Informatics in Primary Care 2008;16:263–70

Refereed papers

Privacy and health information: health cards offer a workable solution

Roderick Neame MA PhD MB BChir
Health Information Consulting Ltd

ABSTRACT

Collections of computerised personal health data present a very real threat to privacy. Access control is difficult to manage in order to maintain privacy and at the same time to retain flexibility of usage. The legal situation is clear, imposing a requirement to respect personal privacy and human rights. Primary users (those whose access is based on a duty of care) may exceed their authorisation and access records where they have no duty of care or need to know. Secondary users (those generating analyses, research reports and financial management data) may be given access to datasets containing identifiers which are not required for their work. The 'owners' of the data (e.g. government) may use them in ways that are inconsistent with the permissions under which the data were provided (e.g. by permitting links to other databases to create 'new' information), behind closed doors and without independent audit.

Currently there is a crisis emerging in which professionals are arguing that they are being compelled to compromise their ethical responsibilities to their patients, and government is responding that their measures are necessary to preserve access to quality data for research and planning. This paper proposes an integrated plan for managing these issues in a manner that is ethically sustainable, as well as in keeping with all provisions of the law, using a personal health card.

Keywords: ethics, law, privacy

Background

Recent events have highlighted one of the intrinsic weaknesses of computerised information resources: the attractions of storing more and more information in one place creates a higher risk of that information being improperly accessed. Copying large databases onto laptops and optical media makes them readily transportable, but also easily lost or stolen. Reports have catalogued numerous losses in the UK of government-held confidential and often personal information,[1–3] and there is evidence that public confidence is being eroded.[4]

It seems unlikely that the losses that have been declared give the full picture. Undoubtedly far more personal information has been improperly accessed and disclosed through authorised system users abusing their privileges – a largely unreported and unmonitored activity. Although it is notoriously hard to obtain figures relating to such losses occurring 'behind closed doors', a report by New Zealand's NSW Independent Commission against Corruption in 1992 on the unauthorised disclosure of government information stated: 'This investigation has disclosed a massive illicit trade in government information. That trade has been conducted with apparent disregard for privacy considerations, and a disturbing indifference to concepts of integrity and propriety.'[5]

A similar report from the UK Information Commissioner in 2006 confirmed that this trade has gone from strength to strength as the number, size and 'value' of these databases in public and private ownership has increased.[6]

Improper disclosure of some confidential information such as personal banking details and passwords can normally be remedied with little more than temporary problems – account details can be changed and financial restitution made, thereby restoring the status quo. But with other types of personal data, such as biometric and health information, no remedy is

possible as the information is 'permanent' and part of the person: once such information has been made known outside the environment in and for which it was provided in confidence, that information cannot subsequently be made secret again. Remedies provided for in law cannot change the fact of the disclosure, and may prove completely worthless to the subject.

Personal health information

All users of personalised information resources potentially threaten privacy. Primary users (those whose access is based on a duty of care) may exceed their authorisation and access and disclose records for patients when they have no duty of care or need to know. Secondary users (those generating analyses, research reports and financial management data) may be passed datasets containing patient identifiers which are not required for their work, therefore breaching the patients' right to privacy.

Primary uses

When patients consult a care provider, they do so with the expectation that their problem will be discussed in private and that the data shared between the two will be only that required for diagnosis and treatment, and for billing; and that providers will keep their own notes/records of each encounter. From the perspective of the patient that is, in a nutshell, the essence of the transaction as regards information. There is no doubt that having timely access to comprehensive health information about an individual can greatly facilitate his or her care, as well as reducing risks and costs. Some methods for sharing patient data between care providers have been developed but are limited by the diversity of point-of-care systems, data classification and coding methods, standards and communications between systems. Whilst there is a clear argument that greater sharing of data between professionals directly involved in the care of the patient is in his or her best clinical interests, there is an equally clear countervailing argument that sharing all or part of their personal record may not be acceptable to the patient, and the law supports this latter viewpoint.

Secondary uses

Secondary uses include a range of business, financial, quality assurance, audit, research, public health and marketing activities:[7] as these fall outside the explicit reasons for which the data was gathered, their disclosure should be subject to legal requirement for the informed consent of the patient. There are exceptions to this: the consent of the patient to limited secondary usage of their data may be given in the context, for example, of health insurance contracts where the contract can only be fulfilled if data is shared with the insurer; and patient consent is not required in relation to statutory instruments relating to public interest (e.g. in the context of notifiable communicable diseases). Of course the situation is different where the identity of the patient is removed from the data in such a way that re-identification of the individual becomes practically impossible.

Ethics, the law and privacy of health information

From an ethical standpoint, patient confidentiality is a long-established principle of health professional practice. Certainly all professional medical associations require their members to show respect for personal information and to keep it private and confidential – generally with severe penalties for improper disclosure.

In terms of the law, there are two key bodies of applicable legislation. One is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 which addresses the protection of individuals with regard to the processing of personal data.[8] The object of the 1995 directive is plainly stated in paragraph 1: 'to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.

There follows a definition of 'personal data':

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Clearly this includes all forms of personal health records and information, even where personal identifiers have been removed or encrypted but there remains sufficient data for the individual to be re-identified.

The other relevant legislation is the European Convention on Human Rights enacted in the UK in 1998.[9] Article 8 states that:

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This is backed up by article 13, which provides that: 'Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity'.

A recent case (20511/03) in the European Court of Human Rights has upheld this right to privacy, finding in favour of a Finnish national whose personalised health data, including her positive HIV status, had been improperly accessed by colleagues who had no duty of care towards her.

Further UK legislation enacted in 2002, the Health Service (Control of Patient Information) Regulations, permits the Health Secretary to exert effective control over all UK health information, including personal data.[10] This act states in section 7 that those engaged in secondary uses of these data must; 'so far as it is practical to do so, remove from the information any particulars which identify the person to whom it relates which are not required for the purposes for which it is, or is to be, processed'.

In other words if there are alternative ways of achieving the stated aims without infringing personal privacy and confidentiality, these must be adopted. The EU Privacy Directive permits secondary uses of personal data (article 7) where 'processing is necessary' in order to fulfil contractual arrangements and other statutory and legal obligations, but explicitly notes that the fundamental rights and freedoms of the data subject must be respected and preserved, so re-enforcing the provisions of the Human Rights Act. The Health Service Regulations of 2002 are subordinate to the requirements of EU-derived legislation where any conflicts may arise.

Ultimately personal medical records are confidential to the patient, whose express consent must be obtained before they can be shared whilst still personalised (unless one of the legal exemptions applies). Arguments based around an 'implied consent' model will always be mired in controversy and legal dispute: too much depends on who makes the implication and on what basis.

The NHS *Connecting for Health* project

The current stated aim of the NHS connectivity (*Connecting for Health*) project is to store relevant clinical information about every patient and to make it available to care service providers as, when and wherever required and also for secondary uses. Given adequate attention to security planning and implementation, there is no theoretical reason why the proposed system should not function as planned and comply with the law. The practical reality, however, is different: regardless of how well planned, implemented and maintained, history indicates that systems security will be breached, most often by authorised users abusing their privileges. Such an integrated store of clinical information would clearly create an attractive target for abuse, and its attraction would only increase with the quantity and quality of data stored within it. In practice the security framework seems less than adequately planned. In an informative review, Ross Anderson highlights some of the weaknesses:[11] in particular he raises serious concerns as to how the access control would function, and how it would embrace patients' rights to exercise control over their own data. It is already possible for the police, revenue, welfare and security services to access (behind government closed doors) many aspects of our private lives recorded in publicly held databases: the likelihood that the NHS confidential patient information resource would be similarly accessed is little short of a certainty, whatever assurances may be publicly provided.

Parameters of a sustainable solution

Principles

There are four principles that should be applied in this domain.

1 The patient should control who may see what of their records – they require a means to exert this control. Where the patient cannot participate (e.g. when unconscious) a means must be provided to by-pass this requirement, subject to audit.

2 There are few secondary data uses where the identity of the patient should accompany the data, and the principle of minimal disclosure should be applied to data sets provided for analysis.
3 Where personal data is required for an approved (but not directly care related) purpose, the permission of the patient should be sought, and where this is given the data disclosed should comply with the principle of the minimal disclosure necessary to meet the stated needs. If refused, the data should be withheld, except where there is an overwhelming issue of risk/harm involving third parties or the public at large.
4 The system of consent/permissions should, at its simplest, be readily managed by both patients and professionals.

For secondary usage, the aim must be to enable the goals to be achieved without compromising personal privacy. Although most do not require the patient to be personally identified, for some studies it may be important to have certain derived data (e.g. sex, age range, area of domicile, etc.); and for other studies it may be necessary to follow the progress of a specific individual through the care system, but again the actual identity of that individual is unimportant. Simply providing access to the full personalised data for these purposes sits uncomfortably with the law and even less comfortably with ethical imperatives.

Context and content

If conceptually one separates the record relating to each healthcare event/encounter into CONTEXT (who, when, where) and CONTENT (what), it is clear that the bulk of the data is content, but what makes it personal and meaningful is the context. Even given knowledge of an individual (such as illnesses and patterns of care encounters) and ready access to content-only records it is highly unlikely that records could be definitely matched to that individual without any contextual tags.

Context

There are numerous attributes of the medical record that must be considered as 'context' and which may enable a record to be linked to an identifiable individual. All these can be removed from the record of care and kept separately, replaced by tokens representing the patient and the provider/institution. Where research and analysis requires some personal context, suitable abstracts and derivatives from these context data can be provided to meet the specific purposes. There is an excellent review of this issue where 18 categories of contextual data which can be used in identifying an individual are listed.[12] A synopsis of these categories, condensed into six general groups, follows:

1 All names (and aliases).
2 All biometric identifiers, including images.
3 All dates (birth, event/encounter, death etc.).
4 All geographic identifiers (e.g. addresses, post codes) which embrace less than 20 000 people.
5 All contact numbers, emails, internet protocol addresses etc.
6 All alternate identifiers, registrations and enrolments relating to administrative functions, insurance plans, vehicles, other.

Content

Separation from the context leaves content of greatly reduced sensitivity. To reconstruct the full care record for continuing patient care (with any omissions deemed important by the patient) requires that the patient has some means to link together context and content and so authorise the care provider to view their stored records. The provider may then store whatever they need of that on their own system for medico-legal and audit purposes: further they may be provided with a limited duration token which enables them to access future patient progress information (e.g. after referral etc.).

Outline of a privacy protecting plan/model

The following outline schema (see Figure 1) is proposed to achieve these ends:

- A central identification unit identifies individuals and issues patient cards (also provider and analyst ID cards).
- Each patient card has a single master ID token (viewable only by issuer and holder); the card holds numerous secondary tokens, one of which is the default patient records ID. The only link between these ID/tokens exists at the level of the card itself, and the card issuing unit.
- At the card issuing unit, the master patient ID is linked with elements of context – for example name and address, gender, enrolment/insurance plan, biometric identifiers, contact details, ethnicity, religion. Appropriate arrangements must be made to update those elements which are subject to change (e.g. address, insurance plan, contacts).

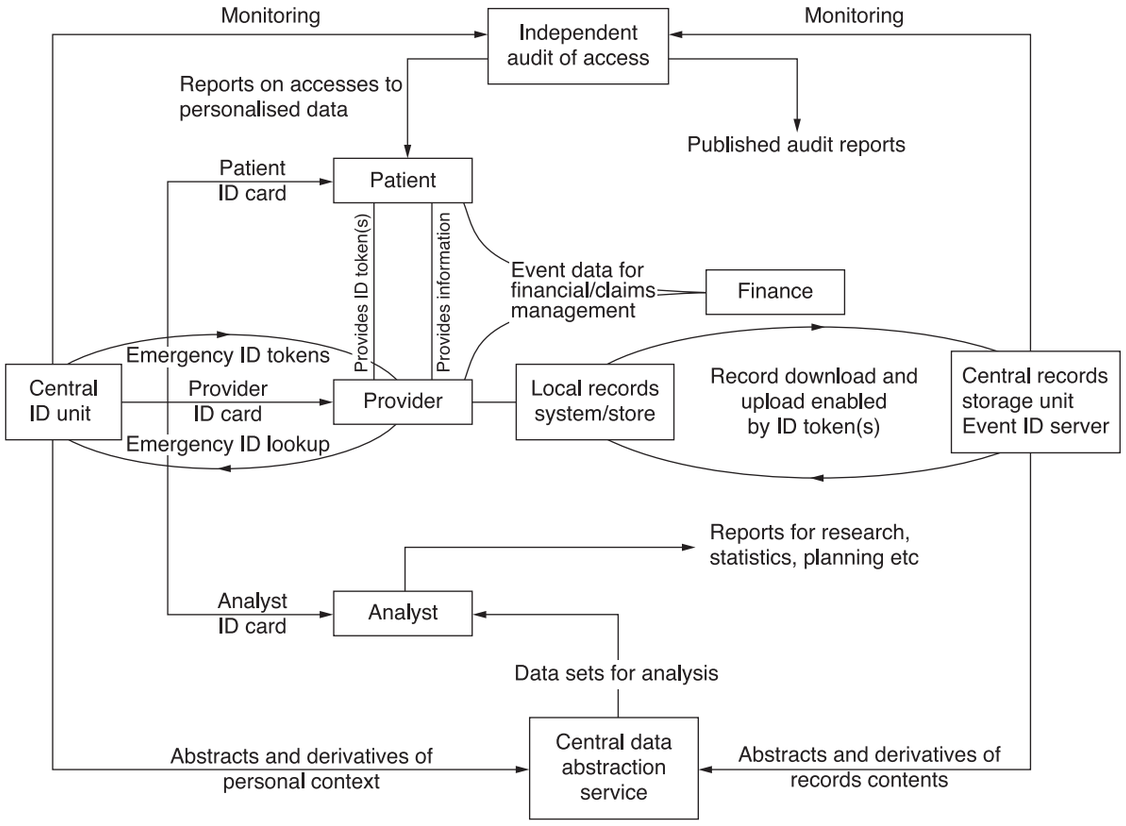

Figure 1 Outline of the privacy protection schema

- Each provider 'knows' the patient in terms of the data they have gathered about them (name, address, date of birth, system registration number, insurer and plan etc.); the patient is assigned an ID on the provider system (unit record number) under which the provider holds their copy of the medical record, now linked to an ID token from the patient card.
- Whilst the patient will normally choose to use their default ID in any encounter, they may prefer to keep certain encounters under another ID/token to maintain their separation.
- As well as choosing the ID/token under which an event/encounter is to be stored, the patient can reveal any of their alternate IDs at a consultation or encounter. Doing so enables the provider to access additional care records held under these IDs (of course only in conjunction with an authorised provider ID card).
- The provider uploads to the central records repository the summary/content of the encounter only, and this record is associated with the ID/token selected by the patient and an event identifier code. (If the patient has no functional ID card for whatever reason, this upload cannot take place.) The event identifier is copied to the patient card.
- The patient can change their ID attached to any specific stored record of a care event/encounter to an alternate ID from their assigned group, so changing which patient ID that record will be displayed under: groupings of events under each ID may be stored on the card and/or on a central server.
- The patient can leave a time-limited token on the provider system allowing continuing access to past as well as any additional records created under any of their IDs shared with that provider until the expiry of the token.
- Secondary users and data analysts submit their data requirements to a central data abstraction service, which abstracts the requisite records for the purposes, linking together events recorded under different IDs for the same patient.
- For each approved analytic/research activity, the abstraction service provides secondary users with sufficient data by way of patient context 'classification' (e.g. age range, sex, region of domicile etc.) to support the activity, but aiming to keep the identity of the patient confidential.
- The identification unit will receive requests where a 'break-in' to personal records for a patient is deemed necessary (e.g. care emergencies). Approval

of such a request will enable the provider to access the relevant records and will at the same time trigger an audit process. Part of the audit process is that the patient and an independent auditor are informed of the access and reasons for it as well as any other relevant circumstances.

- For billing and insurance (public or private) purposes, the insurer will receive data about care events in two parts, linked by the event identifier code. One part will provide sufficient data for clinical audit and determination of whether the billed items of service were appropriate in the clinical circumstances, but without the identity of the patient; when this has been reviewed, the second part is passed to administration for settlement, identifying the patient, provider and the approved items of service being claimed, but without further clinical detail. Clearly there can be some degree of loss of privacy involved, but this is inevitable if the parties to the insurance contract are to be able to fulfil their contractual responsibilities.

Discussion

The central element of this plan is the patient health card. Individuals already hold numerous cards (tokens) used mainly to authenticate their identity in accessing services (e.g. cash/credit, club memberships etc.). This card differs in that it does not actually identify the individual, but securely identifies and tracks their care encounters grouped under several alternate tokens. It also provides the key whereby providers can view events that are otherwise hidden from them. The card gives the patient control over who sees what of their care records: however, where the patient is unable to exercise that control (and no proxy has been identified) the system allows for emergency access to the records, at the same time triggering an audit process relating to that override.

Patients can give their care providers a single use or long-term token to access those of their records that they choose to share. Patients may be using several 'records identities' and may move records between identities if they choose: all these identities are linked together at the level of the patient's card as well as at the central identification service. However, at the simplest level the 'default' status would be that the principal records' identity is applied to all care encounters, and that the care provider is given a long duration records viewing token to store locally.

Patients' identities cannot readily be discovered by analysts or researchers, and even their insurers will normally only have access to the minimum of clinical detail in the personalised part of their claims. It remains possible, although technically very difficult, for analysts to re-identify a small number of individuals either from the combination of clinical and contextual items provided with data for analysis, or by matching data to other information known about a specific target: to prevent this would be to render the secondary usage data largely useless. Naturally central ID unit and data abstraction technical staff can open any records, but in doing so they will trigger the audit/monitoring function.

If a patient loses an ID card, a replica can be provided by the central identification service where all identity tokens are stored: the lost card remains secured by its accession code (PIN), and can be invalidated on the system. All data accesses to personal records will be

The New Zealand Health Information Service (NZHIS)[13]

Essentially the same goals, issues and challenges as are currently being addressed by the *Connecting for Health* project were confronted by New Zealand in 1991. From the outset privacy was identified as being of the highest concern and sensitivity. After two years of development, the NZHIS successfully went live in 1993 (subject to the provisions of the New Zealand Privacy Act, 1993) and has been embraced by public and professionals. The system has an online patient master index (National Health Index, NHI) and online medical warnings system which holds data for each individual on life-threatening conditions and life-sustaining treatments. Care events (all secondary and selected primary events) are reported with a minimum data set submitted by providers. Event reports have personal identifiers removed and are submitted associated with a cipher, but the cipher is in fact the encrypted NHI number for that individual. The encrypted cipher is subsequently re-encrypted at the database access layer to maintain anonymity even from analysts. The Health Minister holds a 'key-in-escrow' that can be used to decrypt identities if there is a sufficiently pressing reason (e.g. incipient failure of an implanted device). All accesses and usages of the system can be traced to a single legally accountable user and are audit trailed with full rollback capabilities. The service falls under the oversight of the New Zealand Privacy Commissioner. Personal health smart cards were debated but not implemented at the time due to their technical limitations: these limitations have now almost completely been resolved.

attributable to an identifiable individual, and a list of those who have accessed which events in their records can be provided to patients on demand.

Primary users of the records (care providers) will have access to whatever records are held locally as well as those available in the central store facility that are approved by the patient. In an emergency where the patient card has been lost or the patient is unable to provide the PIN, the central identification issuing service can provide access to the patient records subject to certain criteria being fulfilled. Emergency access triggers an automatic audit trail informing both an auditor and the patient. Providers will no longer be able to access records of care for which they do not hold the requisite patient token. Where a group practice operates (e.g. a hospital clinic or general practice) and personalised records and patient tokens are locally held (with patient consent), other providers in the group may be permitted to access these to support patient care subject to local access control and audit measures.

Secondary users of health records can have access to full clinical details of care encounters, but will always be restricted in terms of the context that can be associated with these. Selected characteristics derived from the patient details can be made available (e.g. age range, sex etc.) to support analyses, and all the records pertaining to the same individual (irrespective of which identifier token they were stored under) can be linked together for longitudinal studies. In the event that personally identified data is required, for example in studies of familial genetics, it will be imperative that the permission of the patients is obtained to support such research.

Conclusion

There is a significant risk at the present time that the NHS *Connecting for Health* initiative could become derailed or deflected as a result of failing to deal properly with the crucial issue of personal privacy protection: this is the one issue that could stop the entire program from progressing, to the detriment of all.

It would seem that the security framework surrounding current plans for the development of NHS integrated centralised care records is probably in contravention of the EU Directive and/or the Human Rights Act. Where patients have shared their information for a specific purpose (most often for diagnosis and treatment, but this may include research if permission is requested) it is their legal right to ensure those are the sole purposes for which it is used whilst it remains personalised – unless one of the statutory exceptions applies, and this exception is deemed consistent with their human rights. Current plans do not appear to sustain these requirements: it might be different if there were no other way to provide for the primary and secondary data uses within the principles of the EU Directive and the Human Rights Act, but this is not the case, and an alternative has been outlined in this paper.

Unless these issues are fully and openly addressed, there will be rumbling discontent, important records will be withheld and attempts to discredit the system will continue, with various players taking combative political positions.[14] Public confidence is already suffering and will inevitably deteriorate further. Every apparent breach of personal privacy will lead to (most probably successful) legal challenges and the system will become mired in political and legal controversy and discredited, consequently suffering from data degradation and disuse.

REFERENCES

1 Mellor C. *Personal Information Record Losses Reach New Heights.* TechWorld. www.networkworld.com/news/2008/010208-personal-information-record-losses-reach.html (accessed 1 February 2008).
2 Public Servant Daily. *Investigation Reveals Welsh NHS Data Loss.* www.publicservice.co.uk/news_story.asp?id=6521 (accessed 17 July 2008).
3 Browne A. *Lives Ruined as NHS Leaks Patients' Notes.* The Observer. www.guardian.co.uk/society/2000/jun/25/futureofthenhs.health
4 *PI Warns that Breaches are Leading to Collapse of Public Trust in IT Systems.* Privacy International. www.privacyinternational.org/article.shtml?cmd[347]=x-347–559869) (accessed 20 January 2008).
5 New South Wales Independent Commission Against Corruption. *Report on Unauthorised Release of Government Information.* 1992. www.icac.nsw.gov.au/files/html/pub2_24i_Vol_1.htm
6 UK Information Commissioner's Office. *What Price Privacy?* HM Stationery Office: London, 2006. www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf
7 Safran C, Bloomrosen M, Hammond W *et al.* Toward a national framework for the secondary use of health data: an American medical informatics association white paper. *Journal of the American Medical Informatics Association* 2007;14:1–9. www.jamia.org/cgi/content/full/14/1/1
8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities* 1995;L281:31. www.cdt.org/privacy/eudirective/EU_Directive_.html
9 Office of Public Sector Information (UK). *Human Rights Act 1988.* www.opsi.gov.uk/ACTS/acts1998/ukpga_ 19980042_en_1

10 Office of Public Sector Information (UK). *The Health Service (Control of Patient Information) Regulations 2002.* www.opsi.gov.uk/si/si2002/draft/20029890.htm
11 Anderson R. Under threat: patient confidentiality and NHS computing. *Drugs and Alcohol Today* 2006;6:13–17. www.cl.cam.ac.uk/∼rja14/Papers/drugsandalcohol.pdf
12 National Institute for Health, Department of Health and Human Services, USA. *Protecting Personal Health Information in Research: understanding the HIPAA privacy rule.* NIH Publication number 03–5388. 2003. privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf
13 New Zealand Health Information Service. http://nzhis.govt.nz/moh.nsf/indexns/services
14 eHealth Insider. *BMA Votes for Non Co-operation on Central Records.* eHealth Media Ltd, 2007. www.e-health-insider.com/news/item.cfm?ID=2827

CONFLICTS OF INTEREST

None.

ADDRESS FOR CORRESPONDENCE

Roderick Neame
Health Information Consulting Ltd
Homestall House
Faversham
Kent ME13 8UT
UK
Email: roddyneame@taskcare.com

Accepted October 2008