duly authorised, the recipient or responsible party identified, and the recipients privacy and security provisions approved. The data exported should be the minimum consistent with the purpose, and its security assured (e.g. by de-identification and/or encryption)
6. **Record processing:** Data should not be processed (e.g. for business management, finance, or planning), with both identifiers and clinical details displayed except where access to both is essential for the purposes, hence preventing unnecessary disclosures of personal records.
7. **Definitive disposal and destruction:** where personal data are consigned for destruction, steps must be taken not only to 'delete' the file(s), but also to ensure that the deleted files cannot be recovered either from the deleted media or from backup/archived copies.
8. **Technical staff oversight:** IT staff, both internal and external/contractors, are likely to have the technical capability to view anything as well as to conceal what they view/do from data logging, and even to lay false trails. Their activities should be overseen by supervisors and monitored to prevent breaches.
9. **Responsible officer:** an officer of the enterprise should be charged with responsibility for personal information privacy management, and required to make regular detailed reports to management, including audits. This will become a legal requirement under the GDPR for all institutions with more than 250 staff.

The above can assure the privacy protection of records, and, with the exception of record access tables (2 above), which may require application modifications, they should all be readily implementable on current systems. They should absolutely not become an index of excuses for failure to share records.

SHARING DATA FOR SHARED CARE

Sharing care data is increasingly essential: the Caldicott Report[10] is clear that too many institutions hide behind 'data protection' as a reason not to share data, and proposes making 'non-sharing' an offence. The key to the private sharing of data is placing the patient in control of their own records and of who may access them. Schoenberg and Safran[5] outlined a scheme for an Internet-based but confidential medical records repository: the scheme proposed the Web as the communication medium, although the record repositories relied heavily on being secured through the use of names, passwords, and numbers (e.g. NHS number). The problem with such national numbers is that too many individuals have access to the name:number lookup tables for any effective privacy, and such an approach will not be acceptable under the GDPR. Schoenberg and Safran argued against the use

of memory tokens on the basis that the public did not appear to like them: the public appear to love them based on the vast numbers of smart cards in everyday use for banking, mobile phones, store cards, and so on.

The scheme proposed here is based on the same ideas, but ensures that the data remain private and confidential. Patients would be provided with an index of their care events and resulting records made, together with a URL pointer to where specific records can be found. The index can be held on a memory device, preferably secured with a PIN, which 'points to' the URLs where each record is stored on the Internet. Alternatively, these data can be uploaded to the patient's secure Internet depository, which they can access to retrieve records, or pass them to another party. The records to which this index points will be secured against external or internal privacy abusers. They may be encrypted versions of the original (decryption keys held on the index) or an edited version of the original where identifiers (names, dates, places, clinics, and so on) have been erased, leaving just the clinical data: either method makes the records readily accessible but valueless except to those who hold the context and keys. Alternatively, the records and/or index can be uploaded to a place nominated by the patient—for example, their personal secured depository on the Web. Any clinician with a browser and the patient index device (or their depository keys) can thus reassemble and read full records of the patient as and when they require them. This scheme has no need for development of complex inter-operable systems, as it currently seems to be the preferred, but costly, way forward.

The information for sharing can be structured for greater utility (e.g. using XML tags), and can include internal integrity checks: more detail is provided elsewhere.[21]

CONCLUSION

The paper presents an overview of the practical information privacy issues that record keepers must address as a matter of priority: privacy enforcement is becoming stricter, and breaches may incur a major financial penalty. The main sources of breaches are identified, together with effective actions to prevent them: with minor exceptions none of these should present major implementation issues, but there seem to be problems of mindset and education which mitigate against this.

Cost-effective methods for sharing information while respecting privacy are desperately needed. There is no need for major investments in interoperability of systems: the sharing of data can readily be achieved with existing electronic information management infrastructures with the simple addition of an option for patient control (possibly but not necessarily using an identification and control device, such as a smart card), and a routine for posting secured copies of records on the Internet.

Further research/work

Two infrastructure developments are necessary for the sharing scheme to function efficiently. One is that those patients who want to avail themselves of the ability to take control of their records need to be provided with a smart memory device that identifies them, and can carry pointers to where their records are stored, as well as encryption keys and additional context where needed. An alternative would be for them to have an online secure deposit facility into which these details are passed. The other is that care service providers and institutions would need to generate encrypted or de-contextualised sharing records (in HTML) stored on the Web or in the patients secure online deposit facility. All the other technology required is already in place and needs minimal additional investment.

APPENDIX

PANEL 1

Caldicott Reports 1 and 2

The UK Health and Social Care Act[a] (2012) makes strong arguments in favour of NHS reforms to contain costs and improve services. In particular it aims to find ways of joining up the currently fragmented care records, of responding to what patients are saying, and of increasing accountability (highly relevant in the context of recent revelations about poor performance and avoidable deaths in various trusts). To achieve these, the Act paves the way for ready access to care-related information ('evidence') to support commissioning, to assure quality, and to inform best practices, whilst at the same time making clear the need for this to be achieved with full patient confidentiality.

Some 20 years ago in 1997, Dame Fiona Caldicott was asked to review the issue of protection of patient confidentiality at a time when the newly formed 'internal market' was sharing data more freely than was perhaps ethical or legal. This resulted in a report[b] that identified concerns and set out some basic principles. Amongst these were

- Need to replace as far as possible patient identifiers with other tags, with a specific caution that where coded identifiers or NHS numbers are used, there must be strict control over who may have access to the identity look-up tables (recommendations 8,9,13,16).
- Need to restrict the amount of data transferred to the minimum consistent with the needs (Executive Summary V).
- Need to encrypt sensitive messages passing outside the institution (recommendation 10).

Dame Fiona Caldicott was again charged with looking again at the issues of data sharing and privacy protection and reported[c] in 2013. The specific context is the failure by many institutions to share information with others, citing judicious information governance as the impediment. The central issue is the balance between individual privacy and the best interests of the community in terms of the care for others and improvements to services informed by access to private data, and a critical problem is the lack of awareness and understanding of the issues and regulations that pertain.

The recent announcement[d] that government will seek to acquire without consent patient identifiable information from primary care to be placed in a centralised database for access by researchers suggests a significant change to the current arrangements whereby patients have the right to opt out of having their personal information uploaded to the summary care record.[e] The proposed omission of names and addresses, to be replaced by NHS numbers, does not suggest any sort of robust approach to privacy protection (see paper).

[a] http://www.dh.gov.uk/health/2012/06/act-explained/

[b] http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

[c] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

[d] http://www.commissioningboard.nhs.uk/everyonecounts/

[e] http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/faqs/mpsfaqs.pdf

PANEL 2

EU Privacy Directive 95/46/EC and new Draft European General Data Protection Regulation

Information privacy and data protection became a significant issue when diverse national approaches to the issue began to impede free data flows. In 1980, the OECD set out a series of principles[f] to address this, but these were not legally binding or enforceable, which led to the European Directive 95/46/EC.[g] This Directive did not automatically become part of national privacy legislation, but required implementation through national legislation—which was done with variable rigour and sympathy for the core principles. These could be summarised as

Purpose: subjects should be clear about the purpose of the data being collected, and consent to it; the data collected should be the minimum consistent with achieving the stated purpose.
Storage: personal data should be stored securely against all threats and abuses.
Use: personal data should be used only for the purposes declared at the time of collection, and nothing else.
Disclosure: personal data should not be disclosed without the consent of the subject.
Correction: data subjects should be able to access their personal data and require corrections to be made where these were necessary.
Destruction: personal data should be kept only until the purpose of their collection has been achieved, and should then be destroyed.
Responsibility: data controllers should be held accountable to the data subjects for their adherence to the principles of the Directive.

The variability in legislation bringing these principles into practice at the national level led in 2012 to the EU preparing a General Data Protection Regulation,[h] reinforcing and extending the basic principles. This differs legally from the original Directive in that a Regulation requires no enabling national legislation but is automatically incorporated into and takes precedence over national legislation in all member countries, thereby at a stroke harmonising data protection across the Union. The Regulation when introduced in mid-2014 will replace all provisions of and derogations from the Directive.

The Regulation, although not yet finalised, promises significant change particularly by strengthening individual rights, increasing the responsibilities and accountabilities of data controllers (DC), and increasing the monitoring and enforcement by data protection authorities (DPA). Perhaps most significantly, penalties for failure to comply rise from the previous maximum of £500,000 to a maximum of 2% of annual turnover, a figure guaranteed to command the attention of CEOs, and likely to persuade Boards of the advisability of investing urgently in privacy infrastructure and education. Of particular significance for health care, the Regulation strengthens the requirement that any use of personal data, other than for the sole purpose for which they were gathered, requires subject consent. In addition, it excludes the fact of the use of a service as giving 'implied consent' to other uses of the data, leaving the burden of proof of properly obtained consent with DCs. It makes notification of breaches to DPAs within 24 h a duty of DCs. It requires businesses to provide accessible and transparent policies regarding processing of personal data as well as exercising data subjects rights. It includes a personal right to be forgotten and to data erasure, as well as a right to data portability to move to another service provider. It clarifies that data collected under EU law can only be processed consistent with EU law, even if the data are exported into another approved jurisdiction where local laws differ. In addition, it makes all parties to any infringement of the Regulation jointly and severally liable in law. All of these will have a considerable impact on health care institutions.

[f] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[g] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[h] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

REFERENCES

1. Kellermann AL and Jones SS. What it will take to achieve the as-yet-unfulfilled promises of health information technology. *Health Affairs* 2013;32(1):63–8 Available from: http://networkingdefinition.bringthegame.info/153/more-changes-in-health-care-needed-to-fulfill-promise-of-health-information-technology/. http://dx.doi.org/10.1377/hlthaff.2012.0693. PMid:23297272.
2. Medical Protection Society. Access to health records. (Internet cited 07 February 2013). Available from: http://www.medicalprotection.org/uk/england-factsheets/access- to-health-records.
3. Harrison J and Booth N. Applying new thinking from the linked and emerging fields of digital identity and privacy to information governance in health informatics. *Informatics in Primary Care* 2003;11:223–8. Available from: http://www.ingentaconnect.com/content/rmp/ipc/2003/00000011/00000004/art00007.
4. Neame R. Privacy and health information: health cards offer a workable solution. *Informatics in Primary Care* 2008;16(4):263–70. Available from: http://www.ingentaconnect.com/content/rmp/ipc/2008/00000016/00000004/art00003. PMid:19192327.
5. Schoenberg R and Safran C. Internet-based repository of medical records that retains patient confidentiality. *BMJ* 2000;321(7270):1199–203. Available from: http://www.bmj.com/content/321/7270/1199.1.
6. Anderson R. *Security in clinical information systems*. Ver 1.1 1996 (Internet cited 26 July 2012). Available from: http://www.cl.cam.ac.uk/~rja14/policy11/policy11.html.
7. Wiech D. Identity and password management in healthcare. *Identity management solutions*. (Internet cited 26 July 2012). Available from: http://identitymanagementsolutions.blogspot.fr/2011/04/identity-and-password-management-in.html.
8. UK Privacy Debacles. *Open rights group*. (Internet cited 26 July 2012) Available from: http://wiki.openrightsgroup.org/wiki/UK_Privacy_Debacles.
9. Hindocha N. Instant insecurity: security issues of instant messaging. 2003. (Internet cited 07 February 2013). Available from: http://www.symantec.com/connect/articles/instant-insecurity-security-issues-instant-messaging.
10. The Information Governance Review 2013. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf.
11. PR Newswire. Leading cause of data security breaches are due to insiders, not outsiders. (Internet cited 07 February 2013). Available from: http://www.prnewswire.com/news-releases/leading-cause-of-data-security-breaches-are-due-to-insiders-not-outsiders-54002222.html.
12. Verizon. 2010. *Data breach investigations report*. (Internet cited 07 February 2013). Available from: http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.
13. Patel H. What are the most common causes of security breaches? *Help net security*. (Internet cited 07 February 2013). Available from: http://www.net-security.org/article.php?id=959.
14. Secnap Network Security. *Healthcare industry is under-prepared to protect patient privacy*. (Internet cited 07 February 2013). Available from: http://www.secnap.com/support/whitepapers/healthcare-privacy-report-pwc.html.
15. SC Magazine. Healthcare professionals show poor practice when it comes to security. 2008. (Internet cited 07 February 2013). Available from: http://www.scmagazineuk.com/healthcare-professionals-show-poor-practice-when-it-comes-to-security/article/121277/.
16. Directive 95/46/EC of the European Parliament and of the Council. 1995. Official Journal of the European Communities No 1 281/31. Available from: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
17. Proposal for a Regulation of the European Parliament and the Council (General Data Protection Regulation) 2012. (Internet cited 30 January 2014). Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
18. NHS Connecting for Health. Cryptography and the Pathology Messaging Enabling Project. (Internet cited 07 February 2013). Available from: http://www.connectingforhealth.nhs.uk/systemsandservices/pathology/edifact/security/crypto_v5/.
19. Davino M. Assessing privacy risk in outsourcing. *Journal of AHIMA* 2004;75(3):42–6. Available from: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022546.hcsp. PMid:15029778.
20. Macfarlane J. Private medical records for sale: Harley street clinic patients' files outsourced for computer input—and end up on black market. Mail Online, 18 October 2009. (Internet cited 07 February 2013). Available from: http://www.dailymail.co.uk/news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input--end-black-market.html.
21. Neame R. Effective sharing of records, maintaining privacy: a practical schema. *Online Journal of Public Health Informatics* 2013;5(2). Available from: http://ojphi.org/ojs/index.php/ojphi/article/view/4344/3725.