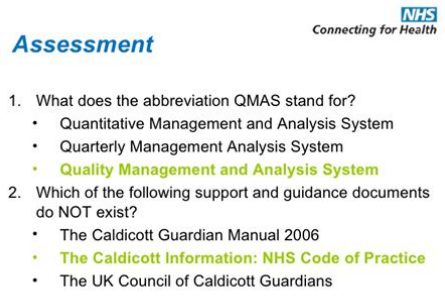
caldicott guardian manual



File Name: caldicott guardian manual.pdf
Size: 1477 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 11 May 2019, 16:31 PM
Rating: 4.6/5 from 800 votes.

Status: AVAILABLE

Last checked: 13 Minutes ago!

In order to read or download caldicott guardian manual ebook, you need to create a FREE account.

Download Now!

eBook includes PDF, ePub and Kindle version

Register a free 1 month Trial Account.
Download as many books as you like (Personal use)
Cancel the membership at any time if not satisfied.
Join Over 80000 Happy Readers

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with caldicott guardian manual . To get started finding caldicott guardian manual , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

Book Descriptions:

caldicott guardian manual

You can change your cookie settings at any time. The UKCGC has also produced A Manual for Caldicott Guardians. It is therefore unable to assist with enquiries related to the conduct of individual Caldicott Guardians. It is intended to be a starting point for newlyappointed Caldicott Guardians, a refresher for the more experienced, and a pointer to possibilities for professional development and support.We'll send you a link to a feedback form. It will take only 2 minutes to fill in. Don't worry we won't send you spam or share your email address with anyone. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others. Organisations typically store, manage and share personal information relating to staff, and the same standards should be applied to this as to the confidentiality of patient information. They should also be compassionate, recognising that their decisions will affect real people—some of whom they may never meet. The importance of the Caldicott Guardian acting as "the conscience of the organisation" remains central to trusting the impartiality and independence of their advice. A key relationship is with the Senior Information Risk Officer SIRO. This aspect of the Caldicott Guardian's role is particularly important in relation to the implementation of the digital and paperless agendas. It was set up to facilitate the sharing of good confidentiality practice and the promotion of a national approach to confidentiality and information sharing. The report made several recommendations, one of which was the appointment of Caldicott guardians, members of staff with a responsibility to ensure patient data is kept secureRetrieved 20200218. Retrieved 20200218.http://cpils.com/userfiles/hotspot-jacuzzi-manual.xml

- **caldicott guardian manual, caldicott guardian manual 2017, caldicott guardian manual, caldicott guardian manual, caldicott guardian manual 2019, caldicott guardian manual 2017, caldicott guardian manual pdf, caldicott guardian manual download, caldicott guardian manuals, caldicott guardian manual 2017.**

By using this site, you agree to the Terms of Use and Privacy Policy. It provides sound foundations for those seeking to expand their understanding of the Caldicott Guardian Role, and its function within Information Governance, and inspiration as to how it can be implemented and developed in their own organisations. The content is based on the latest national guidance including the Caldicott Guardian Manual. A range of topics are covered including the ethical and legal considerations in information sharing, confidentiality, handling requests from the Police, domestic violence, relatives, assurance and the regulators. Handouts, Templates and other tools for decision making and recording decisions are provided. This interesting and informative course is fully interactive; and participants in small groups will face a number of case study challenges throughout the day building personal knowledge, understanding and confidence. We will provide full instructions for accessing the platform along with login details. Led by experienced and highly rated trainers, inhouse training works out costeffective for groups and saves travel time. You are viewing premium content from Croneri. In Practice Caldicott Principles The Caldicott principles, which were updated in 2013, should be employed to examine the conditions under which patientidentifiable information is used or shared. They are as follows. Principle 1 — justify the purposes for using confidential information. Principle 2 — only use confidential information when absolutely necessary. Principle 3 — use the minimum information that is required. Principle 4 — access to confidential information should be on a strict needtoknow basis. Principle 5 — everyone must understand their responsibilities. Principle 6

— understand and comply with the law. Principle 7 — the duty to share personal information can be as important as the duty to have regard for patient confidentiality.http://www.favourlight.com/attachment/hotspot-hot-tub-owners-manual.xml

Overall there should be a balance between the protection of patient information and the use and sharing of this information between agencies to improve care. Patientidentifiable information includes the patient's name, address, full post code and date of birth any pictures, photographs, videos, audio recordings or other images of patients the patient's NHS number and local patientidentifiable codes anything that may be used to identify a patient directly or indirectly, eg rare diseases, drug treatments or statistical analyses using very small sample sizes which may allow individuals to be identified. Another key recommendation of the Caldicott Committee was the appointment in each NHS organisation of a Caldicott Guardian whose role is to oversee the use and sharing of patientidentifiable information. The Caldicott principles are supported by websites offering advice, information, exemplar policies and other resources on the NHS Digital website for England, the NHS National Services Scotland website for Scotland and the NHS Wales website for Wales. The Role of the Caldicott Guardian The role of the Caldicott Guardian for both health and social care covers not only the principles outlined above but also the wider aspects of information management, including the Data Protection Act 2018 the NHS Act 2006 section 251 the Freedom of Information Act 2000 the Human Rights Act 1998 the Computer Misuse Act 1990 the NHS Constitution January 2009, updated February 2015 NHS Information Governance The Caldicott Guardian should be as follows, in order of priority. A member of the management board or senior management team of the health or social care organisation. A senior health or social care professional. A member of staff who has the responsibility for promoting clinical governance or equivalent in the organisation. If it is not possible to satisfy the above criteria, there should be constant review of the assignment of the role to the individual concerned.

This individual should also have a close relationship with the senior health professional responsible for promoting clinical governance or social care equivalent. The Caldicott Guardian must have enough seniority and clear authority from the board or senior management team and Chief Executive to influence strategic policy development and planning. Examples of Caldicott Guardians include Caldicott Guardian Organisation Board Level Clinical Director NHS Trust Provider Board Level Director with clinical governance responsibilities Clinical Commissioning Group Medical Director Independent heath care providers Senior social care professional manager Social care Individual general medical practices are not required to have a Caldicott Guardian; however, they do need to appoint an Information Governance Lead. The Information Governance Lead, if not a clinician, will require support from a clinically qualified individual. Clinical Commissioning Groups are required to ensure that there is an Information Governance Lead within every practice and provide the appropriate support and guidance, if needed. The key function of the Caldicott Guardian is to ensure that the highest practical standards are maintained for the handling of patientidentifiable information between the NHS, Councils with social services responsibilities and other partner organisations. In essence, the Caldicott Guardian acts as the organisation's "conscience" by providing advice on the appropriate sharing of information, some of which will relate to legal and ethical decisions in this area. The Caldicott Guardian also has an important strategic role in representing Information Governance requirements and issues at board or senior management team level as well as at all levels of the organisation's governance framework. This is particularly important in the development of integrated care systems that is currently being driven by Longterm Plan for the NHS in England.

The Department of Health now the Department of Health and Social Care and the Royal College of General Practitioners has published good practice guidelines on the development and maintenance of electronic records for general practice. Key responsibilities of the Caldicott Guardian include the

following. Be a member of the organisation's Information Governance Group. Act as the organisation's "conscience". Confidentiality and Data Protection Knowledge of confidentiality and data protection matters. Seek external advice on these areas, where appropriate. Internal Information Processing Ensure that confidentiality issues are reflected in the organisation's policies and procedures including data protection, information security, Freedom of Information, records management and information quality. Information Sharing Overseeing flows of patientidentifiable information to and from partner organisations IT systems across health and social care disclosure to research interests disclosure to the police. NHS and Social Care Caldicott Guardians in England are required to be registered on the publicly available National Register of Caldicott Guardians, which can be downloaded from the NHS Digital website. In 2002 the recommendation was extended to social care councils with social services responsibilities in England are required to appoint Caldicott Guardians. There is no requirement, however, for social care services in Wales and Scotland to adopt the Caldicott principles although it would be good practice for them to do so. The Caldicott principles and the appointment of Caldicott Guardians therefore apply to NHS organisations in England, Wales and Scotland and councils with social services responsibilities in England. The situation is different in Northern Ireland where health and social care come under the same umbrella and the Caldicott report did not consider these specific circumstances.

The Caldicott recommendations are not binding to Northern Ireland, although the principles are regarded as best practice. Health and social care organisations in this country, however, are expected to comply with the law with respect to the Data Protection Act 2018 and Access to Health Records Northern Ireland Order 1993. Caldicott Guardians in Northern Ireland are referred to as Personal Data Guardians. The UK Caldicott Guardian Council, which is formed from elected Caldicott Guardian members across the UK, was established in 2005. Its main role is to facilitate sharing of confidentiality good practice. In 2006, a manual for Caldicott Guardians was published to provide guidance on this role within an organisation. Since then further guidance has been published with separate documents for England, Wales and Scotland to reflect updates in practice and legislation in the different countries. This guidance is reviewed and updated regularly as required. Patient Confidentiality A duty of confidence arises when a person provides information to another in situations where they expect that the information will be held in confidence, eg between a doctor and a patient. Patients disclose sensitive information relating to their health when seeking treatment. This is done in confidence and the expectation is that staff will respect their privacy and act appropriately. This is embedded in case law, in the professional codes of conduct for health care professionals and is a requirement for an NHS contract of employment, the breaching of which leads to disciplinary measures. The main consequence of this is that patientidentifiable information cannot be disclosed to a third party without the consent of the person concerned.

This means it is important that patients are made aware of the circumstances that must take place in order for high quality care to be provided, eg clinical audit and the sharing of information between members of the care team and between different organisations that are involved in healthcare provision. Patient information is also used for purposes that provide benefit to society rather than directly to patients themselves, eg medical research, public health, financial audit and health service management. However, it is not appropriate to assume that patients will be content to have their information to be used in these ways. In these circumstances it is important to obtain the consent of patients involved. Patients, in general, have the right to refuse the disclosure of their information to third parties and should be made aware of this right. If disclosure is extended to other health professionals involved in providing a patient's care then that care may be limited. In these circumstances patients need to be informed of the consequence of that decision and the possible limitations of their treatment. There are circumstances where the disclosure or use of patientidentifiable information without the consent of patients is justified. These include the following. Clinical audit, validation of patient records and research s.60 of the Health and Social

Care Act 2001 — the public good of using this information outweighs any issues of privacy. This is only applicable in England and Wales. Prevention of and supporting the detection, investigation and punishment of serious crime. Prevention of abuse or serious harm to others, eg child abuse. Where possible the issue of disclosure of information should be discussed with the individual concerned and consent obtained. If the individual refuses then they should be informed of the disclosure that has occurred against their wishes.

If, however, informing the individual will help them evade investigation into serious criminal activities or provoke a violent response this course of action will not be possible. Each case should be considered on its merits and specialist advice may need to be sought, eg from professional, regulatory or indemnifying bodies, as to the best course of action. The General Medical Council has published further guidance on disclosure of information to third parties clarifying the situation with regard to specific circumstances. These include reporting to the Driver and Vehicle Licensing Agency DVLA about concerns with respect to fitness to drive disclosing patient information for financial and administrative purposes reporting gunshot and knife wounds to the police reporting serious communicable diseases disclosing patient information for insurance, employment and other similar purposes disclosing information for education and training purposes responding to criticism in the media. Security of patient information is enshrined in the NHS Constitution. The NHS Care Record Guarantee for England has identified 12 commitments to respect patient rights to privacy and confidentiality while promoting health and wellbeing.

These commitments cover access to the patient's own medical records rules governing the sharing of medical records circumstances under which patient identifiable information can be shared who can make decisions about sharing patient information with other agencies requesting permission to share patient information with other agencies limiting the amount of patient information that can be shared and the consequences of not doing so for future care and treatment dealing with complains and concerns ensuring that patient information held is accurate and correcting factual errors ensuring that staff who work in the NHS are clear about their responsibilities with regard to patient confidentiality through contracts and training ensuring that both paper and electronic patient records are kept securely keeping a record of anyone who has accessed patient records the investigation of circumstances under which patient records have been viewed inappropriately. In general, the process for the management and use of patientidentifiable information is to do the following. Protect — look after the patient's information, ie protect the information from unwarranted disclosures. Inform — record holders must ensure that patients are made aware of how their information is used. Provide choice — ensure that patients have the choice of allowing how their personal information is used or disclosed. Give them the option of giving or withholding their consent. All staff need to be aware of their obligations for maintaining patient confidentiality and this should be set out in their terms of employment. NHS Digital guidance NHS Digital has an easy to follow guide for all health and social care professionals, to help them manage and use personal information appropriately. The guidance is encapsulated in five rules. Patients' or service users' personal information should be used respectfully and confidentially.

Confidential information should be shared among care team members when it is necessary to ensure the safe and effective care of an individual. Information shared for the benefit of the community should be made anonymous. An individual has a right to object to their personal information being shared. This should be respected by all concerned. In order to ensure that the confidentially rules are followed, organisations should develop relevant policies, systems and procedures for this to take place. Supporting the guide to frontline staff, the NHS Digital has also published a Code of Practice on Confidential Information to enable those responsible for developing and implementing policy in organisations. This covers the use of confidential information relating to the development, provision and monitoring of health services and adult social care. Information Governance Information

Governance IG is a component of the Integrated Governance framework published by England's the then Department of Health in 2006. It has four key elements. Information Governance Management. Confidentiality and Data Protection Assurance. Information Security Assurance. Information Quality Assurance. The Caldicott Guardian is central to the Confidentiality and Data Protection Assurance function and has an important input to the other three areas. Organisations are required to have IG steering groups, a member of which, it is recommended, should be the Caldicott Guardian. In response to the high profile personal data losses in 2008, the Department of Health set up an Information Governance Assurance Programme which developed a strengthened Information Governance Assurance Framework. The Information Governance Toolkit provides much of the support to NHS and social care organisations, general practices and the independent sector in this area of work by providing background materials, guidance and an online tool for performance assessment and reporting.

The strengthened Information Governance Assurance Framework comprises more robust annual IG performance assessment standards mandatory IG training for all staff who handle personal data documenting IG performance through statements on Internal Control ensuring that IG assurance is part of the risk management process and is subject to annual, formal internal audits ensuring that there is independent assurance of IG performance through external audit IG performance is monitored and scrutinised by the National Information Governance Board for Health and Social Care. In addition, organisations should take account of the requirements of the Data Protection Act 2018 which include a legal obligation to report a data security breach significantly greater penalties for any possible breach of the General Data Protection Regulation. The Senior Information Risk Owner The role of the Senior Information Risk Owner SIRO was identified and mandated for the NHS and local authorities in England in 2008 recognising the need to have someone at Board level with a specific responsibility for information risk. Organisations are required to identify their information assets as part of the review of information risks when strategic goals are considered. Each information asset should be assigned to an Information Asset Owner IAO who should be a senior member of staff accountable to the SIRO. The SIRO role differs from that of the Caldicott Guardian in that the former is concerned with the risks to information systems generally, whereas for the latter the focus is on patient identifiable information. Both roles must remain separate, however both need to work together as information assets issues may overlap with patient identifiable information. Further Information Publications Its purpose is to protect, promote and maintain the health and safety of the public by ensuring proper standards in the practice of medicine.

The NHS Data Security and Protection Toolkit can be accessed through the NHS Digital website. The council provides advice on the roles and responsibilities of Caldicott Guardians. The Caldicott Committee's remit included all patientidentifiable information passing between organisations for purposes other than direct care, medical research, or where there was a statutory requirement for information. The aim was to ensure that patientidentifiable information was shared only for justified purposes and that only the minimum necessary information was shared in each case. The Committee also advised on where action to minimise risks of confidentiality would be desirable. Central to the recommendations was the appointment in each NHS organisation of a "Guardian" of personbased clinical information to oversee the arrangements for the use and sharing of clinical information.These include Primary Care Trusts should ensure that within every practice there is an Information Governance lead and provide support and guidance as required. If you are not a member, have a look at the information about the benefits of membership and how to subscribe. We help practice managers to get their practice compliant with regulation and to stay compliant. Handouts, Templates and other tools for decision making and recording decisions are provided. It will concentrate on the tasks the Data Protection Officer must disperse. It provides sound foundations for those seeking to expand their understanding of the Caldicott Guardian Role, and its

function within Information Governance, and inspiration as to how it can be implemented and developed in their own organisations. Handouts, Templates and other tools for decision making and recording decisions are provided. Through national updates, expert led extended interactive sessions and practical case studies the conference will support you to improve practice your service.

The conference will also look at the implications of data breaches and effective reporting and management of information governance serious incidents. The authenticity and reliability of records depends on them being created and handled in a properly managed and documented recordkeeping system. This policy defines a structure for NHS Fife to ensure adequate records are maintained and they are managed and controlled effectively. Health Records management is key to this, as it will ensure appropriate and accurate information is available as required This release may be provided by nominated representatives. This responsibility is established and defined by the law Public Records Scotland Act 1937 as amended. Furthermore as an employee of the NHS, any Health Records created by an employee are public records. All staff must ensure that they keep appropriate records of their work and manage those Health Records in keeping with this policy and with any guidance subsequently produced. The duty of confidence continues even after the death of the patient or after the employee or contractor has left the NHS. It is therefore essential staff within the organisation with responsibility for records management comply with the policy otherwise they may be subject to disciplinary procedures. Operational records are defined as information, created or received in the course of business, and captured in a readable form in any medium, providing evidence of the functions, activities and transactions. They include It applies to records in all formats, of all types and in all locations. In achieving this aim, all the NHS Scotland employees should fulfil statutory and other legal requirements, ensuring patient safety and safe custody and confidentiality of patient information at all times. They should be authentic, meaningful, authoritative, and adequate for their purpose and correctly reflect what was communicated, decided or done.

They should be unalterable and after an action has occurred nothing from the Health Record should be deleted or altered. Information added to an existing hard copy Health Record should be signed and dated. Health Records systems should be secure and their creation, management, storage, transport and disposal should comply with current legislation. The minimum patient demographic data should include surname, forename, sex, date of birth, home address, postcode, Community Health Index CHI number and departmental number. Where there is more than one local identifier or case record per patient, a system should be in place to ensure that the existence of all other Health Records is known at all times. There should be no inside pockets or flaps as these can lead to misfiling or loss of documents. Clear instructions regarding the order of filing should be contained within the folder or printed on the dividers. Documents should be viewable in chronological order reflecting the continuum of patient care. All electronic Health Record information systems are password protected and passwords are changed at regular intervals. Health Records should not be accessible to unauthorised persons nor left for any period where they might be accessed by unauthorised persons.The Health Records collection inventory demonstrates how this will be achieved. Transportation methods must be fit for purpose and in accordance with individual departmental procedures. There are various methods employed for both manual and electronic records. A comprehensive Health Record should be maintained for every patient. Each Health Records system should have well defined procedures for the ongoing management of the Health Record from initiation to final disposal in accordance with current legislation. Whenever possible, separate areas are maintained for current and noncurrent Health Records in use within the organisation. Tracer and tracking systems facilitate timeous retrieval of Health Records.

Closed volumes are suitably labelled. Documents are securely fastened within the folder. The method of destruction must ensure that confidentiality is maintained at all times. These should

monitor such things as Health Record availability, use of temporary folders and timescales for receipt of Health Records at wards following emergency admission. The Policy specifies the timescale for retention for all types of Health Records and media, the procedure for transfer between media. The Board will take actions as necessary to comply with legal and professional obligations such as The length of time for retaining Health Records will depend on the record type The local retention schedule will be reviewed every 3 years or earlier in the light of legislative or Scottish Government changes. Auditing Health Records policies and procedures will be done on a systematic basis. The audit will compare current operational practice against defined procedures. The audit cycle will include self assessment against the Information Governance Standards A summary of these standards are listed at Appendix 3. Appendix 4 This includes the creation, use, storage, security and confidentiality of Health Records. Appropriate training should be provided for all users of the Health Records systems to meet local and national standards. All new employees to the organisation will be given basic training as part of the organisation’s induction process. Additional training in the specifics of Health Records management will be provided where appropriate. Training is tailored to specific staff groups and functions including the following The procedure manual is a key management tool and should form the basis for all Health Record system specific training. Some features on this site will not function if you disallow cookies. We use this to improve your customer experience. We also place functional cookies on your device to allow certain parts of the site to work.