



## UKHIT 58 - Contents

Introducing a UKHIT Special Issue: <i>Security and Confidentiality</i> .....	1
Guest Editorial .....	1
Some practical considerations for implementing security and confidentiality requirements in distributed environments .....	2
Rising to the Occasion – Using Knowledge Management to Help Protect Electronic Healthcare Record Information .....	3
Privacy is Paramount.....	4
The Lay of the Land.....	5
The Times They Are A-Changin’ - Public and Private in Ancient Greek Healthcare Confidentiality .....	6
References, Resources – e-Health: Security and Confidentiality .....	7
UKHIT Diary.....	8

UK Health Informatics Today (UKHIT) is published by the UK Health Informatics Society

The opinions expressed in UKHIT are those of the authors and do not necessarily reflect UK Health Informatics Society policy.

Copyright © UKHiS 2009 All rights reserved.

UKHIT is published in electronic form on the UKHiS website:

[www.ukhis.org.uk](http://www.ukhis.org.uk)

## Introducing a UKHIT Special Issue: *Security and Confidentiality*

### Jeannette Murphy

*UKHIT Senior Editor and Senior Research Fellow in Health Informatics, UCL Centre for Health Informatics and Multiprofessional Education (CHIME)*

[j.murphy@chime.ucl.ac.uk](mailto:j.murphy@chime.ucl.ac.uk)

One reaction to this issue of the newsletter, could well be, “Oh no, not another set of articles on security. I know it’s a problem, but it’s not my problem. Any way it’s too technical, too complicated and too political for me.” If that’s your first reaction, can I urge you to set your misgivings to one side and delve in. Nathan Lea, our guest editor, is to be congratulated for finding a group of authors who manage to make the topic of Security timely and accessible. They have avoided polemic -- they don’t claim to have a solution but they have provided some fresh insights into a problem which is often seen as a major stumbling block to the successful implementation of information systems in healthcare.

If you need a further incentive to think about how the issue of security impinges on you, either in your work role or your patient role, here are a few pertinent statistics from a 2008 transatlantic survey of more than a thousand healthcare professionals. The survey, carried out by Credant Technologies,

together with E-Health Insider in the UK and Outpatient Surgery Magazine’s subscribers in the US, found that:

- Over a third of healthcare professionals are unwittingly putting personal information at risk by storing patient records, medical images, contact details, corporate data and other sensitive information on mobile devices (laptops, BlackBerrys and USB sticks) and not adequately securing them.
- A fifth of healthcare practitioners use their own devices for work.
- In the US, a third of healthcare professionals surveyed were downloading sensitive details onto their own personal devices – a basic breach of security practice if they were not complying with the security policy set up by their employer.

There is, however, some good news. The survey found that security practices in the UK are well higher than the standards upheld in the US. In the UK, 56% of healthcare professionals are using strong security to protect their mobile devices (with 35% using encryption, 17% two factor authentication, 3% biometrics, 1% smart cards), which makes data difficult to access. But in the US, only 23% were using strong security to protect their mobile devices.

The recent spate of security breaches in UK public sector organization has had a positive impact on the healthcare sector. There have been two rounds of instructions and guidance to NHS chief executives about the security of data in transit and data on mobile devices. The 2008 survey suggests these have had a positive impact, since 65% of security policies have been revised over the past year.

## Guest Editorial

### Nathan Lea

*Research Fellow, UCL Centre for Health Informatics and Multiprofessional Education (CHIME)*

[n.lea@chime.ucl.ac.uk](mailto:n.lea@chime.ucl.ac.uk)

Sharing of medical information has become a top priority in the United Kingdom’s healthcare strategy. We have seen advances over the last few years in the management of information electronically, and day to day working practice in the industry now relies heavily on emailing, distributed systems and web applications. With these changing working patterns have also come a number of reports about personal data (mis)use: be it the National Audit Office data security scandal, where millions of peoples’ identities and bank details had been transferred to CD-ROMs and lost in the internal mail, or a heightened anxiety about government surveillance of individuals and the resulting privacy concerns, data sharing in general has become topical (if not hotly debated).

The public debate does not focus specifically on healthcare data issues, and the true nature of secure data management in healthcare remains largely, at best, unacknowledged and at

worst, unknown. Knowing what to do, how to behave and whether what you are doing and how you are behaving ticks all the boxes, is elusive. In fact, knowing what boxes to tick is not exactly obvious. Whilst the ethics and the anxieties are debated, one can rest assured that a recently published European Court of Human Rights ruling has set a precedent<sup>1</sup>.

This special issue of *UK Health Informatics Today* has been produced with a non-prescriptive style and an emphasis on providing some food for thought. The contributors have made a valiant effort to discuss their experience, present their arguments, offer their guidance or tickle your intellectual fancy, for which I thank them and the Senior Editor who provided us with an opportunity to shed some light on this topic. I hope you enjoy reading this special issue, and find it helpful in your own efforts.

## References

1. European Court fines Finland for data breach' at [www.e-health-insider.com/News/3992/european\\_court\\_fines\\_finland\\_for\\_data\\_breach](http://www.e-health-insider.com/News/3992/european_court_fines_finland_for_data_breach)

# Some practical considerations for implementing security and confidentiality requirements in distributed environments

## Bruce Beckles

*e-Science Specialist, University of Cambridge Computing Service*

[mmbb10@cam.ac.uk](mailto:mmbb10@cam.ac.uk)

I spend a lot of my time helping scientists use distributed computing environments of various sorts. Such environments can be anything from a collection of several computers connected together to form what is often described as a *cluster*, to a *computational grid environment* consisting of up to thousands of individual computers linked together in some manner. One thing that these environments all have in common is that the users, the administrator(s) and the resources (the computers, etc) are not all in the same physical location. Often they are also not in the same administrative domain (e.g. the users belong to one university, the computers to a different university). Some of the salient characteristics of such environments are:

- not all users are known personally by the administrator(s),
- users do not tend to have a strong sense of responsibility for the environment – indeed they are often unaware of the extent of the environment (who else uses it, what other data is stored in the environment, etc) and the potential consequences of their actions, and
- it is difficult for users to correctly evaluate the security risks in the environments.

One of the consequences of this is that user behaviour that is usually perfectly sensible in the user's normal work environment is no longer appropriate in the distributed environment *but this is not readily apparent to the user*. For example, users may be used to relaxed access controls in their local environment (perhaps because everyone knows everyone else in the lab and data and resources are routinely shared), and so it is of relatively little concern exactly which local user is using the local systems. In the distributed computing

environment, however, it is probably the case that access controls need to be much stricter, so users sharing access credentials may represent an unacceptable security breach from the point of view of the environment's administrator(s). The importance of this restriction may not be fully appreciated by users, since they may never meet the administrator(s) of the environment, and may also not have any ideas about who else is using the environment and for what purpose.

One of the most difficult tasks for people designing, implementing and administering such environments is to ensure that the user is able to use the environment efficiently and effectively whilst not greatly increasing the likelihood of the environment being compromised. Our guiding principle for these environments should be: the distributed computing environment needs to be designed so that *it is easy for the user to use it effectively in a secure manner and difficult to use it in an insecure manner*. If the user has to wrestle with the environment's security mechanisms in order to use it as they would wish, they are likely to either stop using it or try to subvert those mechanisms, i.e. use it in an insecure manner. Perhaps the classic example of this is insisting that users have long, hard to guess passwords. Such passwords are also hard to remember, so users are forced to write them down and store them near where they actually need them (e.g. a Post-It note on the bottom of their screen – so now anyone who walks past their desk – visitors as well as work colleagues – knows their password).

So, perhaps the most important rule for designing such environments is: *the environment's security mechanisms should be integrated into the user's normal work practice as seamlessly as possible*. For instance, if users are automatically granted access to the distributed computing environment when they access their local computing environment (e.g. by logging in to the workstation on their desk) then they will not have to manage an additional authentication credential (password, etc) nor will they have to struggle with an unfamiliar authentication mechanism to get access to the distributed computing environment. This makes the environment both easier for users to use, and less likely to be compromised by users' actions.

Such considerations give rise to two principles to guide us in designing and managing our distributed systems:

- Make it easier to do the right thing than the wrong thing.
- Design the environment to support/complement normal working practice.

How can we apply these ideas in the medical domain? Let us consider an electronic patient record system. We know that senior doctors/consultants usually have very little time to spare when they are seeing patients on the ward. A natural consequence of this is that they will often ask junior doctors and/or nurses to access patient records for them as they work their way through the ward. If the only way the nurse can access the patient's record is by using the senior doctor's access credential then the senior doctor will probably give that credential to the nurse. Unfortunately, this now means that if the nurse wishes, they can get access to other data for which they are not authorised, and it will be difficult to tell that they have done so.

If we support this working practice (principle 2) by allowing the senior doctor to temporarily delegate access privileges to the nurse for records of patients in the ward they are currently in, then the potential security breach is greatly minimised. If, in addition, we make it easy for the doctor to actually do this (principle 1), then it is likely that they will, rather than simply

giving the nurse their credential. There are a number of ways we might do this: one possibility would be to implement a system that issues staff with physical tokens (e.g. smart cards) and have access points (e.g. smart card readers) on each ward. The doctor and nurse insert their cards into the reader as they enter the ward. Now, until the doctor inserts his card again, or a specified period of time elapses, the nurse's access level for patient records is automatically upgraded to allow read access to all patients on that ward. An additional happy consequence of such a scheme is that now our audit records are correct: the system will be able to record which records were accessed by the nurse with the authorisation of the doctor. In the previous scenario where the doctor gives the nurse their access credential, the system will be unable to tell that it is the nurse accessing the records rather than the doctor.

Finally, this scenario highlights another important principle:

- As far as possible, keep records of what *actually* happened – that way, if there's a problem, you have some hope of finding out later who did what and what the effects of their actions were.

A common problem is that systems are only designed to record what the designer expected would happen. In the real world, people are much more creative and will often find wholly unanticipated ways of using the system. If you've designed the auditing component of your systems properly, though, that need not be a problem. My experience tells me that designing secure systems is hard, and that usually we get it wrong not because of subtle bugs (although that certainly happens) but because we haven't thought carefully enough about how the system will actually be used. The first, and last, question you should ask when designing a complex system is: does the system make it easy for users to use it correctly? If the answer is no, expect the system to be compromised once it goes live.

## Rising to the Occasion – Using Knowledge Management to Help Protect Electronic Healthcare Record Information

**Nathan Lea**

*Research Fellow, UCL Centre for Health Informatics and Multiprofessional Education (CHIME)*

[n.lea@chime.ucl.ac.uk](mailto:n.lea@chime.ucl.ac.uk)

A primary goal of the efforts to standardise the Electronic Healthcare Record (EHR) has been to support the sharing of detailed, sensitive medical information between clinicians and carers who are responsible for medical care throughout a person's lifetime. The recent adoption of ISO 13606 as an International Standard for the "...communication of part or all of the... EHR of a single identified subject of care between EHR systems, or between EHR systems and a centralized EHR data repository"<sup>1</sup> represents the importance that the international community places on accurate sharing of information between medical record systems, and further examples of work to help share detailed information on national scales are available from the *openEHR* Foundation<sup>2</sup> and Health Level 7<sup>3</sup>. The extent to which the information in an EHR can be reused time and time again, either for acute clinical interventions and chronic disease

management or as part of medical research is becoming clearer<sup>4</sup>.

In the United Kingdom, access to the information for use beyond clinical care may be granted by explicit patient consent and Research Ethics Committee (REC) approval and where consent cannot be gained, the data may, with further REC approvals, have identifying details removed<sup>5</sup>. Whilst the RECs may provide other stipulations on how the information is used, the rights of individual patients to privacy and the medical profession's duty of confidentiality impose further constraints on how the information can be shared. The constraints are established by legislative controls, international standards<sup>6</sup>, ethical considerations and risk analyses that should be performed for the different usage scenarios, all of which should inform the establishment of information governance policies.

The policies are written for human understanding and interpretation, but in turn must be refined to the point that a computer system can understand and apply them at the point of EHR service provision. Furthermore, the EHR is designed to exist throughout a patient's lifetime and beyond and will need continuous protection for the length of time that the record is valid, which means that the policies themselves will need to be updated in accordance with frequent reviews, legislative changes and risk analyses. In addition, different software systems and users will be processing the information, so the details of how that information should be protected need to be transferred to those systems and understood by the users to allow for consistent and correct behaviour and adherence.

There is ongoing research into the area of computable policy specification<sup>7</sup> and there are commercially available software tools that implement some security assurance, but in both cases they have not been designed with clinical use cases in mind. The specification heuristics of the policy formalisms and tool configuration are complex, and it is impossible to capture and apply the majority of the information security stipulations across all the clinical and research use cases. For example, software tools will manage authentication of users and control access to various resources in a system, but not to the level where a patient deems access to one part of their record to be acceptable under certain circumstances, but not another part (for example HIV status).

Work has started on exploring how knowledge management can help capture the details of a security policy, present those details in a human readable and computable form, and allow them to be reused by EHR record systems and security software. The results so far include the invention of a knowledge management framework that uses the same design principles defined by the EHR standards: an EHR is constructed using a formalism called the Archetype. This formalism defines a blueprint for what each component of a record should be (so for example, a blood pressure measurement should have a systolic and diastolic measurement, where the systolic should be higher than the diastolic) and it will specify which data items, as defined in an information model, should comprise the specific piece of the EHR entry. The information that is contained within this model can then be recognised as a blood pressure reading by any system or user that access it.

A new formalism, known as the Secutype<sup>8</sup>, has been invented to extend the current functionality of Archetypes to the security domain, so that clinical data models and security policy controls can both be specified. Since Archetypes allow for the clear definition of each part of a record, Secutypes can contain

details about the protection requirements for that part of the record, as specified in an information security policy. The Secutype will specify whether a data item should be withheld when a record is accessed (for example a date of birth might need to be withheld if there are anxieties about patient identification in a research scenario), or whether a clinician can access a particular component of a record if it is known that a legitimate relationship exists between the patient and clinician during treatment.

Work is continuing to prepare an editor that will specify and publish the Secutypes. The Secutypes will then be evaluated, as part of my doctoral work, to see how effectively they express policy items, how well they support existing security software, the performance implications of adding them to existing EHR servers and the extent to which they can be reused in different contexts. The evaluations will also include comparisons with existing solutions in these areas.

Maintaining security and confidentiality to protect healthcare records is becoming increasingly challenging as sharing becomes easier, and more uses are discovered for that information. It is likely that greater transparency will be expected by the public in terms of how these areas are managed. This does not mean that the sharing should not occur, but it should be done carefully and responsibly, governed by policy and for the right reasons. In order to achieve this, accountability and automated access are important, especially as numbers of records grow and information is captured with greater detail and accuracy. Knowledge management may be the key to providing that assurance when it is sought and there are expectations for it to be made available.

## References

1. ISO 13606-1:2008 abstract [www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=40784](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40784) (last accessed 28<sup>th</sup> November 2008)
2. The *openEHR* Foundation Clinical Models Project [www.openehr.org/clinicalmodels/project.html](http://www.openehr.org/clinicalmodels/project.html) (last accessed 28<sup>th</sup> November 2008)
3. Health Level 7 Record Information Models: Health Level Seven. [www.hl7.org](http://www.hl7.org) (last accessed 28<sup>th</sup> November 2008)
4. D. Kalra, P. Singleton, D. Ingram, J. Milan, J. MacKay, D. Detmer and A. Rector. Security and Confidentiality Approach for the Clinical eScience Framework (CLEF). *Methods of Information in Medicine* 44 (2) (2005), 193-197
5. National Research Ethics Service Guidance, National Patient Safety Agency. <http://www.nres.npsa.nhs.uk/rec-community/guidance/> (last accessed 28<sup>th</sup> November 2008)
6. ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management
7. M.Y. Becker, Information Governance in NHS's NPfIT: A Case for Policy Specification. *International Journal of Medical Informatics* 76 (5-6) (2006), 432-437.
8. N. Lea, S. Hailes, T. Austin and D. Kalra. Knowledge Management for the Protection of Information in Electronic Medical Records. *Health Technology And Informatics* 136 (2008), 685 – 690.

## Privacy is Paramount

### Dr Ian Brown

Research Fellow, Oxford Internet Institute,  
University of Oxford

[ian.brown@oii.ox.ac.uk](mailto:ian.brown@oii.ox.ac.uk)

The publication in the UK in July 2008 by the Ministry of Justice of Richard Thomas and Mark Walport's Data Sharing Review has seen renewed calls from medical researchers for access to NHS care records without explicit patient consent. Thomas and Walport suggest the government legislate to allow

approved researchers access to "safe havens" of datasets created by government departments. Researchers would face a jail sentence of up to two years for any "deliberate or negligent" breach of data security.<sup>1</sup>

While some level of personal information would be removed from this data, records could still retain coded links that would allow them to be reidentified with a specific individual. Even without such identifiers, it is extremely difficult to fully anonymise records of health status and treatments that might match only a few individuals in a given country.<sup>2</sup>

Medical researchers have led a sustained campaign over the last 15 years for this type of unconsented access to patient healthcare records.<sup>3</sup> Their arguments have ranged from the expense and difficulty in gaining consented access to large and unbiased datasets, to presumptions of public support for medical research in all of its forms, through to communitarian notions that patients are morally obligated to share their medical history.<sup>4</sup> Thomas and Walport support this latter view, stating that:

*"An NHS patient agreeing to a course of treatment should also be taken to have agreed that information given during the course of the treatment might be made available for future medical research projects, so long as robust systems are in place to protect personal information and privacy. After all, that patient may be benefiting from research using health information from earlier patients."*<sup>5</sup>

Researchers have gone as far as to criticise on this basis privacy guarantees in the Connecting for Health Care Record Guarantee that promise to "allow only those involved in your care to have access to records about you from which you can be identified."<sup>6</sup>

It is understandable that some medical researchers feel their preference for larger datasets should over-ride the necessity of gaining patient consent for access to medical histories. However, this position remains extremely problematic from both an ethical and a legal standpoint. Ethical considerations include the critical requirement for trust between patient and doctor<sup>7</sup>; self-determination rights for patients, who must be assumed to be the best judges of their own interests; and the potential for harm to both patient and public health if individuals do not feel able to fully disclose health information to doctors. Legal issues include the duty of confidentiality of doctors to patients and the human right to privacy that is central to European law, deriving from the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and the Council of Europe's Conventions for the Protection of Human Rights and Fundamental Freedoms and Human Rights and Biomedicine.<sup>8</sup>

While these privacy rights are not absolute, exceptions may only be made for "necessary and proportionate" purposes. It is not clear that the inconvenience of requesting explicit consent from patients would justify setting aside their privacy rights, or that the use of statistical techniques<sup>9</sup> or large-scale cohorts of consenting patients (such as the planned 500,000 participants in the UK Biobank initiative) would not be a less invasive mechanism to avoid sample bias. The European Court of Human Rights has set a high value on medical privacy, finding in 1997 that:

*"It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as many be*

necessary in order to receive appropriate treatment, and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community.”<sup>10</sup>

Recent detailed investigations have found that patients do not share the view of some researchers that their consent for use of their records should be assumed, even when the practical obstacles to gaining that consent are significant. Ipsos MORI found that only 35% of a random sample of 2,106 UK adults were willing for even non-sensitive information to be used without consent. Only 10% accepted unconsented access to remove sample bias, while just 5% agreed that a cost of over £500 for gaining consent justified abandoning the requirement.<sup>11</sup> Qualitative studies have found that patients feel consent requirements provide them with critical control over the use of their personal information, and indicate the appropriate level of respect for their autonomy.<sup>12</sup>

Given all of these issues it is not clear why the Thomas and Walport review is so forthright on the issue of sharing patient data without consent. It seems dismissive of deep ethical concerns and potential public anxiety to suggest the government should legislate to over-ride the necessity of asking patients' permission before using their data in research that they may neither understand nor support. It would be deeply embarrassing for the government to have such legislation overturned by the European Court of Human Rights. More importantly, it could cause great damage to the health of patients and their communities if vital trust in the NHS is lost as a result.

## References

1. Richard Thomas and Mark Walport (2008) *Data Sharing Review* Ministry of Justice pp. 70-71.
2. Ross Anderson (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems* (2<sup>nd</sup> edition) Indianapolis: Wiley pp. 293-296.
3. Ross Anderson (1995) *NHS Wide networking and Patient Confidentiality* British Medical Journal 311: 6996 pp. 5-6.
4. See for example The Academy of Medical Sciences (2006) *Personal data for public good: using health information in medical research*.
5. *Data Sharing Review* p. 34.
6. *Personal data for public good* p. 54.
7. Fleur Fisher et al. (2002) *The Risks of Making Assumptions about Consent* British Medical Journal Rapid Responses
8. EuroSOCAP (2006) *European Standards on Confidentiality and Privacy in Healthcare* pp. 5-8. Available from [www.eurosocap.org](http://www.eurosocap.org)
9. B. Blobel (2000) *Onconet: A Secure Infrastructure to Improve Cancer Patients' Care* European Journal of Medical Research 5 pp. 360-368.
10. Z v. Finland ECHR 9/1996/627/811
11. Ipsos MORI (2007) *The Use of Personal Health Information in Medical Research* Medical Research Council pp. 54-55.
12. M. R. Robling, K. Hood, H. Houston, R. Pill, J. Fay and H. M. Evans (2004) *Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study* Journal of Medical Ethics 30:1 pp. 104-109.

## The Lay of the Land

### Karen Tingay

Postgraduate Research Student, UCL Centre for Health Informatics and Multiprofessional Education (CHIME)

[k.tingay@ucl.ac.uk](mailto:k.tingay@ucl.ac.uk)

### Introduction

Anyone who has read or tried to read the Data Protection Act can appreciate how difficult to interpret confidentiality can be within the NHS. Various documents which summarise it (e.g. NHS Confidentiality Code of Practice, 2003) may be easier to

read but can still seem vague. This vagueness may be the result of being unwilling to make hard and fast statements, in which case, this is also a burden I feel unable to shoulder. However, rather than create yet another article which tries to explain the codes of practice and failing, I have summarised the key points and provided links to relevant documents and sources of further information.

The overall sense I get from reading these documents (see list below) is that, while there are rules relating to confidentiality and data security, these are largely dependent on decisions made between the clinician and the local Caldicott Guardian. Some key points are as follows:

- **Identifiable information** Every patient has the right to have their identifiable information held securely in whatever form it is in. Identifiable information includes name, address, full postcode, date of birth, NHS number and local patient identifier (NHS Code of Practice, 2003). Other information which could be used to identify the individual could be, for example, diagnosis and location where the diagnosis is very rare. The Scottish Code of Practice (2008) includes race, gender, age, and physical, sexual and mental health as identifiable. This data could be stored in different formats including, but not limited to, records, images, photographs, audio and video tapes, emails, transcripts or recordings of phone calls, and text messages.
- **Consent** Consent should be sought before patient information is shared. This could be done explicitly in writing or verbally, or implied through the patient's behaviour. Some data sharing models may be written into contracts with the patient, e.g. that information is confidential within the clinical team and may be shared by any member of that team but with no one outside it without consent.
- **Disclosure** Disclosing patient information without the patient's consent can, in some instances, be acceptable. In many cases, however, patient consent should be sought or attempted to be sought even if it is not necessarily required by law. Decisions about disclosing information should be made with the Caldicott Guardian or GP. Whether consent is sought or not, or when information is disclosed without consent, or when information is not disclosed, justification for the decision should be recorded.
  - In interests of public safety. This can only be determined legally, but, for example, may include cases in which the patient or others may be at risk of serious harm, such as child abuse.
  - When ordered to do so in court. However, if the disclosure is felt to be irrelevant, it may be appropriate to object to disclosure.
  - There is a specific statutory requirement, such as a communicable disease.
  - Where you feel that a patient is a victim of abuse and is unable to give or withhold consent for disclosure and where disclosure is believed to be in the patient's best interests.
- **Young people** According to the BMA, “any competent young person, regardless of age, can independently seek medical advice and give valid consent to medical treatment.”<sup>1</sup> Clinicians should consider whether or not young patients understand their treatment options,

<sup>1</sup> [www.bma.org.uk/ap.nsf/Content/Confidentialityunder16](http://www.bma.org.uk/ap.nsf/Content/Confidentialityunder16)

including any possible negative effects. If the clinician feels that the patient is not able to give informed consent or be persuaded to include their parents in treatment decisions then clinicians may disclose the patient's information to their parents without the patient's consent. As with adults, young people's information must be kept secure and confidential unless this is felt to not be in the patient's best interests.

Obviously, this merely touches the tip of the topic and of the huge number of papers, documents and guidance which has been written about it. Other issues such as competency in adults have not been addressed here. But hopefully this article provides enough information to enable you to find out more. This is a very important and complex issue and reliance should not be made on this summary. Find your local Caldicott Guardian, go on courses, even try to decipher the documents yourself. Then check, double check and check again!

### Useful links and references (In no particular order)

- "NHS Confidentiality Code of Practice", NHS (2003)  
[www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/PatientConfidentialityAndCaldicottGuardians/DH\\_4100550](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/PatientConfidentialityAndCaldicottGuardians/DH_4100550)
- "Data Protection Act 1998", Department of Health (2007)  
[www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Recordsmanagement/DH\\_4000489](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Recordsmanagement/DH_4000489)
- "Patient Confidentiality and Access to Health Records", Department of Health  
[www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/index.htm](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/index.htm)
- "Data Protection (Processing of Sensitive Personal Data) Order", Office of Public Sector Information (2000)  
[www.opsi.gov.uk/si/si2002/20022905.htm](http://www.opsi.gov.uk/si/si2002/20022905.htm)
- "Principles of Information Security", Connecting for Health (2008)  
[www.connectingforhealth.nhs.uk/systemsandservices/infogov/security?searchterm=data+protection+security](http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security?searchterm=data+protection+security)
- "Confidentiality: Protecting and Providing Information", GMC (2004)  
[www.gmc-uk.org/guidance/current/library/confidentiality.asp](http://www.gmc-uk.org/guidance/current/library/confidentiality.asp)
- "Confidentiality and people under 16", BMA (1994)  
[www.bma.org.uk/ap.nsf/Content/Confidentialityunder16](http://www.bma.org.uk/ap.nsf/Content/Confidentialityunder16)
- UK Clinical Ethics Network (contains links to BMA, GMC and DH guidance)  
[www.ethics-network.org.uk/policies-and-guidelines/confidentiality-1](http://www.ethics-network.org.uk/policies-and-guidelines/confidentiality-1)
- "Records management best practice in relation to the creation, use, storage, management and disposal of NHS records", Scottish Government Publications (2008)  
[www.scotland.gov.uk/Publications/2008/07/01082955/0](http://www.scotland.gov.uk/Publications/2008/07/01082955/0)
- "Data Protection and FOI - how do the two interact?", NHS (for tools, advice and publications on the Data Protection Act and Freedom of Information)  
[www.foi.nhs.uk/act\\_dataprotection.html](http://www.foi.nhs.uk/act_dataprotection.html)
- "NHS Caldicott Guardians", Department of Health (2008)  
[www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH\\_4100563](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563)
- "Caldicott Guardians", Connecting for Health (2008)  
[www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott](http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott)
- "Caldicott Guardians", NHS Scotland  
[www.confidentiality.scot.nhs.uk/caldicott.htm](http://www.confidentiality.scot.nhs.uk/caldicott.htm)

## The Times They Are A-Changin' - Public and Private in Ancient Greek Healthcare Confidentiality

**Marika van Aerde BA MA**

*Research graduate from the University of Nijmegen*

[m.aerde@live.com](mailto:m.aerde@live.com)

Ἄ ὅ ἄν ἐν θεραπείῃ ἢ ἰδίῳ, ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπεύτης κατὰ βίον ἀνθρώπων, ἄ μὴ χρὴ ποτε ἐκκλάεσθαι ἕξω, σιγήσομαι, ἄρρήτια ἠγεύμενος εἶναι τὰ τοιαῦτα.

*'All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not*

*to be spread abroad, I will keep secret and will never reveal.'*

The Hippocratic Oath (4th Century BC)

In Western European history, Hippocrates is considered to have been the first physician to have separated the discipline of medicine from religion and mystic cults. He argued that disease was not a divine punishment, but a product of external environmental factors, such as living habits and diet. As the above quotation indicates, he believed that physical ailment was a private matter between physician and patient, and far removed from the public world of the Greek pantheon. With this approach, the Hippocratic or Koan school of medicine based its treatments on general diagnosis, patient care and prognosis, allowing for progressive development in clinical practice.<sup>2</sup>

It is perhaps ironic that antiquity's most renowned hospital can be found at Epidauros, the heart of one of the ancient world's largest religious cults. From as early as the sixth century BC, healthcare resorts known as 'sanctuaries' dedicated to Asklepios, the god of healing, were spread all across the Mediterranean. They were resided over by the priests of Asklepios and maintained what appeared to have been a dual system of cult worship and therapeutics simultaneously. Although praised by its philosophers and scientists, Hippocrates' suggested separation between medicine and religion was never openly accepted in ancient Greek society. The contrast between public worship and private healthcare – more so even than the rift between science and religion – called for an approach that would abide by the laws of the Asklepiian cult, and yet incorporate the knowledge of the Hippocratic school.<sup>3</sup>

The boundaries and clashes between private and public held far greater significance for ancient life than our modern day perspective would recognise. Religion was not a matter of private prayer, but of public duty, and therefore the idea of private healthcare was in direct conflict with the Asklepiian cult. However, the physicians at the sanctuaries managed to satisfy both demands with remarkable efficiency. After a patient's required *enkoimesis* at the Asklepiion, a night spent in the temple, the priests would interpret the patient's dream as a diagnosis sent by the god of healing, and would subsequently practice their medicine, as physicians, with all available scientific knowledge in the hospital. By means of payment for their treatment, patients were asked to give votive offerings to Asklepios in the temple when they were cured. In this way, the privacy of medical healthcare was both initiated and completed by an act of public devotion according to the laws of the cult – and thus effectively protected from the public eye, at the same time.

These votive offerings are among the most significant of our few remaining sources on this topic. To a certain extent, their function was comparable to today's healthcare records. Often in the form of relief tablets depicting specific medical scenes or resembling the shape of cured body parts, these offerings recounted the individual injuries and treatments of patients with remarkable detail. The dedication of such an object to a god turned it into divine property, which demanded it to be kept within the temple's *temenos*, the inner sanctuary to which only the cult's priests had access. Particularly in ancient Greek society, this type of offering was an extremely public act that demanded public recognition for those that made the dedication. The safekeeping of the votive objects themselves,

<sup>2</sup> Margotta (1968) 67.

<sup>3</sup> Hornblower & Spawforth (1999) 534.

however, was a matter of strict privacy, even secrecy. This private devotional nature merged effectively with the aspect of public competition in the act of votive offering.<sup>4</sup>

As an example, the dedication relief shown in Figure 1 depicts a patient asleep on a couch during the act of *enkoimesis*; the snake, symbol of Asklepios, is licking the patient's shoulder and represents the diagnostic content of the patient's dream, as interpreted by the priests. In the left foreground a human doctor is treating the patient's shoulder, mirroring the diagnosis from the dream by means of practical medical science. The patient, named Archinos, dedicated this relief to the god in gratitude for his cure, and made sure to have every aspect of the treatment process included. As such, the relief not only served as public proof of Archinos' religious devotion, but also as detailed medical record to be kept private and secure at the sanctuary where he had been treated.



Figure 1: *The Healing of Archinos, ex-voto tablet, 370 BC.* (Athens, National Museum)

Nowadays we no longer need to keep the balance between medical science and religious tradition, but the duality of public and private remains an ongoing, if not increasing issue. The boundaries between private healthcare demands and the public sector often appear to have lost in clarity what they have gained in scientific expertise. The confidentiality of healthcare was an Hippocratic priority, and the Greeks succeeded in transforming the initially conflicting Asklepian laws into the very means to achieve that security and privacy. We no longer have such distinct means at our disposal, and nor do we need to. The times will continue to change, and often for the better – but we must not forget that the past is the foundation of what we tend to take for granted today, and that less may have changed than we would like to think.

## Bibliography

1. Becky, H. (ed) 1957-58. *Anthologia Graeca*. 4 vols. Munich.
2. Gutzwiller, K. J. 1998. *Poetic Garlands: Hellenistic Epigrams in Context*. Berkeley.
3. Hornblower, S. & Spawforth, A. 1999. *The Oxford Classical Dictionary*, 3rd ed. Oxford.
4. Margotta, R. 1968. *The Story of Medicine*. New York.
5. Whitley, J. 2001. *The Archaeology of Ancient Greece*. Cambridge.

## References and Resources – e-Health: Security and Confidentiality

### Jeannette Murphy

*UKHIT Senior Editor and Senior Research Fellow in Health Informatics, UCL CHIME*

[j.murphy@chime.ucl.ac.uk](mailto:j.murphy@chime.ucl.ac.uk)

The following resources deal specifically with security and confidentiality in the context of e-health.

- Anderson R. Patient confidentiality and central databases  
[www.cl.cam.ac.uk/~rja14/Papers/bjgp.pdf](http://www.cl.cam.ac.uk/~rja14/Papers/bjgp.pdf)
- Anderson R. Under threat: patient confidentiality and NHS computing  
[www.cl.cam.ac.uk/~rja14/Papers/drugsandalcohol.pdf](http://www.cl.cam.ac.uk/~rja14/Papers/drugsandalcohol.pdf)
- Anderson R. (2008) Confidentiality and Connecting for Health. *British Journal of General Practice*. Volume 58, Issue 547, pages 75-76.
- Dritsas S, et. al. A knowledge-based approach to security requirements for e-health applications  
[minbar.cs.dartmouth.edu/greecom/ejeta/specialOct06-issue/ejeta-special-06oct-4.pdf](http://minbar.cs.dartmouth.edu/greecom/ejeta/specialOct06-issue/ejeta-special-06oct-4.pdf)
- Hong Y, Patrick TB & Gillis R (2008) Protection of Patient's Privacy and Data Security in E-Health Services. 2008 International Conference on BioMedical Engineering and Informatics  
[ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04548748](http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04548748)
- Kalra D, Singleton P, Ingram D, Milan J, MacKay J, Detmer D & Rector A. Security and confidentiality approach for the Clinical E-Science Framework (CLEF)  
[www.clinical-science.org/industrial/sep2003/AHM2003-DKalra-CLEF-Security-Confidentiality-Paper.pdf](http://www.clinical-science.org/industrial/sep2003/AHM2003-DKalra-CLEF-Security-Confidentiality-Paper.pdf)
- Privacy, Security and Confidentiality  
[www.ahrq.gov/about/annualmtg07/0927slides/estrin/Estrin.ppt](http://www.ahrq.gov/about/annualmtg07/0927slides/estrin/Estrin.ppt)
- Radwanski G (Privacy Commissioner of Canada) (2001) Patient Privacy in the Information Age (speech)  
[www.privcom.gc.ca/speech/02\\_05\\_a\\_010529\\_e.asp](http://www.privcom.gc.ca/speech/02_05_a_010529_e.asp)
- Randell B (2007) A computer scientist's reactions to NpFIT. *Journal of Information Technology* (2007) 22, 222–234.  
[www.palgrave-journals.com/jit/journal/v22/n3/pdf/2000106a.pdf](http://www.palgrave-journals.com/jit/journal/v22/n3/pdf/2000106a.pdf)
- Singleton P. Security and Confidentiality in Integrated Care Records  
[www.nesc.ac.uk/talks/324/3.ppt#256,1,Security and Confidentiality in Integrated Care Records](http://www.nesc.ac.uk/talks/324/3.ppt#256,1,Security%20and%20Confidentiality%20in%20Integrated%20Care%20Records)
- The Confidentiality & Security. Advisory Group for Scotland. Protecting Patient Confidentiality.  
[www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf](http://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf)
- Waegemann CP. Confidentiality and Security for e-Health  
[www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf](http://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf)

<sup>4</sup> Whitley (2001) 140.

# UKHIT Diary

## Feb 2009

### HIMSS AsiaPac09

Theme: Transforming Healthcare Through IT  
Dates: 24-27 Feb  
Venue: Kuala Lumpur Convention Centre  
Sponsor: HIMSS

[www.himssasiapac.org/](http://www.himssasiapac.org/)

## March 2009

### Moving technology into practice: a day in the bay

Date: 11 March  
Sponsor: Royal College of Nursing  
Venue: Wales Millennium Centre, Cardiff Bay, CF10 5AL  
[www.rcn.org.uk/newsevents/event\\_details/rcn\\_events/e-health](http://www.rcn.org.uk/newsevents/event_details/rcn_events/e-health)

### 2009 AMIA Summit on Translational Bioinformatics

Dates: March 15-17, 2009  
Venue: San Francisco, California  
[www2.amia.org/meetings/stb09/](http://www2.amia.org/meetings/stb09/)

## April 2009

### Med-e-Tel 2009

Dates: 1-3 April 2009  
Venue: Luxembourg  
Sponsor: Med-e-Tel  
[www.medetel.lu/index.php?rub=schedule&page=default](http://www.medetel.lu/index.php?rub=schedule&page=default)

### HIMSS Annual Conference & Exhibition

Dates: 4-8 April  
Venue: Chicago  
[www.himssconference.org/index.aspx](http://www.himssconference.org/index.aspx)

### HC2009: Shaping the Future

Dates: 28-30 April  
Sponsor: British Computer Society  
Venue: Harrogate  
[www.bcs.org/server.php?show=nav.10065](http://www.bcs.org/server.php?show=nav.10065)

## May 2009

### AMIA Spring Congress

Theme: People & Populations: Translation to Transformation  
Dates: May 28 - 30, 2009  
Venue: Orlando, Florida  
[www.amia.org/meetings/2009springcongress/](http://www.amia.org/meetings/2009springcongress/)

### MiddleEast09

Theme: Healthcare IT & Management Excellence  
Dates: 5-7 May  
Sponsor: HIMSS  
Venue: Manama, Bahrain  
[www.himssme.org/09/](http://www.himssme.org/09/)

## June 2009

### e-Health 2009

Dates: 21-23 June  
Venue: Algarve, Portugal  
Sponsor: IADIS (International Association for Development of the Information Society)  
[www.ehealth-conf.org/](http://www.ehealth-conf.org/)

### Globalisation and Health Technology Assessment

Dates: 21-24 June  
Venue: Singapore.

Sponsor: HTAi 2009 (Health Technology Assessment International)

[www.htai2009.org/home.html](http://www.htai2009.org/home.html)

### NI2009 Tenth International Nursing Informatics

**Conference Nursing Informatics**  
Theme: Connecting Health and Humans  
Dates: 28 June - 1 July, 2009  
Venue: Helsinki, Finland  
Sponsor: IMIA, Nursing Informatics Group

[www.ni2009.org/](http://www.ni2009.org/)

### Summer Conference PHCSG

Sponsor: Primary Health Care Specialist Group  
Dates: 29 June - 1 July 2009  
Venue: Chesford Grange Warwickshire

[www.phcsg.org.uk/](http://www.phcsg.org.uk/)

## July 2009

### Patient 2.0 Empowerment

Theme: EHR for Personalizing and Improving Care  
Dates: 1-3 July  
Sponsor: The International Council on Medical & Care Compenetics  
Venue: University of Westminster, London, UK  
[2009.icmcc.org/](http://2009.icmcc.org/)

### AIME '09 - 12th Conference on Artificial Intelligence in Medicine

Date: July 18-22, 2009  
Venue: Verona, Italy  
[aimedicine.info/aime09/](http://aimedicine.info/aime09/)

### Assembly on Education and Faculty Development Institute

Dates: July 25-29, 2009  
Venue: Las Vegas, NV  
Sponsor: AHIMA  
[www.ahima.org/meetings/](http://www.ahima.org/meetings/)

## Sept 2009

### Medicine 2.0 Conference

Dates: 17-18 September  
Venue: Toronto, Canada  
[www.medicine20congress.com/](http://www.medicine20congress.com/)

### MIE 2009

Theme: Medical Informatics in a United and Healthy Europe  
Dates: 30 Aug - 2 Sept  
Venue: Sarajevo, Bosnia and Herzegovina,  
Sponsor: European Federation for Medical Informatics  
[www.mie2009.org/](http://www.mie2009.org/)

## Nov 2009

### AMIA 2009 Annual Symposium

Dates: November 14-18, 2009  
Venue: San Francisco, CA  
[www.amia.org/meetings/upcoming.asp](http://www.amia.org/meetings/upcoming.asp)

### The Collaborative Meetings on Health Informatics (CoMHI)

Dates: 21 - 25, November, 2009  
Venue: Hiroshima, Japan  
[home.hiroshima-u.ac.jp/humind1/comhi2009/index.html](http://home.hiroshima-u.ac.jp/humind1/comhi2009/index.html)

## 2010

### Medinfo 2010

Dates: 13-16 September  
Venue: Cape Town, South Africa  
[www.medinfo2010.org/](http://www.medinfo2010.org/)

To have your event considered for inclusion in the UKHIT Diary,

- Please send details as soon as they are available to Jeannette Murphy, UCL CHIME, Archway Campus, Highgate Hill, London N19 5LW or by email: [j.murphy@chime.ucl.ac.uk](mailto:j.murphy@chime.ucl.ac.uk)

# UK HEALTH INFORMATICS SOCIETY

## What is health informatics?

Health Informatics is devoted to the understanding, skills and tools that enable the sharing and use of information to deliver healthcare and promote health.

The phrase 'Health Informatics' is tending to replace the previous term 'medical informatics', reflecting a widespread concern to define an information agenda for health services which recognises the role of citizens as agents in their own care and self-care, as well as the information-handling roles of the non-medical healthcare professions. 'Health Informatics' is an essential and pervasive element in all healthcare activity. It is also the name of an academic discipline, developed and pursued over the past decades by a world-wide scientific community engaged in advancing and teaching about the application of information and communication technologies to healthcare - the place where health, information and computer sciences, psychology, epidemiology and engineering intersect.

UKHiS is a national association for people concerned with health informatics in both of these senses, and is based on the recognition that practical and scientific concerns in this domain are interdependent and inseparable. Twenty years ago medical informatics was seen largely as the computerisation of healthcare. Today, with computers much more a part of routine daily life, there is a tendency to downplay the computers and technology in health informatics, and to stress the meanings of information in the everyday work of healthcare professionals, in communication, shared knowledge and decision-making, and in the complex social and functional needs of healthcare organizations and services. There is more scepticism (notably by the professions themselves) about guaranteed benefits from computerisation for the delivery of healthcare, and more stress (notably by politicians and managers) on technology and organization as a single agenda and on 'culture change' as a key item in that agenda.

The National Programme for IT (NPFIT) is the most ambitious, considered and widely supported agenda for health informatics ever officially adopted on a national basis. The

scope, challenges and problems it offers for health informatics, intellectual and practical, technological and cultural, are daunting and exciting.

## Aims of the UK Health Informatics Society

The UK Health Informatics Society was founded in 1986. Its purpose is to advance the knowledge and application of medical and health informatics. Its main aims are:

- In co-operation with other groups, to develop and serve an informed, interdisciplinary medical and health informatics community.
- To promote an active research and development community in medical and health informatics.
- To provide an open forum for independent, informed discussion and debate.
- To act as a voice for the professional and scientific community in the formation of information policies and strategies in the national health services.
- To advance the quality and provision of medical and health informatics education and training.

Membership is open to all, including professionals, citizens, patients, and users of healthcare and health information, who share the Society's concerns and objectives.

## Activities and services to members include:

- Publishing *UK Health Informatics Today*, a newsletter which keeps its membership informed of current issues in health informatics, book and software reviews, and forthcoming events.
- Organizing and sponsoring a range of open workshops, conferences and other meetings.
- Gathering and delivering advice and comment on health information policies.
- A website - [www.ukhis.org.uk](http://www.ukhis.org.uk) - with information about the Society, conference details and other useful digital resources.
- A listserv (with searchable archive) open to all members.
- Free subscription to the journal *Health Informatics*

**For More Information:** Contact Colin Gordon, Chair, UKHiS. Address: Health Informatics Manager, Royal Brompton & Harefield NHS Trust, Sydney Street, London SW3 6NP, Tel: 07881 625 146 Email: [ColinNGordon@aol.com](mailto:ColinNGordon@aol.com)

**To Apply for Membership:** Complete the form below and send to the address shown.

## UKHiS Membership Application Form

Annual Membership (please tick)

- Individual member £50 (by standing order) or  £55 (otherwise)  
 Student/retired member £30  Departmental Membership £75

Title ..... Surname .....

Other Names .....

Address .....

Postcode .....

Tel: ..... Fax: ..... Email: .....

*Please make cheques payable to UK Health Informatics Society and return to:*

Colin Gordon, Chair, UKHiS. Address: Health Informatics Manager, Royal Brompton & Harefield NHS Trust, Sydney Street, London SW3 6NP