Creating an Infrastructure for the Productive Sharing of Clinical Information

Roderick Neame, MA, PhD, MB, BChir

Managing Director, HIC Ltd,
Homestall House, Homestall Lane, Faversham, Kent ME13 8UT, UK
and
Senior Lecturer, Kent Institute for Medicine and Health Sciences
University of Kent at Canterbury, Canterbury, Kent CT2 7PD

Abstract

The need for a patient-centred approach to health care services delivery is well recognised. Health care has become more specialised with increasing numbers of disciplines and sub-disciplines: in addition both providers and community are increasingly mobile. As a consequence patients see more providers and this has led to increasing fragmentation of patient-centred care, and in particular of the personal health records for that individual. Clinicians and patients alike recognise the need to ensure that care information is patient centred, continuous and integrated in order to optimise the effectiveness of pro-active and reactive care. But current arrangements, including the architecture of medical record and information management systems, are mainly provider and service-centred and may not readily support the sharing of data to this end.

Beneath the surface lie deeper issues that presently mitigate against the comfortable sharing of healthcare information. There are structural issues that must be addressed and resolved before an effective framework for clinical information sharing can be implemented. Crucial elements of this framework are:

- *legislation –who owns the information and how can information privacy requirements be met;*
- *finance – who should pay for the technology required to enable information sharing, and how can providers of more valuable information be rewarded differentially from those providing less valuable data.*
- *Technology - how can flexible but secure data sharing be enabled across the range of technology platforms*
- *Semantic – how can the diversity of nomenclatures and coding systems in use in the global health care environment be accommodated.*

This paper addresses the above issues involved in sharing clinical information, and proposes practical solutions to them.

Introduction

Where a patient is under the care of more than one provider at the same time (this probably applies to the majority of patients in developed countries), there is general acceptance that information needs to be shared between those providers of care. Sharing information about future care plans and past care encounters is important in order to achieve continuity and integrity of care, to minimise missed opportunities (eg for preventive care), to reduce risk (eg of drug/therapy interactions) to reduce duplication and waste, to minimise delays and to improve opportunities for rapid and high quality decision making. All of these translate into reduced costs of care, as well as improved outcomes and patient satisfaction.

However there are embedded obstacles to this whole apparently desirable process of sharing care information. From the perspective of the providers, there are obvious sources of reluctance to share information willingly, including:

✍✍that they may be in competition for patients and are therefore unlikely willingly to share valuable information with their competitors;

✍✍that records may contain elements which are confidential or commercially sensitive or could lead to allegations of malpractice, all of which add to provider concerns over sharing;

✍✍that sharing information should be a reciprocal arrangement: but providers who keep better records as a result of greater investment in technology resent effectively subsidising those whose records are less valuable and poorly organised;

✍✍that purchasers are slow in coming forward with financial arrangements which encourage the sharing of high quality patient information between providers

There is reticence also on the part of the patients. Whilst they are keen that their care providers should have all the necessary information to hand when making clinical decisions, there is growing community concern about arrangements whereby their private and personal clinical records may be shared with others without their knowledge or consent. There is a perception that insufficient attention has been paid to issues of computer security: accumulations of personalised data can prove attractive targets for hackers as well as for those willing to abuse their legitimate access rights.

The Issues

Before sharing of personalised care information is widely accepted as a routine, a number of infrastructure issues must be addressed. Fundamentally the issues can be reduced to the following.

1. Who *'owns'* the data that arises out of a care encounter? Who should be responsible for *maintaining* it, and who should have rights of *access* to it, and under what circumstances?
2. Who should *control* this process of personal data sharing? Who, if anyone, could insist that records be *made available* to another provider?
3. If an arrangement for sharing can be made, should the entire record be available for sharing, or should there be a provision for the provider generating the data to *'edit'* it, or for the patient to do the same?
4. Sharing quality data in most situations will contribute to reducing the costs of care (and therefore increasing the profit margin) of the recipient of the data. Better quality data providers, and those doing a more organised and thorough patient work-up, will confer a greater financial advantage on the data recipient – how should they be rewarded for this?
5. How can the data from a diverse range of technical platforms and clinical applications, and using a wide range of file structures, semantics and coding systems, be shared meaningfully?
6. How can data sharing be achieved securely and without compromising patient or provider privacy?

1. Who OWNS the information?

Whilst in principle there is a willingness to share clinical information about the same individual between providers, in practice this may be in conflict with professional attitudes and sometimes with the law. The level of sharing that can be achieved will be bound up with addressing the issue of who owns the data.

The concept of ‘ownership’ generally implies the right to destroy, sell, edit, give away, disclose or dump the objects (in this case personal medical records). Few would assert the right of any individual to do these. The records can be conceptually separated into the medium (eg paper, disk) and the content. Separate the two parts and without a doubt there is an owner of the medium. However the ownership of the content is less clear. The author (care provider) definitely has some moral and intellectual property rights, as does the identified subject (patient): even the purchaser (eg health authority or insurer) likely has a legal claim at least to any parts of the record content for which they have paid (albeit as agent for the patient). So it follows that when the content is associated with the medium, the rights of the owner of the medium (eg to sell, destroy etc) must be modified to take account of the rights of the parties in relation to the content.

Sorting all this out may be of academic interest in a legal sense. What is quite clear, at least on the basis of ethical and moral considerations, is that whoever is deemed to 'own' the records will find themselves in the position of being constrained from doing many of the things that an owner might expect to be able to do.

However in a sense ownership is not the real issue here. At a very practical level the issues that must be resolved relate to who has a duty to keep and protect those private and confidential records (custodianship), and who has rights of access to them and under what conditions (access). For the most part the world is coming to the view that the provider has a duty to make arrangements for the custodianship of the original records, and to keep securely the *primary* copy of any record they make. [This is essential in any case for their medico-legal protection]. However the patient, as the subject, has a moral right of access at least to some of the information in the record, and should be able to authorise third parties, (such as their purchaser/insurer, other care providers of their choice, their legal advisor etc) to view some or all of that data. Therefore the provider would be expected to make a copy of (some if not all) of the data arising out of an encounter (a '*secondary*' copy) and place this where it is accessible to those authorised by the patient. It might be necessary to impose certain conditions on this accessibility (see below).

This arrangement in no way affects any statutory rights that the patient may have of access to the original (primary) record under Freedom or Information legislation or equivalent, nor the status of the primary record as medico-legal 'evidence'. The option to edit the secondary copy before making it available to third parties is there to protect information that one, the other or both parties to the care event may prefer not to make available to other care providers.

2. Privacy and Control of Data Sharing

The information in the primary patient record is confidential to both provider and patient. The information in the secondary copy is confidential to the patient, but the author should have no concern if that information is shared with others – for example with purchasers, providers, personal advisors and legal counsel.

The provider should have no automatic rights to share personalised patient information with anyone without the consent of the patient, unless required to do so by statute or court order, or unless certain other conditions pertain (see footnote[1]). To disclose personal records without patient consent, even if it is deemed to be in the best interests of the patient, is 'paternalistic' and contrary to the rights of the individual to control who knows what about them. The provider can, of course, safely share records with a colleague (eg for advice or guidance) once the records have been de-personalised. The patient, on the other hand, should be empowered to control access to the secondary copy of all their current and past care event records.

3. Editing Records for Sharing.

The primary copy of the care event record must rest with the author (see above). This copy may contain data that the author feels is confidential to them or commercially sensitive. There is no reason why the entire record should be made available to the

[1] It is widely accepted that certain exemptions should attach to this general prohibition on unauthorised disclosures of information. These include such situations as where disclosure is necessary to prevent a crime, or a threat to public or personal safety.

patient: he or she can be provided with a secondary copy of the event record where some content may have been erased, but not such as to affect the core clinical information. The purpose of the secondary copy is to serve the needs of the patient in making a claim for re-imbursement, as well to support the provision to them of high quality care by other providers with continuity and integrity.

It is generally accepted that the patient has a right to 'tell their own story' in terms of their past care events in any way that they choose, editing, omitting and even embellishing where they think fit, even if that could adversely affect their care. In practice they are free to do just this at present, selectively recalling information to pass to their care provider(s). In the same way patients may wish to edit their (secondary) copy of the event record before passing it to a third party (or indeed to conceal its very existence). To protect the professional integrity of the provider in such situations, if patients are enabled to edit their secondary record copies, the resultant record should indicate that it has been edited, and the identity of the identity of the author should be absolutely protected unless the patient has received their approval for the changes.

4. The Value of Shared Information

There is a significant cost in generating information about a patient, and concomitant value in being able to access that information to support clinical decision making. To generate information requires time and effort, but the information is considered sufficiently valuable to make that investment worth while. To create a high quality information resource in the form of structured and coded electronic medical records about a patient involves significant investment in systems and in data entry. However such a resource has additional value as it can be used not only to support patient care, but also to support other functions, such as billing, workload analyses and clinical audit.

Making this type of information available to a professional competitor runs contrary to good business sense. In essence it involves investment by one provider, who generates and stores high quality data, for the benefit of another provider, who accesses it in order to treat the patient but does not bear the expense of the time, effort and investment required to generate it. Where the records held by one provider are less accessible, well organised or complete, their value is lesser to another provider. Therefore those with better quality records are in effect subsidising those with lesser quality records when they come to share information.

In many health care systems, the fee-for-service philosophy prevails - where a doctor provides more services, he/she receives more income often regardless of whether the services were necessary or not. In this environment there is clearly no incentive whatever to use data generated by another provider: it is financially more rewarding to repeat everything, so earning the profit accruing from providing each service.

The other main philosophy of care system is based on fixed price payments for specific clinical entities (eg iso-resource groupings, DRGs). In this environment every item of service 'saved' increases the profitability: the incentives to use data generated by others are high, but there is no incentive for the provider generating the data (at considerable cost) to share it with another provider who can use the data to increase profitability.

The sharing of data must therefore involve some consideration (eg payment) to the originator as an incentive to invest in high quality data: the consideration would depend on the value and quality of the data. It may also be necessary to incentivise the user to make best use of shared information, or, more probably, to invoke some penalty where a user has failed to access available data and has wasted resources in duplicating that data collection.

5. Sharing data from semantically diverse origins

There are many different technical, semantic and coding schemes and systems in use for the capture and storage of clinical data. More will certainly emerge in the future. Whilst standards may also emerge in time, experience suggests that widespread adherence with them will be a long time coming.

However none of this need affect the successful sharing of meaningful information between providers. All systems can output the data from an encounter as text as if it were to be printed: that output can be passed through as the secondary record to be placed on the web for sharing. All context is first removed, and ideally the record is then inserted into a simple structured template with headings to make for ease of reading (eg complaint(s), diagnoses, medication(s), test(s) etc).

In this way the .html 'meta-language' can be used to achieve inter-readability between the semantically and structurally disparate clinical systems storing patient data.

6. Managing Privacy

The fundamental principle that should be applied is that the patient should be in control of who sees what of their personal information, in line with the general provisions of human rights legislation. As outlined in the preceding text, a secondary (potentially edited) copy of every care event record, to which the patient has rights of access, should be generated.

If this argument is accepted, managing privacy becomes relatively simple. The secondary event record copy can be stored in a readily accessible location, for example on a world wide web server, but with all context (eg date, place, provider, clinic etc) removed. The patient can hold an index of all their care encounters, together with the context (see above), a brief summary of the nature of that encounter (eg cause, diagnosis) and a pointer to the web location where the secondary copy of the record is stored. The secondary copy of their record can include text, images, scanned pages (eg of handwriting) and all other modalities that can be stored and retrieved in mark-up language. In this way the patient can ensure that access to their data is under their own control. The data can be held in plain text which is readable by anyone: there is no bar to holding specific data sets in a structured form, but for this to be generally useful a consensus of many parties is required to agree a standard.

This is something that can be implemented with a smart card, which provides just that type of control over access, and therefore can be considered the ***personal privacy token*** of that individual. An illustration of this arrangement is shown in figure 1.

FIGURE 1 NEAR HERE

It is not just the privacy of the patient, but also that of the provider that must be respected. The provider should be quite willing to be held accountable for the care they provide to the patient, provided that it is accurately portrayed. Making it possible for the patient to edit their copy of the record, which some might argue is their right, would mean that the actions of the provider might more readily be misconstrued. Therefore the provider should have the right to ensure that their name is automatically deleted from the secondary copy of the record if any modifications are made to that copy.

One particular instance where the concept of separation between content and context of an encounter record is especially important is where claims are being managed. It is quite inappropriate for a wide range of claims processing staff to be confronted by content and context together – rarely is this association of data required, and most transactions can be carried out using either one part or the other. Bringing them together at all points means that many people will unnecessarily breach the privacy of the patient, although there are some points where the data may need to be personalised, for example in relation to audit.

In relation to data management for statistical or administrative (eg claims) purposes, the general rule should be that administrative and clinical details should be kept separated as far as possible. The fact that an encounter occurred between a specific provider and a specific patient at a specific time and place is one set of data; the objective details of the event (problems, diagnoses, tests, results, medications etc) are another data set which should be kept separated from the former. The latter, in the absence of the former, is all but meaningless: literally thousands of encounters of most types occur and, in the absence of identities, times and places, there is no way to infer whether one set of data or another relates to one particular individual or another. Likewise an insurer must at the very least know that an event has taken place in order to agree to pay for it: how much will be paid must await analysis of the clinical event details, which may be linked to the administrative details by nothing more than a random number. But precisely how much data is made available to an insurer will depend upon the details of the agreement between the patient and his/her insurer.

Conclusion and Summary

This paper offers a pragmatic solution to the records ‘ownership’ problem, with a separation between primary (archival) and secondary (sharing) copies of the record. It proposes that record sharing should be controlled by the patient through their access to the secondary record copy, which may be edited. The need for a financial framework that supports and encourages sharing of data is highlighted. The practical benefit of separation of context from content in the management of confidential healthcare information is also highlighted.

Address for correspondence

Further information on the above issues and on solutions embodying these principles can be obtained from:

Dr Roderick Neame, MA,PhD,MD
Managing Director HIC Ltd
Homestall House, Homestall Lane,
Faversham, Kent, ME13 8UT, United Kingdom.
Fax: +44 1795 538390
E-mail: 100764.3727@Compuserve.com
URL:http://www.health-info.co.uk