Edition 10 - April 2009

UK Council of Caldicott Guardians

NHS

The Caldicott Guardian

The newsletter for the Caldicott community

Welcome

Welcome to edition ten of The Caldicott Guardian.

It's been a very busy few months for the Council, the National IG conference has had extremely positive feedback, of which more later. The Council also held its Annual General Meeting, at which the election of new members was formalised.

In the Caldicott Guardian this month there is an article about the progress being made on the effective pseudonymisation of data for secondary use purposes. There's a piece about the implementation of information governance in the independent health sector. Security Corner focuses on some of the measures you can take to prevent your online identity being stolen.

Contents

Editorial

Stephen Hinde
Head of Information Governance & Group Caldicott Guardian, Bupa, and outgoing Chair of the UK Council of Caldicott Guardians

Outgoing Chair's message

There is an old Chinese proverb "May you live in interesting times." We have certainly done that. The last eighteen months has seen extensive media coverage of data losses – losses that have affected a significant proportion of the population. The effect of these data loss incidents has had a significant impact on the whole area of data security, information governance and confidentiality in the public and private sectors; with adverse media exposure, fines and enforcement notices issued by Regulators and contractual impact. Indeed, there has been an increase in Letters of Undertaking issued by the Information Commissioner against Health Trusts and Boards over recent months.

The loss of the infamous two CDs by HMRC with 25 million Child Benefit Records led to more security reviews, reports, investigations, policies and logging of losses than any other one incident I am aware of in over 30 years of being involved in Information Governance. This one incident has raised information governance to Board level awareness and commitment.

There were a plethora of Reports published last year as a result of data losses and concerns over data sharing. Council reviewed the recommendations of these Reports from a Caldicott perspective and commented appropriately with respect to changes to IG Policies and the IG Toolkit. Council also responded to the consultation on the Data Sharing Review (Thomas & Walport) and the NHS Constitution with respect to the fundamental Caldicott Principle – that of protecting patient confidentiality.

In the last three years the information governance environment has changed dramatically; public awareness of confidentiality has increased, as have public expectations. But, and this is a big but, we are still experiencing the same issues of data losses, inappropriate data sharing and ineffective information governance. We do not seem to have learned from the many public mistakes of others. In part, this is the result of under funding of information governance over many years; of an out dated cultural approach to confidentiality and a failure to properly support and fund Caldicott Guardians. I have to say that post the "two CDs" debacle I can see a glimmer of improvement in protecting patient confidentiality and in information governance at the end of a long tunnel.

There is much for Council and each of you to do.

NOTE: Stephen is continuing as a member of the UKCCG, although he is handing over his responsibility as Chair to Dr Emyr Wyn Jones.

Pseudonymisation and secondary uses

Wally Gowing, NHS Connecting for Health

Why Pseudonymise?

The NHS makes extensive use of patient level data collected in the processes of delivering care. When use of the patient record data is not supporting the direct delivery of care or healthcare purposes, it is regarded as being 'a secondary use' of the data. *Confidentiality: NHS Code of Practice*[1] sets out what healthcare purposes are and by implication what secondary uses are.

Healthcare Purposes - These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

Confidentiality also states that for purposes other than healthcare, patient data should be effectively anonymised, as such information is no longer confidential.

Anonymised Information - This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post-code and any other detail or combination of details that might support identification.

Pseudonymised Information - This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

This means that it is necessary to de-personalise the data and pseudonymisation is a technique used for removing patient identifiers from records. When consistently applied, pseudonymisation enables records to be linked over different data sets, different organisations and time, so that a population view of health care and associated activities can be developed from the de-personalised records, that is without identifying individuals.

1 Confidentiality: NHS Code of Practice available at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

What is Pseudonymisation?

Pseudonymisation is the technical process of replacing patient labels (ie data items which identify patients, such as name, date of birth) in a dataset with other values (pseudonyms), from which the identities of individuals cannot be intrinsically inferred.

For example:

- Replacing an NHS number with a random number
- Replacing an address with a location code.

Pseudonymisation may be consistently applied, so that a particular pseudonym is always used to replace a particular patient label or inconsistently, such that a particular patient label is replaced by different pseudonyms in different contexts.

Pseudonymisation may be technically reversible, so a pseudonym can be transformed into the original particular patient label; or irreversible, where it is impossible to go back, as the pseudonymisation key will have been discarded.

De-identification is also aided by the use of derivations to make it less likely that the identity of an individual may be inferred from a particular dataset. For example:

- Age at presentation may be displayed instead of date of birth
- Responsible GP practice may be displayed instead of postcode.

Similarly, data may be aggregated so that classes of patients are shown, rather than details of individuals. For example:

- Groups of patients may be displayed in age bands rather than listed individually with their dates of birth
- Groups of patients may be displayed by area of residence rather than individually with their postcodes.

Secondary Uses

There are many potential secondary uses of patient activity records, such as clinical audit, care pathway audit, clinical research and public health surveillance. Other major uses include medical research and supporting the day-to-day business activities of the NHS Commissioning processes. The latter is at the core of running NHS business between commissioners and providers, with commissioning determining which services should be developed, provided and the subsequent monitoring of delivery. Commissioning mainly makes secondary use of data about patient activity in secondary care.

A major facility collating and managing data for commissioning is the Secondary Uses Service (SUS)[2]. SUS acts as a post box service for commissioning data sets, which contain the activity undertaken in secondary care, to be made available from care providers to commissioners. SUS receives data from providers, undertakes data quality checks, performs derivations, such as electoral ward from postcode, and generates additional information, such as grouping the data into Health Resource Groups (HRG) and applying Payment by Result (PbR) tariffs. SUS is based on a data warehouse with data marts for different users and uses.

Currently NHS commissioning and SUS operate under a 'Section 60/251' approval from the Patient Information Advisory Group (PIAG) (now National Information Governance Board Ethics and Confidentiality Committee) for the use of identifiable data for commissioning purposes. The Section 60 approvals have been made on the basis that commissioning and SUS move towards the use of pseudonymised data and that parliamentary regulations are obtained for the holding of any identifiable data, such as in SUS itself.

2 SUS available at www.ic.nhs.uk/services/the-secondary-uses-service-sus

Implementing Pseudonymisation in the NHS

A Pseudonymisation Implementation Project has been started within the SUS Programme to support the implementation of pseudonymisation for secondary uses across the NHS in England[3]. The aim of the Project is to enable the routine use of de-identified data in day-to-day NHS business processes, as well as to support the provision of facilities for pseudonymisation for national systems, such as SUS and the Hospital Episode Statistics (HES) service. To enable implementation within NHS organisations, the Project needs to ensure relevant technical facilities for pseudonymising and, where necessary, de-pseudonymising are made available.

What is De-pseudonymisation?

De-pseudonymisation is the technical process of providing patient labels (ie data items which identify patients, such as NHS Number, date of birth) from pseudonyms in a reversible pseudonymised dataset, enabling the identities of individuals potentially to be revealed. De-pseudonymisation could be used for instance to enable the identification of individuals selected from analysis of notionally 'secondary use' data as being at risk of re-hospitalisation.

The Project team is working with NHS organisations and an Advisory Group to identify how to implement pseudonymisation without adversely affecting business processes, such as commissioning. Many NHS organisations link locally sourced data to that from SUS; the linkage process is dependent on data quality raising the issue of how linkage can be achieved with pseudonymised data.

Currently two different approaches are being evaluated to determine the most appropriate solution for implementing pseudonymisation. Once the approach is clear, various supporting mechanisms, as well as the requisite technical facilities, will be developed. These supporting mechanisms include changes to the Information Governance Toolkit and setting of pseudonymisation standards through the Information Standards Board leading to the publication of a Data Set Change Notice (DSCN).

For NHS organisations, such as PCTs, the implementation may be a significant change project involving formalising local arrangements on data storage and management and access control regimes and modifying business processes. For instance, clarity will be required about who has access to patient identifiable reports and de-pseudonymisation service, processes to support such access will be required and the usage of such facilities will need to be logged and audited.

Project Progress

The Project timetable will be finalised after the current option appraisal phase is complete. The aim is to enable implementation of the use of pseudonymised data from April 2010. Progress will be reported on the CFH SUS website. Further information about pseudonymisation and the Project can be gained by contacting Wally Gowing (wally.gowing@nhs.net) or Chris Shovelton (chris.shovelton@nhs.net).

3 Pseudonymisation Implementation Project information available at
www.ic.nhs.uk/services/the-secondary-uses-service-sus/pseudonymisation

Information Governance in BUPA

Stephen Hinde, Head of Information Governance & Group Caldicott Guardian, BUPA and member of the UK Council of Caldicott Guardians

Bupa is an International not for profit healthcare organisation with operations in six continents covering Private medical, life & critical illness insurance (9.8 million insured customers), health screening, hospitals, aged care, nurseries and health analytics (23.2 millions lives).

As an integrated healthcare company, Bupa maintains patient, member, customer and other information, which must be protected for ethical, legal, regulatory and commercial reasons.

The Bupa Group IS Security policies, rules, standards and guidelines at all levels incorporate the International Information Security Management Standard ISO/IEC 27002 (formally ISO/IEC 17799 and British Standard BS 7799: Part 1). Compliance with this Code of Practice standard is evidenced through completion of the IG Toolkit – the Independent Sector version as ratified by the Digital Information Policy team of NHS Connecting for Health. Five UK businesses with NHS/DH contracts have completed the IG Toolkit. The IG Toolkit is being rolled out to companies across Bupa including those in the UK with no NHS contracts and overseas subsidiaries as a means of improving levels of Information Governance across the Group. The scored IG Toolkit does enable a comparative dashboard across divisions and territories, giving senior management evidence of compliance, or not, with IG standards in a consistent manner.

This programme is promulgated through the Health Informatics Team, part of the Group Medical Department. This Team also co-ordinates clinical information governance activity through the Clinical Information Governance Steering Committee, whose members include all Medical Directors / clinical leads and business IG leads. The Medical Directors have been designated Caldicott Guardians, wherever in the world they are based – some 25 in all.

The Clinical IG Council provides a strategic lead to the implementation of the IG Toolkit and associated continuous improvement and maintenance programmes with a particular focus on the Clinical Information Governance and Secondary Use Assurance initiatives. It is responsible in the UK for the NHS IG Statement of Compliance.

Sitting alongside the Steering Committee is the Group Information Security Council. This Council ensures that security measures are co-ordinated, properly applied and provide evidence of Information Governance, especially as part of ISO/IEC 27001Certification. It is responsible for the Group IS Security Policy, the Information Security Awareness Programme, ISO/IEC 27001 Certification and PCI/DSS compliance. Bupa in the UK holds 2 ISO/IEC 27001 Certificates and is in the process to achieve others in the UK and USA.

These two Committees / Councils along with Divisional Security Councils report to the Group Information Governance Council, chaired by the author, who is also the Group Caldicott Guardian. This Council is accountable to the Information Governance Executive Committee of the Board for Information Governance across the Bupa Group. It is a focus for the consideration of Information Governance issues which impact the ability of Bupa businesses to ethically and securely handle personal data; to comply with the Information Governance requirements of legislation and regulation; and to comply with Information Governance contractual obligations.

The Executive Committee has responsibility for the oversight of Information Governance across the Group. It sets IG strategy for the Bupa Group and directs achievement of Information Governance across the Group through the author.

Report from the National Information Governance Conference "Setting the direction for Information Governance"

The national IG conference held by the UK Council of Caldicott Guardians on the 25 February 2009 attracted over 500 delegates from across the Information Governance spectrum.

The Council was especially pleased that Dame Fiona Caldicott had agreed to open the conference and she delivered the first of several informative and instructive presentations on the evolution of the Caldicott role and the raised profile of Information Governance including the subsequent impact on all involved in operational delivery of Information Governance.

The day provided a forum for policy makers, Caldicott Guardians, IG Managers, Directors and others from health and social care settings to discuss Information Governance, and to gain early information on future developments. The morning speakers delivered a series of lively and engaging presentations and the conference seminars were ably facilitated by members of the Council and members of the Digital Information Policy team.

The conference was hosted by the Digital Information Policy team and expertly supported by the NHS Connecting for Health Events team.

Below is a report about the presentations given by the morning speakers.

Welcome and introductions:
Mr Stephen Hinde, Chair of the UK Council of Caldicott Guardians

Stephen Hinde introduced the National Information Governance Conference and welcomed all delegates and thanked them for participating in the conference.

He spoke about the background leading to the appointment of Caldicott Guardians and in particular the concerns at that time about access to health records by people not involved in the care of the patient. Technology had provided benefits to healthcare, in relation to appropriate information sharing, but the same technology had created more surveillance and increased the potential for large losses of personal data. Stephen mentioned that it was in fact the fall-out from the data loss by HM Revenue and Customs that had raised the profile of information governance to Board level.

Stephen also spoke of how the role of Caldicott Guardian had been introduced to the BUPA Group and of his belief that he was the first Caldicott Guardian in the country, being asked to take on the role very shortly after the Caldicott Report was finalised.

SPECIAL GUEST: Beyond Caldicott: The evolution of the Guardian role

Dame Fiona Caldicott, Principal of Somerville College, University of Oxford

Dame Fiona Caldicott receiving flowers from Mr Phil Walker on behalf of the UK Council of Caldicott Guardians

Dame Fiona spoke about the origins of the Caldicott Guardian including the multidisciplinary working group that had been set up to address professional concerns about the sharing of patient identifiable information within and outside of the NHS. The Caldicott Report reviewed 86 flows of patient identifiable data and tested them to see whether there was a need for the flow and whether all the information transferred was required. It was pleasing to see that organisations were paying more attention to routine monitoring and mapping of information flows.

The working group had no idea that the role of Caldicott Guardian would continue and in fact become more important due to the raised profile of confidentiality and patient awareness. Dame Fiona was especially gratified at the continued relevance of the Caldicott Principles, and said that the Principles had stood the test of time and would hopefully be relevant for decades to come.

Throughout the term of the working group organisations were contacted to find out whether patients had complained about information sharing or confidentiality issues - no such complaints were reported. However, a major development since publication of the Report was the increased awareness amongst patients, families and advocates about the collection, use and confidentiality of personal data. Dame Fiona summarised by saying that the test now is for everyone to ensure personal information is safeguarded and that a patient-centric service is provided.

KEYNOTE ADDRESS: Public confidence in public systems

Christine Connelly, Chief Information Officer for Health, Department of Health

Christine Connelly spoke about risk being the most important thing to understand in terms of information governance and how the role of the Caldicott Guardian would be so much easier if it was about saying that no-one could have access to any personal information. However, the role is about protecting personal information and enabling appropriate information sharing, so that the right people get to see the information when they need it, but only when it is needed for them to their job.

Health and social care was operating in an environment of changing public attitudes, recent research had shown that 91% of citizens are happy for the NHS to store and hold their data in the belief that clinicians will use the information appropriately. When the same people were asked about the broader public sector and private companies, 64% were concerned about how their information was held and used.

The NHS has been managing data for the past 60 years and has always had to manage the risk inherent in that. When single paper files were shared there was still a risk of loss and a risk that an unauthorised person might read the file. Both types of risks rise when information is moved more widely around the system and when the number of patient interactions goes up. Currently about 1 million patients see someone in the NHS every 36 hours and 3.5 million people move GP each year. The possibility of something going wrong is significant due to the huge amount of information being processed each day. For example, the current number of PACS digital images stored would take 300 years to view if one was to sit down and view them all - the volume of information stored creates its own risk.

Although the NHS is moving towards the digital age, in the current mixed environment - paper and electronic records - losses of paper records are reported as serious untoward incident (SUI) more frequently than digital losses. The Department of Health takes all losses very seriously and Christine mentioned that she receives SUI reports from the Digital Information Policy team, which she in turn reports to the Minister for Health. The NHS is starting to manage the issue of small scale losses, but the introduction of databases holding well-organised, larger sets of information in central locations has created another risk. Caldicott Guardians and Senior Information Risk Owners have to consider and balance the risk of small scale losses; the risk to large databases and the risk that information is not available when required - all the while recognising that any loss is unacceptable.

Many of the losses are due to people doing their job with the best of intentions, when something unexpected happens resulting in the loss of a file, laptop, DVD or memory stick, or a theft from the place of work or in transit. Organisations have to consider what action (if any) needs to be taken when a member of staff loses personal information. This will depend on the circumstances surrounding the incident.

Christine illustrated this with two examples of data loss, the first occurred when a district nurse was visiting a patient and had other patient records locked in the car boot, and the car was stolen from outside the patient's house. The nurse was following procedure and it was unlikely that the thief was looking for the information, although it could still find itself in the public domain. The Trust decided it would be inappropriate to discipline the nurse. The second example involved the loss of 80 patient records taken away for the purpose of research. However, the Trust policy made it clear that the doctor had no authority for accessing the records and she was dismissed. A more difficult scenario to make a decision on is where someone has not followed the correct procedure, but circumstances have forced them into non-compliance.

Organisations need to ensure they have clear policies for staff, ensure all measures are taken to protect data, give staff the right tools for the job, provide training and ensure staff are informed of the consequences of failure to comply. The Department is assisting with this by clearly stating policies and making guidance and tools available - e.g. the IG Toolkit.

In summing up, Christine emphasised that organisations need also to explain why things are done and only in this way would a real change in behaviour and mind-set be achieved. Each person needs to understand that information is valuable, privileged and should be treated with care, and that it is an important element of the person receiving care or treatment. Christine asked delegates to explore how communicating the intent of information governance and changing behaviour can be achieved.

The National IG Board for Health and Social Care (NIGB)

Harry Cayton, Chair of the National Information Governance Board for Health and Social Care

Harry Cayton informed the delegates that he was impressed by the turn-out for the conference and the level of support and interest there had been in attending. He spoke of how the delegates were in the front-line of a real shift in the way information was used, and also central in the public debate about the relationship between citizens, their information and the government. The NHS also had a role in the debate about the use of personal information for anti-terrorism, child protection and improving public services.

The starting point for the NIGB was the review of information governance carried out by Harry which built on the Caldicott Report and identified 9 separate bodies giving advice on information governance and accountable in different ways. The

recommendations of the IG Review were:

- The development of a simpler framework for information governance
- Greater resource and support for Caldicott Guardians
- A single body to provide advice and policy development
- Clarification of lines of communication

Linked to the Review was the development of the NHS Care Record Guarantee as the explicit contract between patients and the NHS designed to describe good practice.

Initial expectations were that the Patient Information Advisory Group (PIAG) would take on a new wider statutory role as the single body providing IG advice, and proposals were made to Ministers for this to happen. However following legal advice it was decided that a better option would be to create a new body. This was included within the Health and Social Care Bill and the NIGB became a statutory body in November 2008. Former members of PIAG and others now form the Ethics and Confidentiality Committee of the NIGB to consider the section 251 applications.

Members of the NIGB are drawn from two groups:

- Nominated individuals - e.g. from the Association of Directors of Adult Social Services, the British Medical Association, the Royal College of Nursing, the UK Council of Caldicott Guardians and the Academy of Medical Colleges.
- Publicly appointed members - a mix of people, including patients, a lawyer, a rabbi and an ex-Chief Constable, appointed by the NHS Appointment Commission.

There are also bodies that have observer status on the Board, including the Department of Children, Schools and Families, the Scottish Government and the Welsh Assembly. Northern Ireland has also been invited to send a representative.

The primary purpose of the NIGB is to support the sharing of information, in a safe, secure and confidential way for the right purposes, and that will include sometimes saying that information should not be shared. The Board:

- Monitors information governance practice
- Advises the Secretary of State
- Publishes guidance
- Manages section 251 applications

The NIGB provides advice and guidance to anyone who uses health and social care information, including advising members of the public. Harry spoke of a current issue about patients requiring information in their health record to be removed when they believe it is incorrect. The information cannot be deleted as it may have been relied upon by the clinician in making a clinical decision. Therefore the Board is working with patients and clinicians to produce guidance for organisations to apply when they receive a correction request or there is a dispute about recorded information between the patient and the clinician.

The Board is advisory and not executive which means that they cannot tell anyone what to do, however, they have great influence as they can give advice whether asked for or not and can require NHS and social care organisations to inform the Board what they have done with the advice. The responses can then be published as part of the NIGB Annual Report. This holds public bodies to account in a public way and allows a public debate about why advice has not been taken and why best practice identified by the NIGB has not been implemented.

The Board has raised two concerns with the Secretary of State for Health recently, the first related to the NHS Constitution and the provision

for researchers to access patient information without consent. This led to a wording change to the Constitution document. The Board is now in the process of talks with the Department of Health to enable the recruitment and participation of patients in clinical research without breaching consent or confidentiality requirements.

The second concern raised was about the information sharing proposed in the Coroners and Justice Bill. The NIGB has advised that health and social care records should be exempt from this provision.

NIGB decisions are made in line with an explicit ethical code which is published in the Annual Report. This is an important part of public accountability and it enables people to understand and challenge the rationale when there is more than one "right" answer. All decisions start with application of the Caldicott Principles, with the interests of patients and service users coming first and a recognition that informed consent and personal autonomy underpin the provision of health and social care. The Board seeks to ensure that the right information is available to the right people at the right time to provide individual care. The Principles are sometimes in tension with each other so the Board has also developed criteria to weight the debates.

The Board's work programme covers health and adult social care; currently it is working to gain a better understanding of social care and has recently developed a Social Care Record Guarantee, which if implemented, will enable health and social care organisations to more safely share personal information. Specific work has been undertaken on children's health records, including how to involve children in decisions about their care especially in relation to Gillick competence issues; and consideration of whether ContactPoint will contribute to child protection. The Board is reviewing the particular challenges of introducing the electronic health record into the mental health setting. Current work also includes building a national framework around the development of the databases being created by the NHS Information Centre for Health and Social Care and use of the personal information for clinical audit and research.

Statements of working collaboration are being developed with various bodies and the first of these is with the UK Council of Caldicott Guardians.

The aim of the NIGB is to provide clear, consistent and practical advice as it is essential that advice is "do-able" in the real world. Harry illustrated this by relating the work being carried out with smartcard and registration authority colleagues to develop group working cards, so that A&E staff can login with one card but still have individual accountability. Similar work was being carried out pharmacies in relation to electronic transfer of prescriptions. These illustrate practical solutions that follow proper principles and that people can understand, causing them to be less likely to create unsanctioned short-cuts.

Harry summed up by saying that privacy was not an ancient right in the UK, but a hard won achievement of modernism. Privacy was increasingly important as we move into the electronic age as technology has the ability to enable us to better manage our lives but also has more potential for our privacy to be invaded.

Supporting collaboration across local authorities and the NHS

David Johnstone, Chair of the Electronic Social Care Record Implementation Board

David Johnstone spoke of how the crucial area of collaboration between health and social care must be achieved if the health and social care service is to meet the needs of everyone. His presentation focused on the practicalities of achieving collaboration illustrated with examples to stimulate discussion of what collaborative working means. The transformation programme of health and social care is about the service putting individuals at the centre where individual needs come before organisational convenience, and where patients and service users contribute to the care plan and the care record.

David illustrated his points by relating the experience of Devon integrated care services - a joint working arrangement between Devon PCT and Devon Social Services. There were obvious benefits to working in this way, including the use of a single assessment process so that individuals do not have to repeat the same story to different care professionals; a reduction in bureaucracy; and the sharing of information enabling better care and practice. Collaborative working also breaks down barriers between the different professions, provides value for money and improved patient outcomes.

Devon has 23 integrated complex care teams clustered around general practices of approximately 30,000 patients. The aim of the teams is to work with people with chronic and long-term conditions primarily looked after within the community. The information governance and information sharing issues were identified at the outset of the programmes with the individual service user having the crucial role - assessments can be commenced by any member of the team and the service user is then asked whether that information can be shared with other relevant members of the team. The teams work within the National Information Governance Board principles, whereby the interests of the patient come first; informed consent and personal autonomy underpin the provision of health and social care; and the right information is available to the right people at the right time to provide individual care whilst preserving confidentiality. This means that service users have appropriate control over and access to their own information, and its use. Permission to use the information is reviewed and revised on a regular basis.

The complex care team process is based on the "virtual ward" principle which means getting the care out of the acute sector and into the community where most other services (housing, the third sector, etc) are. Patients and service users are cared for in their own homes and identified by various case finding tools and through the experience of the complex care team members.

The integration began with the PCT provider services and there are now general practices interested in becoming involved to see how they can share their information with the team. In terms of systems, the South West peninsula (4 PCTs and 4 local authorities) has developed a single integrated care planning system enabling health and social care staff to input into the same case management system, the care record can then be shared with all those who have permission to do so. Encryption technologies are also being rolled out and specialists are looking at how the system can be integrated with general practice systems. The electronic single assessment process that drives the service is being put into the acute sector and ambulance services so that the care record will also be available in these areas.

There are technological, cultural and organisational challenges to working in this way but unless the

challenges are met health and social care provision in the community will not be improved. The overall challenge is bringing together confidentiality and information sharing and putting the individual at the centre enabling them to have access, knowing what is in their record, contributing to them and monitoring their own condition.

David summed up his presentation by saying that it is essential to the promotion of health and welfare that health and social care services use all the resources of the community and is not a sickness-based service built around the acute sector. The multidisciplinary way of working with the individual at the centre is the future for health and social services. He left the delegates with a few thoughts about the future, in particular that the IG standards should be mandated for adult social care; that there was a need for a national forum to bring together the planning of information strategy, implementation, structure and governance; and whether social care for adults and children should be covered by the same Government Department.

The IG assurance framework
Phil Walker,
Head of Digital Information Policy,
NHS Connecting for Health

Phil Walker spoke briefly of the HM Revenue and Customs (HMRC) loss of data in 2007 and how this had impacted on the work of the Department of Health and NHS Connecting for Health. He related a quote from the Permanent Secretary for Health that having a major data loss incident is a "career threatening event". Following the HMRC data loss the Prime Minister pledged that the public sector would do everything it could to improve data handling, which set the tone for the following 12 months.

In Government the Cabinet Office carried out a data handling review and published mandates and recommendations covering stronger accountability; mandated security standards; culture change and greater scrutiny. This also required that all departments implement information risk management throughout their delivery chains. Where a department could not enforce implementation they were directed to influence change.

In the NHS data loss incidents came under the spotlight and serious untoward incidents have happened on a regular basis, this is distressing on the one hand but on the other the transparency that reporting requires provides opportunities for lessons learned. The size and complexity of the NHS increases the risks to personal data and the reporting requirement is more stringent than in Government departments due to the special nature of health records. Phil spoke of the incidents that had been reported to and investigated by the Information Commissioner and that 8 Trusts had been required to sign undertakings to improve their data handling and information security. The most common causes of reported incidents were that either data or kit had been lost, or kit had been stolen. Sometimes the losses/theft had occurred in circumstances where data should never have been put at risk and in those cases disciplinary considerations arise. In other cases, removing the data from the organisation is part and parcel of working in the community.

David Nicholson wrote a series of letters to all NHS Chief Executives making it clear what their responsibilities were including:

- Introduction of IG within the Statement of Internal Controls - Chief Executives have to state whether IG is managed well or if not, explain why not and what measures are being taken to improve.

- Encryption measures that should be in place and central assistance with deployment.
- The mapping of data flows, as it was clear that few organisations understood what data they had and where it was being transferred to and from so that the risks could be managed.
- Ensuring that risks are managed effectively.
- The role of SHAs in particular in moving the agenda forward.
- The role of the PCT as commissioners of care.
- Ensuring that assurances are sought from organisations regarding managing information effectively.

In relation to the requirement for stronger accountability identified by the Cabinet Office, alongside the new requirement for information governance to be added to Statements of Internal Controls, there were additional requirements for a new mandated role of Senior Information Risk Owner and a new hierarchy for managing information risks. The IG toolkit was revised to cover the Cabinet Office recommendation and e-learning modules for SIROs and Information Asset Owners have been provided on the IG Training Tool.

The Cabinet Office mandated security standards require that encryption becomes the norm, that procedure on secure disposal of data and hardware are adhered to and that penetration testing is carried out. Many organisations use overseas support for data processing e.g. data cleansing, and there has been a lot of concern in Government about this. A new Ministerial Committee has been set up to review personal data held overseas and to review all Government proposals for overseas processing. There has been a suggestion of something similar for the NHS but this was unlikely due to the size of the NHS - however the Department will assist by providing clear guidance on what is expected and how additional risks should be managed. NHS Connecting for Health was delivering stronger access controls in later releases of software. Standard contract clauses are already provided through the Office of Government Commerce and other means. Organisations need to focus on managing contracts and on what contractors do with the data.

Culture change was also identified as necessary in the Cabinet Office data handling review. One of the main things is to make people aware that information governance is not just about IT. There is also a need to ensure that everyone who handles personal data knows how to do so in the right way. There is a desire to show that the NHS takes data handling and incidents seriously and applies disciplinary measures where necessary. At the same time many organisations acknowledge that their policies, procedures and training are inadequate and if an incident occurs the fault is not only the individual's. The data handling review recognised that staff working in information governance roles across the entire public sector do not have an appropriate career structure and do not have the opportunity to move into senior positions. This is being looked at for the NHS coupled with work to make clear to organisations how important IG roles are.

In terms of greater scrutiny, information governance now has to be included within organisations' annual reports. All Government departments were directed to publish an information charter for the public - in the NHS the Care Record Guarantee serves this purpose. However, organisations need to be clear about how the commitments in the Guarantee are met, and be clear about the reasons if a commitment cannot be met with information about how long it will take to meet the commitment. The reporting process for incidents is in place and working well.

Within the Department an Information Governance Assurance Programme was set up to look at the Cabinet Office minimum standards, review what the NHS was already doing, identify any gaps and put measures in place to bridge the gaps. The Programme recommended that the IG Framework was extended to all parts of the delivery chain. Phil displayed a list of all the different bodies in the Department of Health delivery chain - these included all NHS organisations; general practices; other independent contractors, e.g. pharmacists, dentists and eye-care services; Walk in Centres; Arms Length Bodies such as the Information Centre for Health and Social Care, NHS Business Services Authority, Blood & Transplant and many more; funded bodies e.g. screening programmes; Social Care & other Business partners; and the Third Sector, i.e. community and voluntary organisations. Many of the smaller organisations have no concept of information governance and no communication channels to inform them what they need to do. New channels are being established to reach these organisations.

Over the years there have been several different interpretations of what IG is about, so the Department is now working with the Information Standards Board to define a new framework standard that clearly states what IG is about and the areas it covers, in terms of management & accountability; process; people; and assessment & audit. Organisations need to reassure Ministers, and to assure each other that they are working to the same standards and providing assurance in the same way. The NHS Operating Framework contains a clear line on what information governance performance should be for 2009/2010, and this is reinforced in Guidance for Board Members and in national contracts for services. Version 7 of the IG toolkit has been amended to ensure it is aligned with what is required across Government. There is a need to engage with NHS Internal Audit colleagues to ensure that there is external assurance of organisations' performance.

Additionally, information governance was seen as a core standard for better health by the Healthcare Commission and there is a need to ensure that this link is retained with the new Care Quality Commission.

For the future the team:

- Are working to bring all organisations in the Department of Health's delivery chain into the information governance framework.
- Has begun talks on amending national contracts for independent contractors.
- Is improving guidance and training provision.
- Is looking at professionalisation of IG roles and a career structure.
- Is taking steps to understand and address the gaps in capabilities within the service.

Information governance - the wider picture
Richard Thomas, Information Commissioner

Richard Thomas spoke about the wider picture, i.e. outside of the NHS and of how up till recently data protection had a poor reputation with begrudging Government interest and was seen as of low commercial priority, and as complicated and legalistic. The situation had now changed; research had shown that the public was taking data protection more seriously and that organisations now see it as a reputational issue, which could affect the confidence of their consumers and service users. Individuals rank protecting personal data highly alongside crime concerns and 86% of those asked now know about their rights to access their data. Data protection and Freedom of Information issues were now setting the news agenda and there were several drivers for change

including the high-profile data losses, more, cheaper and better technology, storage and portability and globalisation.

The regulator had changed as well and had developed a modernised, strategic approach. The Information Commissioner had recently published a Data Protection Strategy which sets out its approach to data protection - prevention of breaches rather than application of the rules for their own sake. The Strategy sets out the assistance that will be provided to the vast majority of organisations that want to get data protection right, whilst tougher action will be taken against the small minority that do not.

Data breaches have played a part in raising awareness of data protection and although there is no legal obligation to report breaches to the Information Commissioner, it is encouraged as a good practice measure. By the end of January 2009, there had been 365 breaches reported, of which 89 were NHS breaches. The Information Commissioner's Office has investigated and taken action in eight NHS cases so far. Each organisation was required to give a formal undertaking to put things right - this is one stage short of a formal enforcement notice.

Richard asked the delegates to remember that data protection is about risk assessment and management and that it's not just about information security but also about mistaken identity, mismatches, inaccuracies, out of date data and excessive data. The Commissioner has examples of real people who have suffered real problems because organisations have not got the governance of data protection issues right. Governance is crucial and it was at the top of the recommendations set out in the data sharing review undertaken with Sir Mark Walport. Governance and accountability have to be considered in conjunction with policies, procedures, contracts, compliance, technology – systems architecture, privacy issues and people.

There was a plethora of relevant reports addressing some of these issues, including:

- A Surveillance Society? - Home Affairs Select Committee
- Her Majesty's Revenue and Customs – Kieran Poynter PricewaterhouseCoopers) and the Independent Police Complaints Commission
- Ministry of Defence – Sir Edmund Burton
- Data Handling in Government – Sir Gus O'Donnell, Cabinet Secretary
- Data Sharing – Thomas / Walport

For the future the Criminal Justice and Immigration Act 2008 gives the Information Commissioner the power to impose financial penalties for deliberate or reckless breach of the data protection principles, and notification fees are to be increased for the largest organisations. Richard also discussed the provisions in the Coroners and Justice Bill for data sharing orders; these had been recommended in the data sharing review and the intention was to enable information sharing in some circumstances where there are currently legal restrictions. The process would enable greater scrutiny than occurs at present and more safeguards as the process requires:

- An explicit data sharing order put forward in advance.
- A privacy impact assessment.
- The proposal to be submitted to the Information Commissioner's Office.
- The Information Commissioner's Office to submit an opinion regarding the proposal's compliance with the Data Protection Act.
- The proposal to be laid before Parliament for debate.

Although there will be more scrutiny the orders have generated controversy in the medical arena due to the scope of the orders - this is much wider than recommended in the Thomas/Walport review, which recommended them for defined circumstances and not as a way of achieving a major change in public policy.

Data protection has a global context and the ICO has commissioned RAND Europe to review European data protection law, its strengths, weaknesses and examination of avenues of improvement provide effective protection whilst minimising burdens. The report is due April/May 2009. The European Commission has also recently announced a review of the European Directive on Data Protection. Richard informed the delegates that he had recently attended a conference of APEC - Asia Pacific Economic Cooperation at which similar data protection issues were debated.

In summing up, Richard asked the delegates to take away as the main message the absolute priority of governance and accountability.

On the afternoon of the conference the delegates attended seminar sessions covering:

- The NHS Information Governance Assurance Framework.
- Using confidential patient information for research and other purposes: the role of PIAG.
- NHS Information Governance Risk Management and Assurance Framework.
- Supporting the NHS Information Governance Assurance Framework.
- Information Governance in Social Care - Pain or Gain.

A panel question and answer session and Chair's closing comments was followed by the IG Practitioner Fringe Event covering the Information Governance Assurance Framework and Information Governance as a professional discipline; and the Annual General Meeting of the UK Council of Caldicott Guardians.

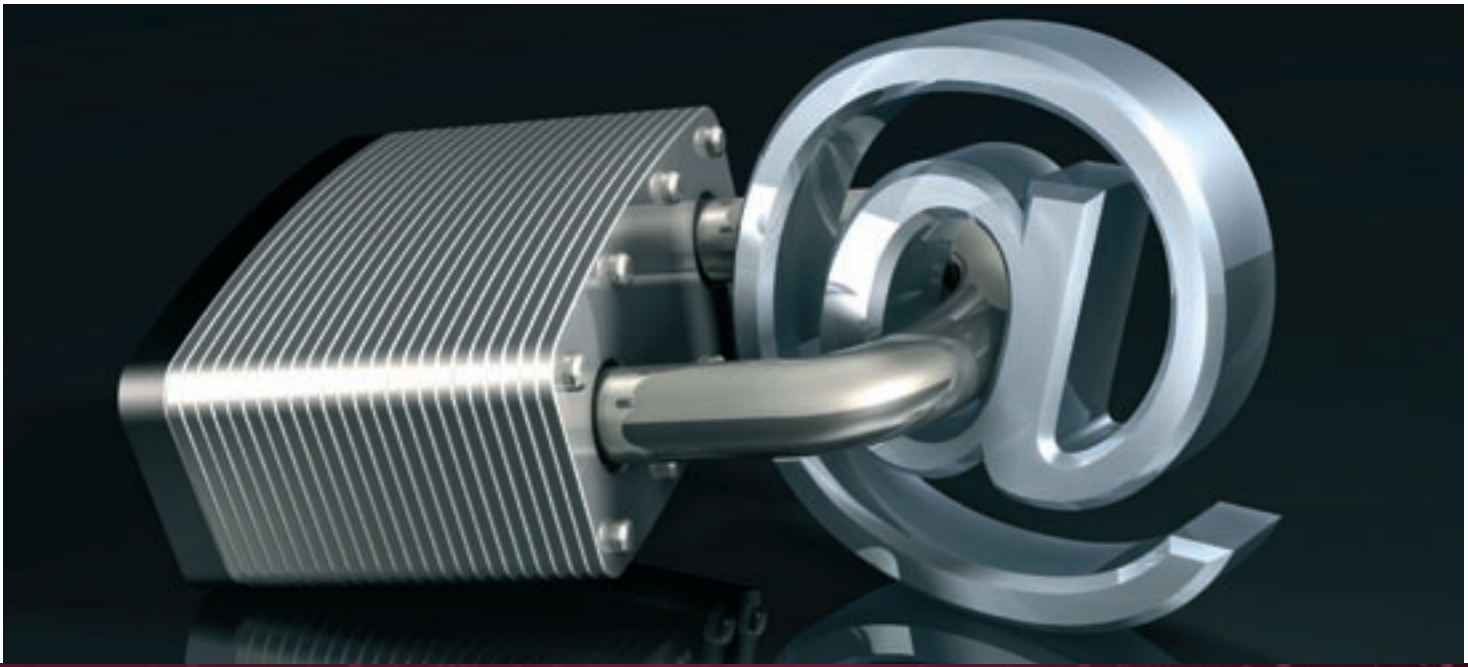
The conference slides and papers are available on the NHS Connecting for Health events system: etdevents.connectingforhealth.nhs.uk/all/2174

Security corner
Online Identity Protection: Your identity is at risk!

The Internet is now over 20 years old and during this time its use has become more widespread than most anticipated when it was first conceived. An ever increasing array of daily tasks may now be undertaken 'online' from booking a holiday, ordering a pizza, to applying for a passport; the Internet is the first port of call for many. The widespread availability of "Internet Ready" devices, such as mobile telephones, games consoles, television and stereo equipment, even refrigerators, have all contributed to the growth of an "online" culture, with an increased global citizenship accessing a growing range of services electronically.

As a consequence the amount of personal data in use over these systems and devices has increased accordingly. The varied range of online services that may hold personal data about its subscribers or users has increased dramatically during the lifetime of the Internet. This data is valuable. Advertisers routinely attempt to gather as much data as possible about those who may be interested in, or use their products. If enough personal data can be aggregated from different locations, it may be possible for criminals to masquerade as another individual using the personal information they have obtained. Often this is with the view of committing some kind of fraudulent activity, such as ordering goods or services online using stolen credit card or bank account details. Unfortunately the victims are often unaware that any fraudulent activity has taken place until they are alerted by their bank, building society, or indeed the police.

The development and popularity of numerous social networking sites has exacerbated this problem and lead to further increases in the availability of truly personal information online, as users unconsciously disclose important information, without realising the security implications of their actions. This in turn has increased the chances of previously disparate or anonymous data being aggregated and made attributable to a specific individual. Data of this type is particularly valuable to criminals. It may be "harvested" by hackers and then sold in bulk to criminal gangs for later use,



or else used specifically to target an individual. In some cases email messages, or even websites themselves may be "spoofed", meaning that a website appearing to be from a legitimate source, may in fact be a cleverly crafted replica of a website, whose aim is to fool users into thinking it is legitimate and thus entering their usernames and passwords. In most cases banks, online games, and social networking sites are the victims of "spoofers". In the case of banks, any email asking a user to enter their credentials should always be viewed as fraudulent. Banks will NEVER ask users to enter their credentials into any website. Banks will write to you in hard copy using the Royal Mail or similar, to inform you of any changes to their service.

In order to try and avoid falling victim to online criminals, users of web based services should carefully consider the security of their personal data, and seriously consider taking steps to ensure that any equipment used to connect to the internet is configured as securely as possible. Security features may be installed or activated to detect the presence of any malicious code, "spy-ware" or other snooping technologies, e.g. key logging software or hardware, which may discreetly record keystrokes including usernames and passwords.

Those online systems requiring personal data should first be examined for evidence of secure facilities, e.g. the "secure" padlock icon in the browser application software, or the "HTTPS" prefix in the URL or address bar of the website in question. Care should ALWAYS be taken to examine the security facilities before any personal data is disclosed. If in doubt, users should contact the website administrators to seek advice and reassurance.

Social networking sites usually offer security features which enable the account holder to set permissions for who can view their pages. In many cases the default permissions enable everyone to see the page, unless the settings are deliberately changed to restrict access. Consideration should be given to the amount and type of data entered onto such sites. Seemingly innocuous data e.g. hobbies, age, pets, favourite bands, football teams etc may be used in conjunction with other information including names, date of birth, address etc. This information, in the hands of determined and malicious criminals may, be used together to fraudulently claim a false identity, possibly to apply for more credible forms of proof of identity – e.g. driving licence application forms etc.

The system being used to connect to the Internet should be kept up to date. Software security patches, anti-virus definitions, anti-spyware, firewall configurations, etc should all be maintained, and used at all times when connecting to the Internet as a means of preventing or deterring online attacks (hacking). Care should always be taken when downloading files, opening attachments, or connecting to new unknown websites. Often, malicious code (viruses) may be hidden inside software or programs that appear to be valid. These are often referred to as Trojans, after the Trojan horse in the story of Troy. Any files found to contain malicious code should be deleted or cleaned immediately. If problems continue, users should seek advice from their anti-virus software supplier. All the main anti-virus solution vendors have a website and helpdesk facility available to their subscribers.

News and updates

NEW e-learning modules for Senior Information Risk Owners, Information Asset Owners and those responsible for information risk management

Following the recent release of NHS Information Risk Management: Good Practice Guidance, the Digital Information Policy team have produced e-learning modules to further support those responsible for information risk management, including Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs).

Modules 2 and 3 are specifically aimed at SIROs.

1. Information Risk Management – Introductory Level
2. Information Risk Management – Foundation Level
3. Information Risk Management for Senior Information Risk Owners and the Information Asset Owners – Introductory Level

Individuals concerned will need to register as a user (if not already) through 'Register now' by completing the online application form and selecting the SIRO/IAO/IRM job roles. Log in details will be sent via email. Once logged in, go to the 'Learning tools' section, click the plus sign by 'Information Risk Management', select the relevant e-learning modules and launch the e-learning.

A Certificate can be obtained within each module upon successful completion of the assessment (assessments are due for release in due course). Alternatively, a record of your interaction and progress with the e-learning modules is available through the reporting and user management tool, accessible by your organisation's IGTT Administrator. These will suffice as evidence of compliance with part of standard 121 and provide for the requirements of the Data Handling Review.

The IG Training Tool can be accessed at: www.connectingforhealth.nhs.uk/igtrainingtool

For any assistance with the IG Training Tool please contact our helpdesk at exeter.helpdesk@nhs.net

Results of elections: the UK Council of Caldicott Guardians

Elections to the Council are now complete. They were carried out by postal ballot in accordance with the Constitution. The election timetable for 2008/2009 was as follows:

- Call for nominations:
  Week beginning 27 October 2008
- Closing date for receipt of nominations:
  22 December 2008
- Issue of voting papers:
  Week beginning 12 January 2009
- Closing date for receipt of completed voting papers: 2 February 2009
- Counting of voting papers: 9 February 2009
- Declaration of result:
  Week beginning 16 February 2009
  and at the AGM (25 February 2009)
- Nominations for Chair and Vice-Chair:
  23 February 2009
- New members take office:
  25 February 2009, on appointment at the AGM

New members

The following members were elected to represent the specified sector for a period of 3 years:

Independent sector

Stephen Hinde - BUPA Group

Social services sector

Ben Heal - Health and Social Care Dept, Sefton Council

Sandra Howard - Adults Social Care and Health, London Borough of Waltham Forest

Mental health sector

Tom Dening - Cambridgeshire & Peterborough NHS Foundation Trust

Mike Foster - Oxfordshire and Buckinghamshire Mental Health NHS Foundation Trust

Primary care sector

Mary Monnington - Somerset Primary Care Trust

Rob Bellingham - NHS Blackburn with Darwen

Claire Warner - NHS Dorset

Acute hospitals sector

Christopher Fincken - Hereford Hospitals NHS Trust

Emyr Wyn Jones - Doncaster and Bassetlaw Hospitals NHS Foundation Trust

Guy Turner - Royal West Sussex Trust

Health, social care and voluntary organisations not already represented

Martin Strange - Lloydspharmacy Ltd

For the complete list of Council members, please visit the Caldicott Guardian web pages at: www.cms.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/membership/index_html

Vacancies

There are still vacant seats in the following sectors:

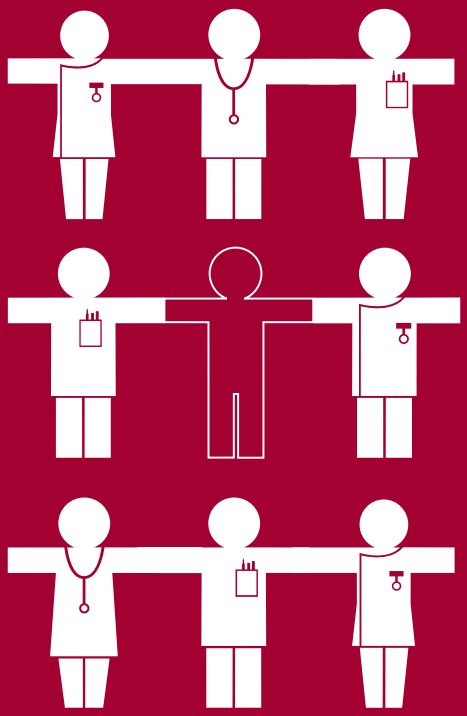
- Strategic health authorities and regulatory bodies (1 vacancy)
- Regional ambulance services (1 vacancy)
- General medical practitioners (1 vacancy)
- Wales (2 vacancies)
- Northern Ireland (2 vacancies)

Contacts

For information about the UK Council of Caldicott Guardians, to suggest a topic or contribute an article for future issues of The Caldicott Guardian, please contact the Secretariat at: ukccgsecretariat@nhs.net

For assistance with Information Governance issues, please send an email to: exeter.helpdesk@nhs.net

NHS
Connecting for Health



NHS Connecting for Health is delivering the
National Programme for Information Technology

Ref: xxxxx