The Caldicott Guardian

The newsletter for the Caldicott community in health and social care

Welcome to edition 13 of The Caldicott Guardian

This issue has been much delayed due to circumstances outside of our control, but we hope you find it interesting and informative, and worth the wait! Click the blue text on the right to go directly to the information you want.

If you have any specific issues that you would like to see covered in the newsletter and particularly if you would like to contribute an article please contact the Council's Secretariat, details are in the Contacts section of the newsletter.

July 2010

Contents

UK Council of Caldicott Guardians

Department of Health

Editorial: Steve Hinde - Member of the UK Council of Caldicott Guardians

Oil slicks and Information Governance

You may think that the BP disaster in the Gulf of Mexico has no relevance to Caldicott Guardians but I think there are four important lessons that we can draw from the incident, what happened before and the reaction to it.

First: the outsourcing of a service or process is just that. Responsibility for the service or process cannot be outsourced. Neither can reputation. Do you know what services and data have been outsourced? Do you have processes to review the Information Governance of the outsource partner? Before the contract was signed? During its operation? It's your responsibility under the Data Protection Act. It is you who will be subject to a penalty from the Information Commissioner's Office in the event of a breach, and it is your reputation that is at risk.

Second: the need for proper risk assessment before a new system or process is introduced and, perhaps more importantly, for the duration. All too often where a risk assessment is made, it is never reviewed thereafter. Circumstances, threat vectors and risk appetites change for organisations, regulators and the public over time, especially after incidents elsewhere. Think Alder Hey and Bristol Royal Infirmary. Think Soham or Baby P.
Risk assessment is a requirement of the IG Toolkit. BP demonstrates the need to continually re-assess risk assessments regularly and effectively.

Take a look at a paragraph from BP's Annual Report and Accounts

> The group generally restricts its purchase of insurance to situations where this is required for legal or contractual reasons. This is because external insurance is not considered an economic means of financing losses for the group. Losses are therefore borne as they arise, rather than being spread over time through insurance premiums with attendant transaction costs. This position is reviewed periodically.

BP took this approach in 1991 and has not bought insurance for any exposures of above $10m since. The reasons given at the time included that insurance premiums paid during the 1980s had far exceeded insurance losses recovered, that BP knew its risks better than any insurance underwriter, and that the risks were bearable by BP. The "self-insurance" strategy paid off during the 1990s but in this decade there has been a litany of events starting with three in Scotland in 2000. The current incident brings the total to four in the US with two in the Gulf of Mexico. Analysts predict the final bill for BP will be $49 billion!!

One reason for this series of lapses may be that, in not having to undergo the process and rigour of presenting and justifying its risk management programme and performance to insurance underwriters each year, BP has not benefited from having sufficient external expert advice on risk management – one of the non-financial benefits of buying commercial insurance.

Early on in my internal audit career I remember the Organisation & Methods Department coming to a similar conclusion to BP's regarding car insurance. The company switched to third party only. The author of the report was much feted by management for his insight and the savings to the group. Within a month, the report author had written off two brand new cars, which more than wiped out the savings on insurance premiums.

Third: the need for Crisis Management to manage the incident and recovery, and to manage the media. Both are important. The BP incident has demonstrated that poor handling of the media may result, rightly or wrongly, in a perception of inadequate management of the response to the incident. In addition, there has been a succession of PR clangers. Not all CEOs are very good at public relations, as so aptly evidenced by Tony Hayward. Saying the amount of oil leaking into the Gulf was miniscule in comparison to the volume of water in the Gulf may be factually accurate, but it shows a gross misunderstanding of the concerns of the public living on the Gulf. It might be miniscule but a little is a lot if it is all on your beach.

BP has received a very bad press in the US bordering on hatred. Compare this to the biggest corporate catastrophe of all time, the Union Carbide (now Dow Chemical) gas leak at Bhopal in which thousands of people died and hundreds of thousands have suffered poor health ever since. There was a similar public outrage and a demand that lessons should be learned and compensation paid. Subsequently, there was US pressure on the Indian government to stop the court case for compensation.

The judge continued with the case which has just ended after 25 years without the participation of Union Carbide! One elderly lady, who was partially blinded, has been in poor health since the explosion and lost most of her family has just been told she will now receive her share of the compensation – just £3! Try typing "I hate Union Carbide" into Google. You will get just eight matches. Type "I hate BP" and you will get 65,500.

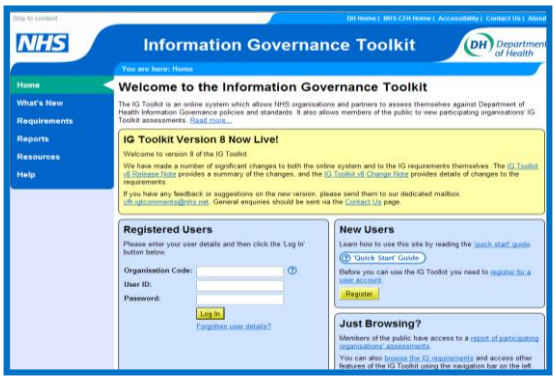
The poor media image has resulted in a perception that BP has not been effective in its response to the explosion and leak. Perception may not be reality. There is a public perception of impact on fishing, but some fishermen have discovered that they can make far more money by hiring their boats to BP for the cleanup than in fishing. Thus the shortage of shrimps may have more to do with the indirect effects of the oil spill than direct impact on the shrimping waters.

And **fourth**, if you are going to have an incident, try to have it at the optimum point in the political cycle. Before the mid-term elections, when the President's ratings are falling, is not the best time. Particularly when during the last major disaster in the area - Hurricane Katrina - the then President reacted slowly and ineffectively. Oil incites much angst and comment in the media.

So too does the loss or disclosure of personal information.

The Information Governance Toolkit - Version 8 is here!

The IG Toolkit is now in its 8th year and has evolved to the point where it is being used by over 20,000 organisations and increasing annually.



It was decided that a major overhaul was needed for version 8, so back in July last year a consultation process was started with users from all backgrounds, from Strategic Health Authorities and NHS trusts through to general practices, pharmacists and commercial third parties. 300 questionnaires, 20 workshops and 2 phases of user testing later, version 8 is ready!

Significant changes have been made to virtually all parts of the system (in line with the suggestions and views gathered), including a major consolidation of the IG requirements themselves.

A key improvement was to make the system more intuitive, so you should be able to get started without having to read any further (although there is a Quick Start Guide for you to refer to). If, however, you want a summary of the key changes then please read the IG Toolkit v8 Release Note (PDF 620Kb).

You can also download the IG Toolkit v8 Change Note (Excel 358Kb) which provides details of changes to the requirements.

Submission deadlines

The final submission deadline for version 8 assessments for **all organisations** is **31 March 2011**.

Trusts and Strategic Health Authorities are additionally subject to 3-stage reporting. However, for version 8, the Baseline and Performance Update submission dates are both **31 October 2010**, effectively creating a two-stage assessment. This is to allow organisations time to acquaint themselves with the new evidence-based approach.

Therefore, by **31 October 2010**, Trusts and SHAs should click the Submit Baseline button and then immediately click the Submit Performance Update button on the Assessment Summary page.

At any point, your next deadline (and the time remaining) is shown in the At a Glance section on the Home Page and also on the Assessment Summary page.

Feedback
Please send any feedback on the new changes to the dedicated feedback mailbox cfh.igtcomments@nhs.net (this mailbox is for feedback **only** and it will close on **31 July 2010.**
For general enquiries, use the **Contact Us** page on the website).

Consolidated and reduced requirement set

The requirement set has been consolidated and/or merged duplicate or obsolete requirements have been removed. Some new requirements have also been added.

Some were existing requirements which now also apply to additional organisation types; two requirements are completely new to the IG Toolkit (8-323 and 8-324).

Number of Requirements	Acute Trust	Ambulance Trust	Commercial Third Party	Dental Practice	Eye Care service	General Practice	Mental Health Trust	NHS Business Partner	NHS Business Services Authority	NHS Direct	Pharmacy	Primary Care Trust	Prison Health	Secondary Use organisation	Social Care	Strategic Health Authority
V7	62	47	17	N/A	N/A	14	62	27	50	52	17	54	16	17	51	36
V8	**45**	**35**	**17**	**16**	**16**	**13**	**45**	**29**	**34**	**38**	**16**	**41**	**18**	**30**	**40**	**28**
+/-	-17	-12	0	N/A	N/A	-1	-17	+2	-16	-14	-1	-13	+2	+13	-11	-8

New powers for the Information Commissioner

In May 2010 the Information Commissioner's Office (ICO) revealed that the NHS continues to have the highest number of reported data breaches - over 300 out of the 1007 breaches involving people's personal information. Many of the 300 breaches affected dozens or hundreds of people meaning that 1000's of people have had their personal information put at risk. Please download the ICO press release for more information.

The vast majority of mistakes were due to human error rather than to technological problems and the Commissioner emphasised the importance of staff training and monitoring staff compliance with procedures and processes.

In the light of the Commissioner's new powers to impose monetary penalties it is now even more important that organisations ensure their staff are trained in and comply with measures to protect personal information. The new powers, which came into force on 6 April 2010, are designed to deter data breaches and enable the Commissioner to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998.

Most NHS organisations are already obliged to inform the ICO when a data breach occurs. The power to impose a monetary penalty is part of the ICO's overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data. The ICO has produced specialist guidance about how it proposes to use this new power.

Information Governance milestones

The year 2009/2010 has been a particular challenge for the IG Policy team of Department of Health (DH) Informatics, as the pharmacy community has joined the wider NHS in demonstrating their Information Governance assurances via the Information Governance Toolkit. More than eleven thousand separate businesses make up this community, and details of each of these were collected from local Primary Care Trusts (PCTs) and used to pre-register on the IG Toolkit.

In collaboration with the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain and colleagues in DH Pharmacy Policy, a package of materials including a comprehensive guidance and companion training leaflet was developed. An email and telephone helpdesk service was established to provide support and advice. This was promoted by local PCT pharmacy leads, online and within the paper materials distributed to each pharmacy. Feedback from the many pharmacies who contacted the helpdesk was very positive.

The year has also seen a significant uptake in the number of users registered on the NHS Information Governance Training Tool. In fact, the IG Training Tool now has over 12,000 organisations with 80,000 plus registered users. There are 21 e-learning modules which are tracked, tested via assessments with certificates issued for those who obtain 80% or more on the assessment. It also contains 93 items of trainer materials which can be used to support bespoke face to face training and group sessions.

Last but not least, we're all quite excited about the work we've been involved with throughout the year with our consultant partner Tony Heap. Tony has been busy all year with the extensive development of the IG Toolkit (the creatively titled 'version 8'), and going up and down the country asking users of the Toolkit how it could be improved, whilst members of the IG Policy team have been re-drafting all the existing requirements into a format which will make it easier to manage in future releases.

In version 7 there were over a thousand separate documents to manage, and that number has decreased to less than 80. Version 8 has just been launched and you can find out more about it in the version 8 article on page 4 but make sure you visit the site to see the changes in action.

The Summary Care Record – Caldicott Compliance

Dr. Emyr Wyn Jones DM FRCP, Secondary Care Clinical Lead
Summary Care Record - National Implementation, NHS Care Records Service, NHS Connecting for Health

NHS Connecting for Health is introducing Summary Care Records (SCRs) for patients in the NHS across England. The SCR is created by uploading data from GP systems to the central technical infrastructure known as the National Spine. The SCR currently includes, as a minimum, a core patient data set which includes information on medications, allergies and previous adverse reactions to medications. A GP can also choose to enrich a patient's SCR by adding further information, if it is thought that there would be particular benefit to the patient and to healthcare providers responsible for their care, for example end of life care plans.

In future, it is possible that information from other sources will be added to the SCR - for example, details of GP 'Out of Hours' consultations or of attendances at Hospital Emergency Departments. This is dependent on development and deployment of appropriate technical solutions and also on the outcome of a review of the scope of the SCR which has been commissioned by the Minister of State for Health.

Some patients and clinical professionals, and their representative organisations, have expressed concerns that holding sensitive personal information on a large central electronic database opens up the possibility of data being accessed inappropriately and used for purposes other than the provision of personal healthcare. Technical safeguards have already been put in place to protect the security of this electronically held data and the SCR programme has also introduced significant Information Governance processes so that maintenance of confidentiality should be ensured, whilst ensuring that information is made available for clinical decision making by those who need to know.

These safeguards are entirely consistent with the recommendations of the Caldicott committee on confidentiality and appropriate use of patient identifiable information - that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the six "Caldicott Principles":

Principle 1 - Justify the purpose(s) for using confidential information

The SCR is no different from any other component of a patient's medical record in that it contains potentially sensitive information, which has been provided by the patient or their representative in strict confidence to the doctor (or other heath professional), for the sole purpose of allowing the provision of healthcare to that patient. There is an absolute obligation under the Common Law of Confidentiality that the information must only be used for that explicit purpose and for no other purpose unless the patient has given fully informed consent for the other use, or unless there is an over-riding public interest reason for disclosure.

Therefore, apart from disclosure in the case of over-riding public interest or when access is required by statute or court order, the only justifiable uses of identifiable information contained in the SCR are to facilitate the provision of healthcare to that individual. This includes use of the information to audit

the quality of care delivered; facilitate the administrative tasks associated with provision of healthcare, including communication and correspondence between health professionals; identification of resources, including finance to ensure appropriate provision; and the arrangement of appointments with healthcare professionals.

Use of identifiable information for purposes other than the delivery of safe and timely healthcare is not justified, unless the patient has given informed consent. This applies to the use of identifiable information for epidemiological and research studies, unless exemption from the need for informed consent has been given following application to the Ethics and Confidentiality Committee of the National Information Governance Board for Health and Social Care (NIGB).

A further safeguard which has been put in place to ensure that clinicians comply with consent requirements when accessing the SCR is the necessity to seek Permission to View (PTV) from the patient when the SCR is to be viewed. This is consistent with the NHS Care Record Guarantee for England, which states that:

> "*We will ask your permission if we need to look at information in your Summary Care Record. When this is not possible, for example in an emergency when you are unconscious, we will tell you later...*"

This requirement is automatically prompted on the computer screen when trying to access an SCR and the clinician is asked to record that the PTV has been sought and consent given.

A necessary over-ride is in place to take into account clinical circumstances when the patient may not be capable of consenting, for example when the patient is unconscious or is considered not to have capacity to give consent because of confusion, intoxication or for other reasons. The clinician may then decide, in the patient's best interest, to view the SCR without obtaining PTV.

That action will be automatically logged and reported to the organisation's nominated Privacy Officer who may then investigate to ensure that the access without consent was justified on the grounds of providing best clinical care.

This emergency access facility to view the SCR without first obtaining PTV can also be utilised when access to the record is considered to be required in the Public Interest or on the rare occasions when access is required by statute or court order. Each request of this sort will be reviewed first by the organisation's IG team and Caldicott Guardian before information is released.

Principle 2 - Only use confidential information when absolutely necessary

As with all patient data, whether held on paper records or electronically, identifiable information contained in the SCR should only be used and shared when absolutely necessary. There are clinical situations where appropriate care can be provided safely and appropriately without having to access the core clinical data contained in the SCR. Clinicians need to make reasoned judgments as to whether accessing core data held on the SCR is necessary in order to safely meet the immediate needs of the patient.

Principle 3 - Use the minimum confidential information that is required

Caldicott principles are applicable to identifiable patient or service user information. If the information is not identifiable then these constraints on sharing and on use of the information are not applicable. The easiest safeguard for the use of clinical information, including that held on the SCR, for any purpose other than the direct provision of healthcare to the individual patient, is to anonymise it. If anonymisation is not feasible, then Caldicott principle 3 should be applied and the minimum identifiable information should be used or shared. This may involve some form of pseudonymisation or use of the NHS number or other single unique identifier, without disclosing more easily identifiable information such as name, address or date of birth.

Principle 4 - Access should be on a strict need-to-know basis

Identifiable, clinical information should be shared only on a "need to know" basis. Therefore, the only people who should have access to clinical data contained in the SCR should be those directly involved in the patient's care. Staff can only be given permission to access patients' SCRs after their local Registration Authority agent has verified their identity and role and issued a Smartcard, which when used with an individual's password, allows an audit trail to be created, recording every instance when the SCR has been viewed.

The need to seek explicit Permission to View (PTV), as detailed above, can be applied to work groups - groups of clinical staff who might be working together in a particular care setting to deliver care to the patient. These work groups can be pre-defined to ensure that only clinical staff who have a need to know can have access to the information contained in the SCR.

Additional controls are incorporated into SCR viewing by creating Role Based Access Controls (RBACs), which limit the extent and nature of the information which can be accessed by individual members of staff, depending on their specific roles and the requirements to enable them to carry out their professional duties. Thus, nursing staff may require a different level of access to sensitive clinical information when compared with doctors, for example. These RBACs are applied to a healthcare professional's Smartcard by the local registration authority once approval is granted by the originating organisation.

Principle 5 - Everyone must understand his or her responsibilities

Doctors, nurses and other health professionals understand the value that patients put on confidentiality. This understanding underpins the nature of the relationship between patient and professional. They know that they are bound by their professional codes of practice and are accountable to their professional regulatory bodies for conduct and performance and this includes the way they deal with information given in confidence. This includes information contained in a patient's SCR.

Similar principles apply to the relationship between Social Care professionals and service users. These principles are as relevant to information contained in the SCR as they are to any other source of clinical or care information.

Health and Social Care organisations are required to comply with recommendations in the Caldicott report on the confidentiality of patient and service user-identifiable information. This includes an understanding of when it is appropriate to share confidential information. Sharing must be justified on a "need to know" basis and only minimal identifiable information can be used, with anonymisation being the norm unless there is a need for identification in order to meet the purpose for which the information was provided in the first place. Health and Social Care workers are bound by their contracts of employment which should include privacy and confidentiality clauses.

Everyone who works for the NHS (or for organisations delivering services under contract to the NHS) has to comply with the NHS Care Record Guarantee for England, which was first published in 2005 and is regularly reviewed by the National Information Governance Board (NIGB) to ensure that it remains clear and that it reflects current law and best practice. It sets out the rules that govern how patient information is used in the NHS and what control the patient has over this. It covers people's access to their own records; controls on other's access; how access will be monitored; options people have to further limit access; access in an emergency and what happens when someone cannot make decisions for themselves.

Principle 6 - Understand and comply with the law

The law is very clear on the need for Data Protection and Human Rights and anyone who uses or discloses confidential health or other personal information without consent can be held liable in law for their actions.

The Information Commissioner has confirmed that the proposals for the roll out of the SCR comply with the requirements of the Data Protection Act 1998 (DPA). All individuals who have access to health records, including the SCR, should have an understanding of the law with regard to data protection, confidentiality and security and should be contractually required to comply with their employing organisation's Information Governance protocols and procedures, or be subject to formal disciplinary procedures.

Employees should know the identity of their employing organisation's Caldicott Guardian who should act as the "Conscience of the Organisation" providing advice and direction on questions of when it is appropriate to share confidential information.

Conclusion

There is particular public and professional anxiety about the implementation of the Summary Care Record (SCR) Programme in England because of the fact that sensitive and confidential information is to be held on a national electronic database (the national "Spine"). This raises a set of concerns about the potential for information to be inadvertently or illegally accessed through hacking or other electronic breaches of security. Also, and importantly in the public mind, is the concern that a national database of personal information might be used by governments and those in power for malign purposes of controlling or otherwise policing or manipulating the population for political or other purposes – a fear of "The Big Brother State".

As far as the first of these anxieties is concerned, the Information Governance and data security controls that the National Programme, within NHS Connecting for Health, has put in place are significant and considered more robust than most commercial systems in place for protecting data security, for instance in the banking sector. Added to that, the protocols for obtaining consent and permission to view the SCR are well defined with audit trails and procedures for identifying breaches and taking appropriate follow up action.

These processes and protocols are entirely consistent with the six Caldicott Principles and it is essential that Caldicott Guardians in health and Social Care organisations should be aware of the Information governance controls that are built into the SCR implementation process. Caldicott Guardians need to be in a position to provide reassurance and informed opinion when their advice is sought in relation to accessing the SCR.

As far as the second public anxiety about the uses that centrally held information can be used, reassurance about this is dependent on the accountability of government and its component parts and the public and the professions have to be reliant on the trust that has to exist within a truly democratic society.

References

1. Department of Health and the UK Council of Caldicott Guardians, 2010. *The Caldicott Guardian Manual.* Department of Health. Available at: www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources/guidance

2. Clay, R., 2009. *Summary Care Record Scope.* NHS Connecting for Health. Available at: www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrscopel.pdf/view

3. NHS Connecting for Health, 2009. *Information Governance and the Summary Care Record.* NHS Connecting for Health. Available at: www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig

4. BMA Press Office, 2010. BMA calls for roll-out of electronic records to be suspended, *British Medical Association*, 10 March 2010. Available at: web2.bma.org.uk/pressrel.nsf/wlu/SGOY-83DDX9?OpenDocument&vw=wfmms

5. National Information Governance Board for Health and Social Care (NIGB), 2009. *NHS Care Record Guarantee for England*. NIGB. Available at: www.nigb.nhs.uk/guarantee

6. NHS Connecting for Health, Summary Care Records web pages: www.connectingforhealth.nhs.uk/systemsandservices/scr

The Royal College of Physicians: IG Training Tool modules for hospital record keeping

As part of the commitment to support the NHS and associated partners with the promotion of effective Information Governance, the IG Policy team worked for several months with the Royal College of Physicians (RCP) and NHS clinicians to create two e-learning modules on clinical record keeping standards.

1. The importance of good clinical record keeping addresses the general principles of good record keeping and is relevant to any clinician who writes in the health record.

2. Record keeping standards for hospital inpatients is targeted specifically at doctors and specialist nurses who clerk patients, and is based on the RCP Generic Record Keeping Standards for hospital admission clerking, inpatient handover and hospital discharge.

A further module on secure handling of confidential information is in development. Although primarily aimed at medical students and junior doctors, it is suitable for students and the newly qualified from any of the health and social care professions. The module aims to raise awareness of the potential risks to confidential information and provide the target audience with useful knowledge on reducing the risks and ensuring that confidential information is protected.

The modules are available in the IG Training Tool which can be accessed at: www.connectingforhealth.nhs.uk/igtrainingtool

Further information about the RCP Generic Record Keeping Standards is available at: www.rcplondon.ac.uk/clinical-standards/hiu/Pages/Medical-records.aspx

Security Corner: Access considerations for movers and leavers

Caldicott Guardians will want to be aware of the potential information governance issues that may arise where inactive or unnecessarily privileged information system user accounts may exist.

The problem: Unused user accounts have the potential for unauthorised access to patient systems and records. If misused, this could lead to possible data leakage and loss of Confidentiality, Integrity and Availability (CIA). Also, greater access to network drives, applications etc than is necessary for a person's role can introduce risks and allow adverse impacts should an account be compromised by an attacker.

The potential risk and impact of accidental damage to systems is greater the more access that is available.

Accrued access: Effective access management means ensuring staff get access only to the information and systems they require to do their job. It's not uncommon for individuals progressing through and up an organisation to carry their existing accrued "access" rights with them as they move, and here lies a big challenge. While there's often a major driver to provision access so that people can effectively take up new positions, there often isn't equivalent consideration to review and reduce or decommission unnecessary access rights when they are no longer required.

The risks and security implications of system access must therefore be fully understood by all departments involved in staff movement and an auditable process must be put in place for staff movers as well as new starters and leavers.

Disabling versus deleting: When a member of staff leaves their employment the immediate response of many organisations is to delete the affected user's account. However, in certain situations, consideration may be given to temporarily *disabling* the account; rather than *deleting* it. This response is possible for two main reasons.

Firstly: There are situations whereby a person may temporarily leave an organisation and then return to work for the same organisation in the same post. For example, an employee on maternity leave or perhaps someone who is taking a career break.

Secondly: Some operating systems remove entire access to resources, systems and infrastructure when an account is deleted. If a member of staff leaves and is being replaced by a new employee, it is possible the organisation may want the new employee to have a similar level of access as their predecessor.

Where user accounts have been temporarily disabled, regular reviews must be made to ensure there have been no attempts to use such accounts and if so investigation must be made.

Security Corner

In summary

1. Organisations must consider carefully whether or not an account needs to be temporarily disabled or permanently deleted. However, when there is uncertainty the most appropriate option is likely to be deletion.

2. Watch for unnecessary accrued / accumulated systems access privilege of people moving within the organisation. Ensure that their access levels are reviewed and maintained appropriate for their position. Access privileges that are no longer required should be revoked.

3. Avoid simply renaming or reallocating a temporarily disabled account. Whilst this process is typically quick and easy there are a number of potential security and patient confidentiality issues that could arise.

The Information Governance Policy team has produced the NHS IG Checklist for Staff Movers and Leavers that can be used for staff who are leaving their NHS employment or who are moving to another position within the organisation.

Caldicott issues

This section of the newsletter aims to detail, in anonymised form, issues raised by the wider Caldicott community and discussed by the UK Council of Caldicott Guardians. The responses expressed in this column do not constitute legal advice; they are the considered opinion of the Council. If you require legal advice you should consult your organisation's legal advisors.

The Council welcome any queries that promote similar discussion, so please see this as your opportunity to raise issues, obtain a response and assist the Council to build up a body of answers to frequently asked questions and develop expertise across the community. This month we look at the New Safe Havens required as part of pseudonymisation processes and sharing information in the absence of patient consent.

Pseudonymisation and new safe havens

An acute trust posed a question about the pseudonymisation processes required as part of the changes in Secondary Use in April 2011. The trust's initial intent was to pseudonymise all patient identifiable data before using it internally or sharing with PCT colleagues.

However the Pseudonymisation Implementation Project (PIP) guidance requires that patient identifiable data is sent to the PCT who should then pseudonymise the data in a new safe haven before further use. The trust is not convinced that the PCT has the same views on information governance as the trust and has concerns that commissioning staff will gain access to identifiable data.

Considerations

In reaching its decision the Council discussed secondary use of data by commissioners and were in agreement that commissioning staff should not have access to identifiable data. The rationale behind the PIP guidance was also discussed, and the fact that there were equally valid arguments for pseudonymising the data *before* it leaves the provider organisation. However, the decision to use 'new safe havens' would also minimise risks to data and enable NHS work to proceed. As the 'new safe havens' have not yet been set up some Council members have refused commissioner requests for identifiable data and have supplied pseudonymised data only.

The Council's decision

The Council's advice is that identifiable data should not be sent directly to commissioning staff but rather, in line with page 7 of the PIP guidance, each organisation should create a 'new safe haven' to receive identifiable data, carry out data quality, linkage and derivation tasks. Once the 'new safe havens' are in place they will need robust governance around them including security measures and appropriate staff training with specific competencies for pseudonymising data so that where necessary identifiers can be restored.

Sharing without consent for an independent inquiry

A trust had two in-patients who were involved in a serious assault on a family member. One (A) is charged with the offence but charges have not been taken forward against the other (B).

The Strategic Health Authority (SHA) is setting up an independent inquiry into the incident and they have requested the clinical records of patient B. The mental state of patient B has improved with treatment and B now undoubtedly has capacity to give or withhold consent on matters to do with his/her care and treatment. B has declined to give consent for the records to be disclosed to the SHA's independent investigator.

The investigator has informed the consultant in charge of the case that if necessary the notes will be obtained through the Secretary of State.

The advice of the organisation's Caldicott Guardian is that there are no grounds to act against the patient's wishes, especially as non-disclosure carries no risk to the safety of any third parties. There is also concern about the potential for damage to the delicate therapeutic relationship with the patient by going directly against B's wishes. Therefore, if the records are required, the SHA will have to pursue the necessary formal channels.

The Council were asked for their opinion on whether:

- The line of reasoning set out by the Caldicott Guardian is correct; and
- The SHA would be able to obtain disclosure via the Secretary of State, or would this only be available via a court order?

Considerations

The Council considered whether there were any other grounds for disclosure, eg a statutory gateway or an overriding public interest. There was also discussion regarding the necessity for an independent enquiry and whether it formed part of a 'lessons learned' process. If so, there might be scope for it to be undertaken as a local critical incident review using an independent chair.

The Council's decision

The Council were in agreement that if the investigator could not formally justify why the records were required, the Caldicott Guardian is correct to refuse the request. If the investigator supplied a valid reason then the public interest in disclosure could be determined. As consent has been declined and without a statutory gateway or evidence of an overriding public interest in disclosure the correct route for the SHA was to obtain a court order, this would provide appropriate protection for the patient and for both organisations.

News and updates

New members appointed to the UK Council of Caldicott Guardians

Further to the call for representatives for the UK Council of Caldicott Guardians, the following candidates have been confirmed as new members by the Council at the beginning of their meeting on 13th July 2010. As only one nomination form was received from each of the sectors a vote was not necessary.

Strategic health authorities/regulatory bodies: Professor Yvonne Doyle, Regional Director of Public Health, Southeast Coast SHA.

Acute sector: Dr Simon Gabe, Consultant Gastroenterologist & Honorary Senior Lecturer North West London Hospitals NHS Trust.

Mental health sector: Dr Dele Olajide, Consultant Psychiatrist, South London and Maudsley NHS Foundation Trust.

Primary care sector: Dr John Richmond, Substance Misuse Specialist, Delphi Medical Consultants Ltd.

Vacancies
Nominations are invited for the remaining vacancies in the constituencies set out below:

- Ambulance services (1 vacancy)
- Primary Care sector (1 vacancy)

Commitment
The term of office runs for three years and the commitment is to four meetings per year, alternately held in London and Leeds.

The Council's work to date has encompassed reviewing papers, training materials and consultations, contributing to responses for Caldicott queries, submitting articles for the Caldicott Guardian newsletter and representing the Council on the National IG Board and at external events.

More information can be found at: www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/

Eligibility to stand
Candidates must be Caldicott Guardians within the UK formally registered with NHS Connecting for Health/ Department of Health.

If you are a Caldicott Guardian and are not registered, please visit the Department of Health website at the address below then download and complete the appropriate form for your organisation type: www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563

IMPORTANT: Please return the registration certificate by post (not fax or scan) to the address stated on the form.

Experience
Candidates should be able to demonstrate a commitment to Caldicott Guardianship, to protecting and appropriately sharing personal information, and be prepared to develop and maintain links with their constituent sector and with other national organisations to ensure that the work of the Council is broadly disseminated.

If you are interested and have good independent judgment and the ability to work effectively as a member of a team whilst being able to speak your mind, please contact the Secretariat for a nomination form: ukccgsecretariat@nhs.net

Decommissioning ContactPoint

Ministers have confirmed the arrangements for the closure and decommissioning of ContactPoint.

A Written Ministerial Statement has been made informing Parliament that ContactPoint will be shut down on 6 August. The Government is continuing to consider the feasibility of a more proportionate approach to supporting frontline professionals to help protect vulnerable children from harm.

A letter to Directors of Children's Services and Chief Executives of ContactPoint National Partners sets out the timetable for shut down and decommissioning, provides guidance for local authorities, National Partners and other partners on the activities they need to undertake, and confirms funding and other support available during this period.

The letter will be issued to Directors of Children's Services to cascade to local authority heads of audit, heads of finance and ContactPoint project sponsors. Implementation Coordinators will be contacting local authorities to go through the letter and to respond to queries and support them where necessary.

The letter and the Written Ministerial Statement have been placed in the House Libraries are available on the Department for Education website under the 'In the News' section at: www.education.gov.uk/news/news/ctptclose

Standards for the provision of teleradiology services in the United Kingdom

Teleradiology has huge potential for improving the efficiency of radiological services and increasing patient safety. However, it also presents significant dangers if its introduction is not guided by a set of standards to give it structure.

We live in a large European community of 27 countries all of whom set their own regulations, have their own governance, and have their own rules for their medical professionals. Changing methods of delivering diagnostic imaging services and the increasing commercialisation of aspects of healthcare, including telemedicine and teleradiology, means that there will be increased fragmentation of where and how services are delivered. Increasingly, there will be a greater opportunity for radiologists from within and outside the European Union (EU) to report on images for United Kingdom (UK) patients.

The Royal College of Radiologists has published *Standards for the provision of teleradiology services in the United Kingdom*.

These standards are the result of consultation with medical, lay and IT experts and are essential to maintain high-quality diagnostic imaging reporting within the UK in an ever-increasing commercially competitive environment. The setting and acceptance of such standards should be seen as part of the patient safety and quality, innovation, productivity and prevention (QIPP) agenda.

The standards can be divided into the following areas:

- standards to ensure patient safety;
- standards applicable to image and report sharing in general, including compliance with the duty of confidentiality;
- standards applicable to a radiologist providing a reporting service through a teleradiology service provider;
- standards applicable to a teleradiology service provider;
- standards specific to a healthcare organisation using a teleradiology service;
- standards applicable to the provision of image viewing at home for the on-call radiologist.

Attention to the guidelines and standards outlined above will ensure the sustainability of local diagnostic imaging services and maintain high-quality standards of reporting, ensuring patient safety and confidentiality. We hope that they will be of value to all NHS organisations looking to outsource some part of their imaging services.

The Royal College of Radiologists is pleased to be able to offer you a complimentary copy of *Standards for the provision of teleradiology services in the United Kingdom.* To obtain your free print copy, please email your postal details to publications@rcr.ac.uk or telephone 020 7299 1162.

Please allow 28 days for delivery.

Conference: Confidentiality and Information Governance - Implementing the GMC and Care Quality Commission recommendations in health and social care: Thursday 16 September 2010

This conference, endorsed by the **UK Council of Caldicott Guardians**, is chaired by **Dr Andrew Harris** *Chair of the Ethics and Confidentiality Committee* of the National Information Governance Board for Health and Social Care. Dr Harris will look at developments since the Caldicott review and the practicalities of sharing information and information risk. Other speakers include **Mr. Ben Heal** and **Mr. Christopher Fincken**, social care and acute sector representatives respectively of the UK Council of Caldicott Guardians.

Delegates will hear about Information Governance and Confidentiality from the patient perspective. The conference continues with a focus on the practicalities of handling primary and secondary patient information including a legal update and developments in implementing the new General Medical Council's (GMC) guidance on Confidentiality.

The GMC Confidentiality guidance came into effect on 12 October 2009. The purpose of this guidance is to help you identify the relevant legal and ethical considerations, and to help you make decisions that respect patients' privacy, autonomy and choices and that also benefit the wider community of patients and the public.

The conference then continues to look at effective information sharing and governance using case studies from:

- the social care perspective;
- the police perspective;
- sharing information for clinical audit, quality improvement and commissioning;
- sharing information with the independent and voluntary sector.

Information governance breaches are currently a serious concern for NHS Trusts. Without a comprehensive system in place you may be opening yourself up to detrimental consequences. The closing session highlights solutions for overcoming difficult ethical decisions and sharing information and records with patients and carers. The conference will provide a wealth of information along with new ideas of how to improve both Confidentiality and effective data sharing in your organisation. Find out more by downloading the brochure at www.healthcare-events.co.uk

Consultations

The Scottish Government: Consultation on proposals for a new Public Records (Scotland) Bill

The consultation seeks views on new legislation to improve record keeping across the public sector in Scotland.

Consultation closes: 4 August 2010
www.scotland.gov.uk/Publications/2010/06/22154359/0

The Scottish Government: Consultation on Extending the Coverage of the Freedom of Information (Scotland) Act 2002

The consultation seeks views on whether FOI legislation should be extended to cover private organisations that deliver a public service, such as the building and/or maintaining of schools and hospitals; privately managed prisons and prison escort services; the building, managing and maintenance of trunk roads; trusts created by local authorities for the provision of leisure and culture; Glasgow Housing Association and the Association of Chief Police Officers in Scotland

Consultation closes: 2 November 2010
www.scotland.gov.uk/Publications/2010/07/20123725/0

Ministry of Justice: Call for evidence on the data protection legislative framework

The Government has issued a Call for Evidence on current data protection law to help inform the UK's position on negotiations for a new EU data protection instrument, which are expected to start in early 2011. The Call for Evidence seeks evidence about how the European Data Protection Directive 95/46/EC and the Data Protection Act 1998 are working, and their impact on individuals and organisations.

At the same time as launching this Call for Evidence, the Government has published a provisional post implementation review impact assessment of the Data Protection Act 1998, on which comments are also welcome. This impact assessment complements the Call for Evidence and publication of a full impact assessment is planned for the end of 2010.

Please note that the Call for Evidence is not a formal consultation, but an evidence gathering exercise.

Call for Evidence closes: 6 October 2010
www.justice.gov.uk/consultations/call-for-evidence-060710.htm

Contact us

- To contact the UK Council of Caldicott Guardians, to suggest a topic or contribute an article for future issues of The Caldicott Guardian, please email the Secretariat at: ukccgsecretariat@nhs.net
- For assistance with Information Governance issues, please send an email to: exeter.helpdesk@nhs.net or telephone 01392 251289
- For assistance with Information Governance for community pharmacies, dental practices and eye care services please contact: pharmacy.assurance@nhs.net or telephone 0113 394 6540

Caldicott web pages: www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

UK Council of Caldicott Guardians