NHS
West Hampshire
Clinical Commissioning Group

INFORMATION GOVERNANCE STAFF HANDBOOK

Version 9.4 (March 2018)

CONTENTS

1. INTRODUCTION

1.1 This document is intended to support and assist you in meeting your obligations to good information governance and sets out some of the responsibilities and expectations you are required to demonstrate in your everyday working practices for West Hampshire Clinical Commissioning Group (CCG).

1.2 Information governance (IG) is the practice used by all organisations to ensure that information / data is efficiently managed and that appropriate policies, system processes and effective management accountability provides a robust governance framework for safeguarding information.

1.3 Information governance enables organisations to embed policies and processes to ensure that personal and sensitive information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully.

1.4 NHS organisations hold numerous amounts of personal confidential and sensitive information, and all staff should be able to provide assurance that the information governance standards are fully understood and incorporated within their working practices.

1.5 Personal, personal confidential and sensitive information / data can be contained within a variety of documents. For example:

- Health records
- Staff information
- Corporate information
- Commissioning information.

1.6 It is important for staff to be aware of what constitutes personal, personal confidential and sensitive information / data. Further details on types of information are available within the Data Security Awareness Level 1 e-learning package, which replaces the annual IG training provided through the IG Training Tool, which is available on https://nhsdigital.e-lfh.org.uk/.

2. LEGISLATION, REGULATIONS AND KEY SUPPORT ORGANISATIONS

2.1 Members of staff should be aware of the legislation surrounding information governance that stipulate how organisations should safeguard information, what processes are in place to use, secure and transfer information and also how patients and members of public have access to personal/business information. The organisation must comply with the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications
- Environmental Information Regulations
- INSPIRE Regulations.
- Health and Social Care Act 2012
- Common Law Duty of Confidentiality
- Access to Health Records Act 1990
- Human Rights Act 1998
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998

The organisation must also have regard to the following standards and Codes of Practices:

- International information security standard: ISO/IEC 27002: 2005
- Caldicott Principles
- Current performance standards (NHS Digital Information Governance Toolkit)
- Data Sharing – Data Protection Code of Practice – ICO
- Confidentiality: NHS Code of Practice – Confidentiality: NHS Code of Practice Publications – Inside Government – GOV>UK
- Confidentiality Supplementary Guidance – Confidentiality: NHS Code of Practice – supplementary guidance, public interest disclosures – Publications – Inside Government – GOV.UK
- Records Management Code of Practice for Health and Social Care 2016
- NHS Digital Code of Practice on Confidential Information
- Information Security NHS Code of Practice
- CCTV
- Privacy Notices Code of Practice - Data Protection - ICO
- Anonymisation

- Personal Information Online Code of Practice

2.2 The Information Commissioners Office (ICO) is the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. You can find out more about their work and guidance here: https://ico.org.uk/.

2.3 NHS Digital (previously the Health and Social Care Information Centre or HSCIC) is responsible for providing national information, IT services and data to clinicians, commissioners, patients and researchers from right across the health and care economy. You can find out more about their work here: https://digital.nhs.uk/

2.4 The Information Governance Alliance is the authoritative source of advice and guidance about the rules on using information in health and care. Set up in response to a request that there should be a single authoritative source of information and guidance for the health and care sector, the IGA has been established to bring together resources from member organisations to consolidate specialist knowledge, provide a single source of authoritative and credible guidance and to establish a national information governance network. You can find out more about their work here: http://systems.digital.nhs.uk/infogov/iga

2.5 The NHS South, Central and West Commissioning Support Unit (CSU) information governance team has, on behalf of the CCG, produced a suite of policies, processes and procedures, which are available on the CCG website.

2.6 Adherence to information governance principles ensures compliance with the law, best practice and embeds processes that help staff manage personal confidential data (PCD) and sensitive information appropriately. It must also be noted that embedding information governance processes enables patients and service users to have greater trust in the CCG and enables effective working across partner organisations.

3. INFORMATION GOVERNANCE STRUCTURE

3.1 CCG Chief Officer

The CCG chief officer has overall responsibility for information governance within the organisation. As chief officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Annual Governance Statement which the chief officer is required to sign annually.

3.2 CCG Senior Information Risk Owner (SIRO)

The senior information risk owner for the CCG is an executive board member with allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at board level. The SIRO must provide the chief officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The CSU information governance team will support the SIRO in fulfilling their role.

3.3 Caldicott Guardian

The Caldicott guardian is the person within the CCG with overall responsibility for protecting the confidentiality of PCD and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to feedback any information governance issues to the CCG Board and relevant committees. The CSU information governance team will support the Caldicott guardian in fulfilling this role.

3.4 NHS South, Central & West Commissioning Support Unit Information Governance Team

The CSU information governance team are responsible for ensuring that the information governance programme is implemented throughout the CCG. The team is also responsible for the completion and annual submission of the information governance toolkit requirements for the CCG. They will support the CCG in investigating IG incidents and serious incidents requiring investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols. They will also provide local IG training either face to face or by monitoring staff use of the IG Training Tool.

3.5 Information Asset Owners (IAO)

The SIRO is supported by IAOs. The role of IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO on the security and use of the assets. The CSU information governance team will support the IAOs in fulfilling their role.

3.6 Data Custodians/Information Asset Administrators (IAAs)

Data custodians/IAAs are also required to support the CCG SIRO and will work with the CSU information governance team to ensure that the Data Protection Act and Caldicott Principles are applied within working practices in their own areas of responsibility.

4. CALDICOTT AND DATA PROTECTION ACT PRINCIPLES

4.1 The Caldicott principles

4.1.1 Previous Caldicott reviews have made recommendations aimed at improving the way the NHS uses and protects confidential information. All NHS employees must be aware of the seven Caldicott principles which apply to both patient and staff data.

Principle 1:	Justify the purpose - why is the information needed?
Principle 2:	Don't use patient identifiable information unless absolutely necessary – can the task be carried out without identifiable information?
Principle 3:	Use the minimum necessary patient identifiable information – can the task be carried out with less information?
Principle 4:	Access to patient identifiable information should be restricted to required/relevant personnel.
Principle 5:	Everyone with access to patient identifiable information should be aware of their responsibilities – lack of knowledge is not acceptable
Principle 6:	Understand and comply with the law.
Principle 7:	The duty to share information can be as important as the duty to protect patient confidentiality.

4.1.2 For further information on the Caldicott Reviews undertaken previously, please use the following links:

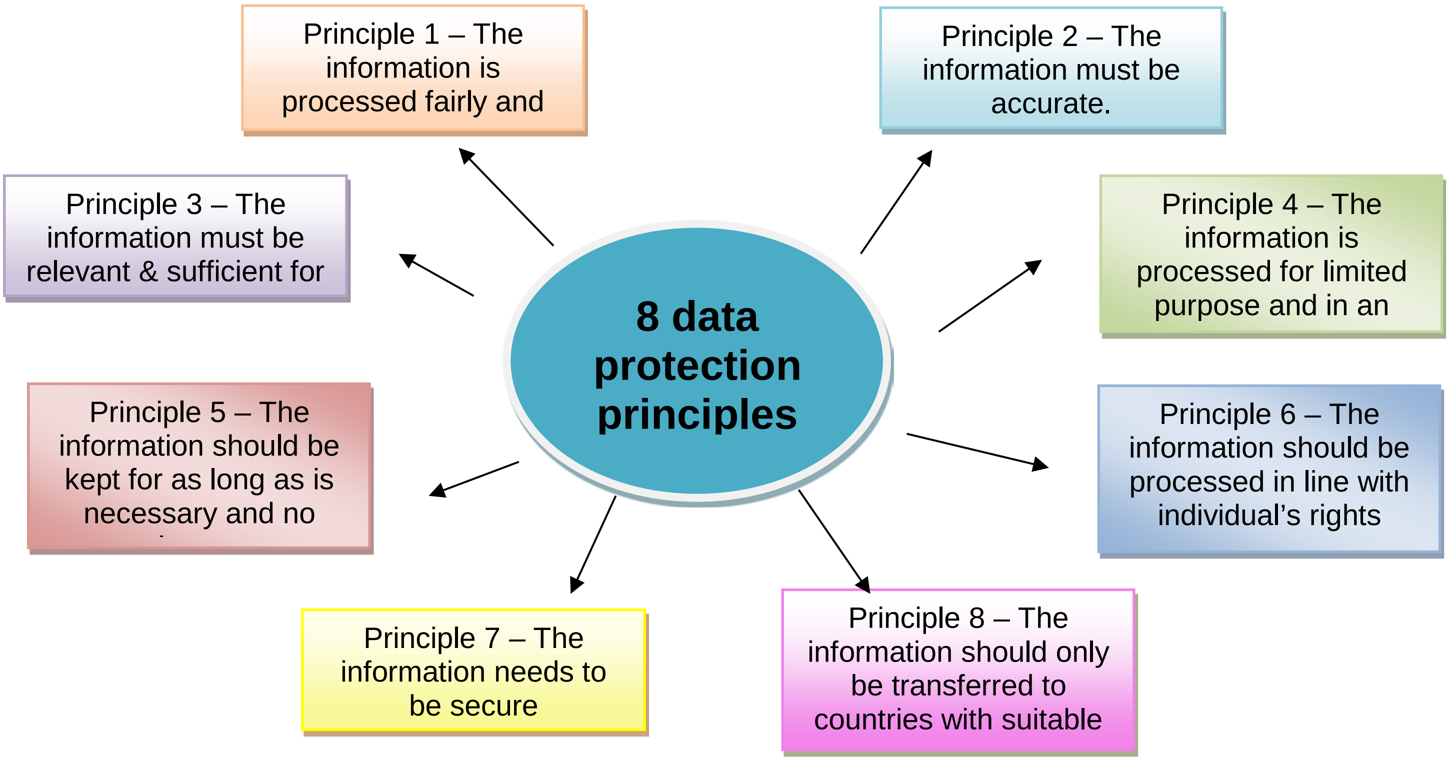
Caldicott 1
http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

Caldicott 2
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Caldicott 3
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

4.2 Data Protection Act 1998 and the Data Protection Act principles

4.2.1 All organisations in the country must comply with the Data Protection Act 1998. Data protection law is enforced in the UK by the Information Commissioner's Office (ICO) and has the power to fine organisations up to £500,000 for data protection breaches. The following diagram displays are the eight Data Protection Act principles that must be followed when handling personal and sensitive information. These principles should be considered when handling both corporate and clinical records.



Principle 1 – The information is processed fairly and
Principle 2 – The information must be accurate.
Principle 3 – The information must be relevant & sufficient for
Principle 4 – The information is processed for limited purpose and in an
8 data protection principles
Principle 5 – The information should be kept for as long as is necessary and no
Principle 6 – The information should be processed in line with individual's rights
Principle 7 – The information needs to be secure
Principle 8 – The information should only be transferred to countries with suitable

4.2.2 These Data Protection and Caldicott principles translate into **key rules for all staff to follow:**

- Patients and staff should be fully informed about how their information may be used
- There are strict conditions under which personal, personal confidential and sensitive personal data may be disclosed
- Individuals have the right to see what information is held about them, and to have any errors corrected. They also have the right to request copies
- Identifiable information should be anonymised wherever and whenever possible
- The disclosure or sharing of personal data is permissible where exemptions apply
- Sharing of personal data between organisations can take place with appropriate authority and permissions
- Sometimes a judgement has to be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified
- Personal data should be kept secure and confidential at all times.

5. GENERAL DATA PROTECTION REGULATION (GDPR)

5.1 The General Data Protection Regulations (GDPR) comes into force in the UK on 25 May 2018 and is the new legal framework in the EU which includes new elements and significant enhancements to the UK Data Protection Act (DPA) 1998. The Regulations introduces a principle of ‘accountability’ and requires that organisations must demonstrate compliance. The financial penalties have been significantly increased from the current maximum fine of £500,000 to 20 million Euros or 4% of the organisations’ annual turnover, whichever is highest. The Regulations have increased individual rights’ introducing new concepts of ‘Data Portability’ and the ‘Right to Erasure’ (the ‘Right to be Forgotten’). A significant addition is the principle of ‘accountability’ and being able to provide evidence of compliance with the Regulations.

5.2 All information governance related policies and procedures will be reviewed towards the end of the 2017/18 financial year to incorporate information relating to GDPR in readiness for implementation in May 2018.

6. GUIDE TO CONFIDENTIALITY

6.1 Everyone working in or for the NHS has the responsibility to use personal, personal confidential and sensitive information in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This guide sets out the key principles and main ‘do’s and don’ts’ that everyone should follow to achieve this for both electronic and paper records.

6.2 **The common law of duty of confidentiality** requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

6.3 What is **Identifiable** data?

- Name
- Address
- Post code
- Date of birth
- NHS number

6.4 What is **Personal** data?

As per the Data Protection Act 1998 and defined by the ICO; personal data means data which related to a living individual who can be identified:

a) From that data, or

b) From that data and other information which is in the possession of, or is likely to come into the possession, of the data controller, and includes any expression or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

6.5 What is **Personal Confidential** data (PCD)?

6.5.1 This is a term used in the 2nd Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people.

6.5.2 The review interpreted ‘personal’ as including the Data Protection Act definition of personal data, but included data relating to the deceased as well as living people, and ‘confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’ and is adapted to include ‘sensitive’ as defined in the Data Protection Act.

6.6 What is **Sensitive Personal** data?

6.6.1 Sensitive personal data is different from Personal Data. Sensitive personal data means personal data consisting of information as to:

a) The racial or ethnic origin of the data subject

b) Their political opinions

c) Their religious beliefs or other beliefs of a similar nature

d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)

e) Their physical or mental health or condition

f) Their sexual life

g) The commission or alleged commission of any offence or

h) Any proceedings for any offence committed or alleged to have been commited, the disposal of such proceedings or the sentence of any court in such proceedings.

6.6.2 Under **current legislation** commissioners can only process or have access to personal confidential data if:

- Consent has been obtained from the individual or
- The data has been anonymised or
- The data is in respect of safety, safeguarding or in the public interest. Any decision taken to share personal confidential data as a result of the above should be documented and agreed by the SIRO and Caldicott guardian.

6.6.3 Staff should check with the CSU IG lead if they have any queries on whether to access or process personal confidential data.

6.7 **Some of the ways to keep information secure and confidential ar**e:

6.7.1 **Organisational arrangements**
Make sure you know the name of the following (you will find it on your IG structure):

The SIRO	The CSU IG manager
The Caldicott guardian	Your departmental data custodian/IAA
Your IAO	

6.7.2 Limiting unnecessary access to personal information

- Do not discuss confidential matters outside of work, or even with anyone at work who does not need to know it; be aware that other people may overhear
- Do not leave working papers lying around the office, or put confidential items exposed in in-trays; remove documents from photocopiers and fax machines as soon as possible after use
- Hold keys and other access means, such as combination of locks, securely away from the point of storage when not in use. Ensure that there is an appropriately secure system in place to allow access in event of emergency or an individual's absence
- Keep offices locked when unoccupied, and maintain overall building security
- Keep workstations and other computer equipment secure, being particularly careful with laptops when not in use, especially not leaving them unattended in cars
- Lock away portable devices
- Do not write down your computer passwords or share them with anyone
- Ensure that your PC monitor screen cannot be seen by other people, being careful in public reception areas. Security screens should be used where needed.
- Do not leave your PC unattended whilst it is logged-in to the network or any system. Lock your screen every time you leave your desk

6.7.3 **Ensuring authorised access only**

- Access to records will be on a 'need to know' basis only

6.7.4 **Accuracy, retention and disposal**

- If adding information to records, ensure accuracy and relevance; any queries should be raised with the information asset owner
- If you are an information asset owner ensure that records are held with informed consent, are relevant for the purpose held, and are kept accurate and up–to–date; ensure that records are archived yearly and held no longer than necessary for their purpose and in

accordance with the Records Management Code of Practice for Health and Social Care 2016: http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

- Ensure any personal or sensitive information is confidentially destroyed in accordance with the CSU ICT information security policy (adopted by the CCG); note that ordinary waste bins and ‘recycling’ bins are not to be used for papers showing personal or otherwise confidential details
- Dispose of redundant equipment, especially disc or tape copies of confidential or sensitive information, in the proper manner through the CCG’s ICT provider.

6.7.5 Off-site working

- Do not take records or other confidential information out of the office and especially off-site unless authorised
- If you are authorised to take information off site always make sure that a list of the records that you take off site is retained at your base
- Protect the security and confidentiality of the information at all times. If records are taken off-site by agreement, they should be transported out of sight in the boot of the car and removed to a place of safety on arrival at your destination.

6.7.6 Requests for information

If you receive a request for information about a patient, staff member and it is not usually part of your job to respond, refer to the Subject Access Request section below:

6.7.7 Abuse of privilege

- Do not pass any information to your own relatives or friends, and do not attempt to find out details about them
- Do not pass on any information for personal or commercial gain.
- Do not attempt to access your own records unless through the appropriate procedure

6.7.8 Disclosures

You may, as part of your job, need to disclose patient information to others:

- Keep the amount of information disclosed (even within the NHS) to the minimum necessary
- Do not duplicate records, (on paper, or in a computer) unless absolutely essential for the purpose
- Ensure that confidential information is only disclosed to a non – NHS organisation, such as social services, in accordance with an agreed information sharing protocol (ISP) or similar agreement; if in doubt, refer to the CSU information governance team

6.7.9 Patient contacts and patient details

- Do not leave messages that contain personal, confidential or sensitive information on home answering machines as it may not be the person for whom the message is intended for
- White boards or other displays that contain personal or confidential information should not be visible to the public
- Any notes containing personal data written whilst taking a phone call or other message should be confidentially destroyed

6.8 Transferring personal confidential data or sensitive information

The ICO regularly reports on a number of unsecure transfers of information via fax, post and emails and has imposed monetary penalties on organisations who have failed to comply with the Data Protection Act. In order to prevent this occurring within the CCG, it is the responsibility of each individual member of staff to ensure that the following processes are followed when transferring personal identifiable and sensitive information.

6.9 NHSmail process

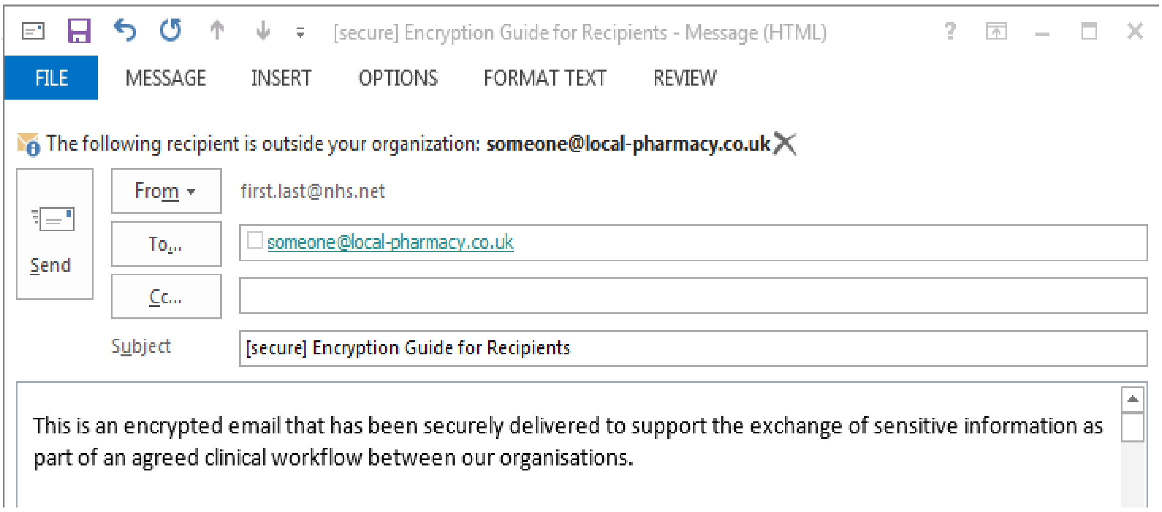
6.9.1 It is policy that emails containing any PCD or commercially sensitive information should be sent using an NHS.net account. Therefore, if you're emailing from your @nhs.net account to another @nhs.net account, then you can be confident that the content of your message is encrypted and secure.

6.9.2 Guidance for sending emails to non-secure domains.

Please be aware that the Local authority email domain (gcsx.gov.uk) is in the process of being retired so NHS Digital have made some changes on NHSmail from 1st April 2017.

As a result there has been a change in the way that NHSmail sends emails with sensitive data to other email systems. When sending emails with sensitive data outside of NHSmail you must use [secure] in the subject line of your email (the word secure must be in square brackets as in screenshot below), [secure] is not case sensitive. The Encryption Guide for NHSmail must be followed to ensure you understand all guidance and instructions on using this feature.

Example screen shot below:



The following recipient is outside your organization: **someone@local-pharmacy.co.uk**

From: first.last@nhs.net

To...: someone@local-pharmacy.co.uk

Cc...:

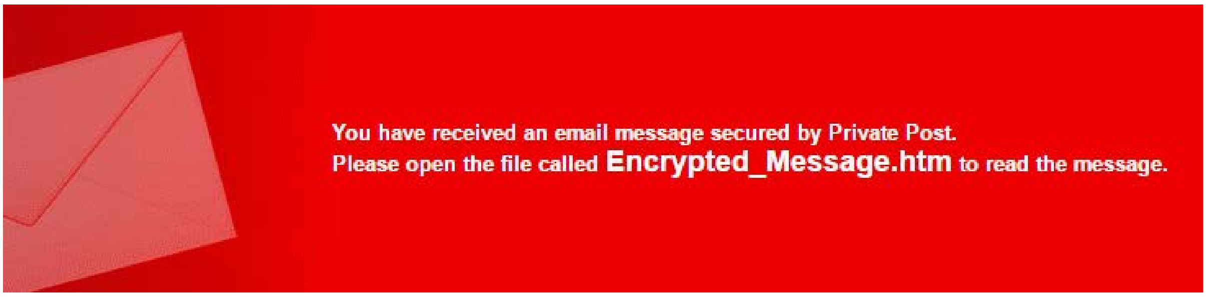
Subject: [secure] Encryption Guide for Recipients

This is an encrypted email that has been securely delivered to support the exchange of sensitive information as part of an agreed clinical workflow between our organisations.

Guidance for Accessing Encrypted Emails

An encrypted email sent from an NHSmail address (ending @nhs.net) will contain a link to access the encrypted message. The message reads:

PRIVATE AND CONFIDENTIAL
You have received an email message secured by Private Post. Please open the file called Encrypted_Message.htm to read the message.



You have received an email message secured by Private Post.
Please open the file called **Encrypted_Message.htm** to read the message.

(example of an encrypted NHSmail in Gmail)

The NHSmail Accessing Encrypted Emails Guide must be followed to ensure the recipient follows the registration process in order that they are set up with an account with the NHSmail encryption provider. The Guide also provides advice on replying and forwarding encrypted emails.

The NHSmail portal (https://portal.nhs.net), NHSmail Support Site will provide you with information and guidance on sending and receiving emails outside the NHSmail service – please refer to the Sharing Sensitive Information Guidance.

As a user of the NHSmail platform you must operate in accordance to the published guidance, policies and procedures to ensure you are using NHSmail effectively, appropriately and safely. Please refer to the materials below to ensure you are adhering to NHSmail guidance:

- NHSmail Acceptable Use Policy (AUP)
- Information Management Polices
- Sharing Sensitive Information Guidance

- Encryption Guide for NHSmail
- Accessing Encrypted Emails Guide
- Encryption Guide for Senders

6.10 Email guidance

- Do not put personal or sensitive information in the subject header of an email
- Check what you are ‘forwarding’ or sending when using the ‘reply all’ option in case the information is not intended for further sharing
- Ensure that any attachments do not include information that should not be shared such as hidden tabs of patient names or identifiers
- Make sure you select the correct recipient from the address book
- Remember that any email you send that contains information about an identifiable individual could be disclosed under the right of Subject Access (see below)
- Good management of emails and folders is essential
- Sending CCG information to private or personal email accounts should be avoided
- Do not use the ‘cc’ option, only send to those who need the information and not ‘just in case’
- Think very carefully about using the ‘Bcc’ option; it is appropriate for protecting the anonymity of recipients but not in every situation.

6.11 Safe haven fax process

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so or when an alternative secure method is not available. The following rules must apply:

- Ensure it is sited in an area that is restricted to those who need to access the information
- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it
- The sender is certain that the correct person will receive it and that the fax number is correct
- Telephone the recipient when you are sending the fax and ask them to return the call to acknowledge receipt and number of pages.
- The confirmation of receipt should be checked to ensure the fax has been transmitted to the intended recipient, where possible the receipt should be attached to the original document
- Confidential faxes must not be left lying around for unauthorised staff to see
- Only the minimum amount of personal information should be sent

- All confidential faxes sent should be clearly marked ‘private and confidential’ on the front sheet
- Frequently used numbers should be programmed into the fax machine ‘memory dial’ facility; this will minimise the risk of dialling incorrect numbers
- If you receive a call requesting that confidential information be sent via fax always call the requestor back to confirm the caller’s identity using an independent number source. Make every attempt to find a more secure way of sending the information first
- Always seek advice if you are unsure whether or not to send any information via fax
- If it is highly sensitive ensure someone is at the receiving end waiting for it
- If you receive faxes that contain personal information store them in a secure environment
- Fax machines should be turned off out of hours.

6.12 Safe haven post process

6.12.1 It is recommended that staff members follow these guidelines:

- Some examples of documents that may need added protection when sending in the post are:
  - Birth certificates
  - Driving licences
  - Marriage certificates
  - Passports
  - Bank statements and other financial information
  - Patient information
- All incoming mail should be opened away from public areas. Outgoing mail (both internal and external) should be sealed securely and marked ‘private and confidential’ if it contains person-identifiable or sensitive information
- Ensure post is sent to a named person and clearly addressed
- A return address should be shown on all post
- Staff sending documents by external post or courier, use a ‘signed for’ delivery service. PCD should be sent by Special Delivery. Use appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the address is typed or written clearly in indelible ink
- Double envelope the documents for added security
- Include a return to sender address on the back of the envelope
- Confirm receipt with the intended recipient as soon as possible
- When staff are sending mail outside of the NHS, send documents only to known, named, authorised personnel marked ‘confidential’

- Consider carrying out a risk assessment if appropriate

6.12.2 The ICO has issued further guidance regarding the potential for identity theft which can be found at https://ico.org.uk/for-the-public/identity-theft

6.12.3 The National Fraud and Cyber Crime Reporting Centre has also issued guidance which can be found at http://www.actionfraud.police.uk/fraud_protection/identity_fraud

7. SUBJECT ACCESS REQUESTS

7.1 Under the Data Protection Act 1998, all living individuals or 'data subjects' have a right to be informed of the following:

- If the CCG holds, stores or processes personal data about them
- A description of the personal data held, the purposes for which it is processed and to whom the personal data may be disclosed
- A copy of any information held
- To be informed as to the source of the data held.

7.2 Support will be given by the data custodians to ensure all requests are responded to in line with the 40 day legislative timescale (although a 21 day deadline has been set by the NHS. The CCG Subject Access Request Guidance should be used as the agreed procedures and each request should receive prompt attention. Staff should notify their data custodian / information asset administrator immediately on receipt of a subject access request.

7.3 All staff have a responsibility to ensure they support the data custodians with the subject access request process for the CCG.

7.4 Your personal information can only be obtained through the subject access request process. If you access your personal information through systems used within the CCG, disciplinary action will be taken.

8. REPORTING POSSIBLE BREACHES OF SECURITY OR CONFIDENTIALITY

8.1 Each member of staff has the responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way. Members of staff should always:

- Report any incident that could possible relate to a breach of confidentiality, for example the loss, theft or corruption of information, a network security breach, loss or theft of a computer, password misuse etc to their data custodian / information asset administrator
- Think carefully before sharing PCD without explicit consent, as staff may be held accountable for any unauthorised disclosure.

- Do not open any suspicious emails. Report any possible cyber security incidents to the CSU IT service desk immediately.

8.2 If in any doubt, ask your data custodian / information asset administrator, your line manager or the CSU information governance team who may pass the query to the CCG's SIRO or Caldicott guardian.

Monitoring access to personal identifiable and sensitive information

8.3 Staff members should be aware that electronic systems that access, process or transfer PCD are monitored on a continuous basis. Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with the CCG's disciplinary procedures. In addition, unauthorised disclosure of personal information is an offence and could lead to prosecution of individuals and / or the organisation.

8.4 The Information Commissioner's Office (ICO) is able to issue monetary penalties to any organisation found to be in breach of the Data Protection Act. A fine of up to £500,000 may be incurred for a serious breach. The ICO can also conduct an investigation into less serious breaches which can lead to an organisation having an enforcement notice/undertaking imposed upon them.

8.5 The ICO may impose the monetary penalty notice if the organisation has seriously breached the Data Protection Act principles and the breach is:

- Likely to have caused substantial damage or distress
- Deliberate or the organisation must have known or ought to have known that there was a risk that a breach would occur and failed to take reasonable steps to prevent it.

9. IT SECURITY

9.1 Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the CCG, therefore the organisation must ensure that the information is properly protected and is reliably available. The organisation must ensure that:

- Access to all CCG confidential or sensitive information whether held on paper or electronically must be restricted
- That doors and windows are closed properly, blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team or it is suspected that someone else knows the code
- All employees wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access.
- Visitors are met at reception points and accompanied to appropriate members of staff or meetings and also should be asked to sign in and out of the building

- Employees on termination of employment or contract must surrender all relevant CCG equipment including IG cards
- All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset.

9.2 All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. The organisation will investigate all suspected and actual security breaches.

9.3 Remote working and portable devices

9.3.1 The developments with information technology have enabled staff to adapt to more flexible and effective working practices, by providing mobile computing and portable devices. Although these working practices are advantageous, it is important for all staff to understand the associated risks to the information, and the responsibility to ensure that information accessed remotely or held on portable devices, is protected by adequate security.

9.3.2 It is important for staff to protect information which is processed remotely or is stored on portable devices and staff should read relevant CCG policies to ensure good practice.

9.3.3 Staff are responsible for the security of any portable devices issued to them, and should take all necessary precautions to avoid loss, theft or damage. In the event of loss, damage or theft occurring, they must report this immediately to their line manager who can gain support from the CSU Information Governance Team. Any loss should be reported through the CCG risk management process.

9.4 Remote working and portable devices best practice guidance

- Encryption is mandatory in all mobile devices used to store CCG information.
- Any portable computing device must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, ensure that it is safely stored out of sight.
- Staff should take extra vigilance if using any portable computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the organisation’s stored information by a third party “overlooking”. There are security measures which can be deployed to support this if such travel is common to the role, staff should enquire through their line managers.
- Staff should not leave the device unattended for any reason unless the session is “locked” and it is in a safe working place, devices should not be left in an unattended publically accessible room for example. If possible staff should take the device with them.
- Ensure that other ‘non’ authorised users are not given access to the device or the data it contains.

9.5 Passwords and pin codes

- Passwords should be a combination of letters and digits of a pre-determined length and combination of characters, typically using the lower case of the keyboard
- Passwords and/or PINs should not normally be written down, but if unavoidable should be held on your secure drive in a passwords folder, and never kept with the device or in an easily recognised form
- Regular password changes reduce the risk of unauthorised access to the machine and therefore passwords should be changed at least every 60 days, but more frequently if required.

9.6 USB/portable computing devices

- Sensitive corporate information and PCD must not be stored or transferred using any unencrypted “USB memory” device
- Where it is not possible to encrypt sensitive/personal information, the advice of the CSU information governance team should be sought and, a one off data transfer solution should be found using a secure method
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available
- Information should not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible.
- Staff must ensure that any suspected or actual breaches of security are reported to their line manager or the CSU information governance team
- Staff must ensure that the mobile devices are used appropriately at all times
- Staff should not under any circumstances use any mobile device whilst in control of a vehicle
- All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information

10. INFORMATION GOVERNANCE MANDATORY TRAINING

10.1 Every individual who works for the organisation is required to complete mandatory annual information governance training. This includes all new starters, existing and temporary members of staff, and contractors. The CCG has a responsibility to ensure that those working with its information are aware of the IG principles and the risks to the reputation of our CCG which may occur, if processes are not followed.

10.2 All new staff are required to complete the Data Security Awareness Level 1 e-learning package provided by NHS Digital via https://nhsdigital.e-lfh.org.uk/. Existing staff must complete IG refresher training annually either through face to face training delivered by the IG team or by completing the Data Security Awareness Level 1 e-learning package provided by NHS Digital. Training must be completed by the deadline set by the CCGs SIRO and Caldicott Guardian at the start of the financial year.

10.3 The CSU information governance team in discussion with the CCG have conducted a training needs analysis and identified IG training which will need to be completed by those within different job roles and functions.

10.4 New starters, temporary members of staff/contractors and general queries regarding training, please contact a member of the CSU information governance team via Scwcsu.igenquiries@nhs.net.

11. RECORDS MANAGEMENT

11.1 Records management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal. It is a requirement of the Data Protection Act to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

11.2 Records management is crucial to all NHS organisations. If records are not managed effectively, the organisation would not be able to function as required and expected, and to account for what has happened in the past or to make decisions about the future. Records are a fundamental corporate asset and are required to provide evidence of actions and decisions, enable the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the Data Protection Act 1998 and the Freedom of Information Act 2000.

11.3 The NHS has two categories of records; health and corporate.

11.3.1 Health records can be considered records which contain the following:

- All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, and so on).

11.3.2 Corporate records can be considered records which contain the following:

- All administrative records (for example. personnel, estates, financial and accounting records, notes associated with complaints).

11.4 Corporate records support strategic decision making and enable the organisation to protect the interests of staff, patients, public and other stakeholders. Corporate records should:

- Be accurate and complete
- Be arranged systematically
- Be sufficient to enable other member sof staff to carry out their tasks
- Demonstrate compliance with legal and regulatory requirements.

11.5 Corporate records can be considered records which contain the following:

- All administrative records (such as personnel, estates, financial and accounting records, notes associated with complaints

11.6 Records within the NHS can be held in paper (manual) or electronic form and all NHS organisations have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Records Guarantee under the National Care Record service.

11.7 **Paper (manual) records**

- A uniform filing system should be implemented to ensure that documents are grouped appropriately and consistently. Records that are frequently used should be stored within secure filing cabinets or secure areas (locked rooms, coded areas). Infrequently used records should be archived in secure rooms. If records are no longer needed and do not need to be kept according to the retention timeframes, the records should be confidentially destroyed
- The filing system should:
    - o Be kept simple and easy for all to understand.
    - o Be discussed with line management to determine whether records are to be kept manually or electronically and which is the definitive version.
    - o Be labeled accurately and clearly, labels should be brief, have a meaningful description of the contents, and be intelligible to both current and future members of staff
    - o Be reviewed at the end of every financial year. This will identify if records need to be retained, archived or destroyed. A tracker card or spreadsheet to include who uses the file, location of where the file is situated and also retention review date is good practice to keep.
- The records should:
    - o Be uniform where possible and where appropriate templates used
    - o Have version controls applied which are periodically reviewed
    - o Not contain PCD in the title of the record which should be kept in a secure location in your filing system
    - o Have their pages numbered as this will help confirm if pages have been removed or are missing
    - o Be restricted and only permission to access PCD granted to a limited number of staff who require it
    - o Be reviewed on a periodic basis to ensure that destruction and archiving rules apply
    - o Annual confidentiality audits will be carried out by the data custodian for each service and results shared with service leads

11.8 **Electronic records**

- The filing structure should:

  - Be named accurately, simply and be easy for all to understand.
  - Be created so that members of staff can follow the same filing structure
  - Be managed and it is recommended that 'creating or deleting folder responsibility' is restricted to a limited number of staff. This reduces the possibility of duplication, loss of information and more storage space being needed. Should a member of staff require a new folder to be created, they will need to be granted permission from the lead administrator
  - Be based on uniform technology which determines the naming conventions for files and folders.
- All records should:
  - Be named accurately, simply and be easy for all to understand
  - Be reviewed at the end of every financial year. This will identify if records need to be retained, deleted or archived
  - Have version controls applied and be periodically reviewed.
  - Be controlled with access granted through use of logins, password protection and encryption
  - Once a project is completed, all associated electronic documentation should be contained in a zipped file, accurately named / dated and stored within a secure folder on the organisations network. This will decrease storage space and keep all common documentation together.

12. WHAT TO DO IN THE EVENT OF MISSING CORPORATE OR HEALTH RECORDS

12.1 Missing records are a serious risk to the organisation and it is therefore vital that a tracing procedure is undertaken. Should records go 'missing' the following procedures should be followed:

1) Highlight the fact that a record is 'missing' to the IAO and work colleagues as soon as this becomes apparent.
2) Search in the place you would normally expect to see the record but look either side and above and below where it should be filed (should the record be manual). Search in other folders or conduct a 'search' within your files (should the record be electronic).
3) Should the record remain missing after your search, you will need to report the incident to your Information Asset Owner. They will decide if it needs to be reported to the CSU information governance team via the Emergency Management and Risk Manager as per the Incident Management Policy and Guidance.
4) Relevant staff should be made aware of the name of the record that is missing.
5) The CCG SIRO and Caldicott guardian should be informed of the loss by the CSU IG team and advised of the level of the information risk.
6) Consideration will then be given as to whether the loss needs to be reported to the Information Commissioner's Office.

12.2 Inform the IAO and CSU IG team if the notes have been located.

12.3 Any queries relating to lost records should be directed to the CSU IG team via the Scwcsu.igenquiries@nhs.net mailbox.

13. FREEDOM OF INFORMATION

13.1 The Freedom of Information Act 2000 (FOIA) encourages transparency within the public sector and assumes that openness is standard so that, for example, decisions on how public money is spent or services provided can be seen and understood.

13.2 Identifying an FOI request

13.2.1 Any member of the public can ask to see information that is held by the CCG and any member of staff may be approached and asked for information under the FOIA.

13.2.2 The law requires the CCG to respond **within 20 working days** of receipt and staff need, therefore, to be alert to any requests received to ensure they are processed promptly and appropriately.

13.2.3 The FOIA gives a right of access to information and does not require justification or the reason behind the request to be provided by the requestor.

ALL staff have a duty to:

13.3 **Recognise requests made under FOI**; enquirers do not have to mention the term FOIA so consider this if the request **does not** fall into one of the following categories:

- A solicitor’s letter
- A complaint
- A request for access to personal records
- A press enquiry
- Research
- A routine enquiry which can be responded to as “business as usual” such as advice, leaflets, contact details.

13.4 **Provide help and advice to applicants:**

- Direct all requests to the FOI lead for action
- Advise applicants that the request must be written (email is acceptable) and includes a name and contact address; help them put their request in writing if necessary
- Direct requesters to the online CCG publication scheme if it is known the information requested can be sourced there

- Advise there are a number of exemptions within the FOIA under which the CCG may not be obliged to provide the information requested
- Advise that a fee may be applicable, depending on the type and size of the request.

13.5 Requests for information you may hold:

13.5.1 The CCG, its staff and hosted organisations are obliged to respond to requests; failure to comply with the FOIA has legal implications not only for the CCG but for each individual member of staff. More detailed advice is held in the CCG FOI policy, 'procedure for handling FOI enquiries'.

13.5.2 Under the FOIA all types of recorded information can be requested and may be disclosed, including everything written in notebooks or on "Post It" notes as well as your formal paper and electronic records. Very little information is "exempt" – this is only applicable where the public interest is best served by non-disclosure

13.5.3 For all FOI questions and queries please email the CSU scwcsu.westhampshireccg@nhs.net mailbox**.**

14. NEW OR EXISTING PROGRAMMES AND PROJECTS

14.1 It is the responsibility of all staff to incorporate information governance into their working practices and to also make partner organisations provide assurance that information will be handled in a secure and appropriate manner. As part of the information governance framework, we ask staff to consider IG implications when starting new projects and programmes.

14.2 It is important to include your CSU information governance manager at programme and project initiation stage to advise of the IG elements which will need to be considered. A privacy impact assessment is a tool used by the CSU IG team to help establish IG implications at the start of a programme and project.

14.3 A Privacy Impact Assessment is a tool used by the CCG and recommended by the Information Commissioners Office to help establish and risk assess information governance implications / considerations at the start of a programme and / or project.

14.4 Identifying information governance elements at an early stage will ensure:

- The project / programme is based on a 'privacy by design' model
- Necessary information sharing agreements are in place
- The CCG is aware of and can effectively monitor data flows.

14.5 It will also eliminate the potential of failing to comply with the Data Protection Act 1998 and subsequent fines from the Information Commissioner's Officer. Once the privacy impact assessment has been completed, the document must be forwarded to the CSU IG team who will arrange for it to be considered at the fortnightly PIA Panel. Any identified recommendations will be fed back to the project / programme lead and when finalised the CCG and Caldicott guardian will approve it.

14.6 A PIA should be considered as a living document, should project or programme parameters change which could affect the original IG actions or recommendations made, then a review should be undertaken to ensure no additional risks are created. These can then be controlled and mitigated for as part of the ongoing project / programme.

15. BUSINESS CONTINUITY PLANS

15.1 Business continuity management is a method used to identify potential impacts that may threaten the operations of the CCG or the CCG itself. The fundamental element of business continuity is to ensure that whatever impacts on the CCG, the organisation continues to operate. Business continuity plans will help shape organisational resilience to ‘threats’, plan counteractions and minimise interruptions to the CCG activities from the effects of major failures or disruption to its information assets (such as data, data processing facilities and communications).

15.2 Each directorate has contributed to the WHCCG business continuity plan. It is the responsibility of members of staff to be aware of the location of this plan, and what procedures to follow in the event of potential ‘threats’ to the operation of the CCG.

15.3 For further information regarding business continuity plans, please contact the Emergency Management and Risk Manager.

16. INFORMATION SHARING

16.1 It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The CCG needs to ensure that mechanisms are in place to enable reliable and secure exchange of data as set out in relevant legislation.

16.2 Staff sharing PCD with other agencies should be aware of the requirement to have an information sharing agreement / operational agreement in place for the routine sharing of person identifiable information. This will provide the CCG with the assurance that these organisations are able to comply with the safe haven ethos and meet legislative and related guidance requirements.

16.3 Information sharing agreements / operational agreements should document:

- The purpose for the information to be shared/purpose of the agreement
- What information will be shared
- Who the information will be shared with
- Senior management/executive endorsement of the information sharing agreement and arrangements

- Structures of sharing information.
- Legislation and regulations which are required to be adhered to under the Data Protection Act 1998.

16.4 For further advice and guidance on information sharing agreements / operational agreements, please contact a member of the CSU IG Team.

16.5 Information sharing procedure

- Sharing of information can only be authorised either by the CCG Caldicott guarding or the CCG SIRO. A member of the information governance team can provide advice and guidance on this
- It is the responsibility of each staff member to manage the risks to security of information when it is shared
- Requests for sharing information outside of the organisation must be assessed against the Caldicott and Data Protection principles and approved by a member of the CSU IG team and the CCG's Caldicott guardian and SIRO.

16.6 For further advice and guidance, please contact the CSU IG team.

17. SMARTCARDS

17.1 Smartcards are required to use and access IT systems essential to healthcare provision. CCG staff need to use smartcards in order to gain access to patient information, for example, the Choose and Book service, the Electronic Prescription Service (EPS), Secondary Use Service (SUS), Summary Care Record (SCR) and Electronic Staff Record (ESR).

17.2 Individuals are granted access to a smartcard by their line manager based on their work and their level of involvement in patient care. The use of smartcards leaves an audit trail.

17.3 It is up to the registration authority (RA) sponsor to verify the identity of all healthcare staff requiring access to patient identifiable or sensitive data. Individuals will need to arrange to visit the RA sponsor based at Omega House (CCG Business Manager) or Fareham Civic Offices for Continuing Healthcare (CHC Senior Administrator) and will be required to provide photographic proof of identity with driving licence or passport. A proof of address in the form of two community bills will also be required.

17.4 Staff should be aware that disciplinary action may be taken if smartcards are shared or lost.

17.5 **Line manager responsibilities**

- To identify all roles within their area of responsibility which require access to the system and ensure that all employees, including temporary/ agency/bank and locum employees, are provided with appropriate access

- To ensure for all roles that involve access to the system that job descriptions and any recruitment materials make reference to the need to be registered and the role's responsibilities in relation to using the system
- To complete the standard form for Registration of a New User (Appendix A) and send to the CCG RA sponsor:

  Sponsor 1

  CCG Business Manager, Omega House, 112 Southampton Road, Eastleigh SO50 5PB

  Email: whccg.admin@nhs.net

  Sponsor 2

  Senior Administrator, Continuing Healthcare (CHC), West Hampshire CCG, 5th Floor, Civic Offices, Civic Way, Fareham, Hampshire PO16 7AZ

  Email: whccg.admin@nhs.net

- To ensure that all new starters within their area of responsibility, including agency/temporary employees, receive training in order to be able to access the system
- To ensure that all employees are aware of information governance policies, associated documentation and their responsibilities in relation to use of and access to the system
- To immediately inform the RA sponsor of any leavers, starters, staff changes (including changes to access rights) in relation to smartcard users.

17.6 Staff smartcard code of practice / user responsibilities

- Use your smartcard responsibly and in line with your access rights
- Immediately inform the CSU IG and RA sponsor should your smartcard be lost, stolen or misplaced
- Ensure that you report any misuse of the smartcards
- Ensure that you keep your smartcard and log-in details confidential; in particular you must not leave your PC logged in and you must not share or provide access to your smartcards or passwords
- Ensure that you accurately complete the necessary paperwork, provides suitable identification and attends any appropriate appointments in order to register on the system or have your smartcard updated/re-issued
- All members of staff using smartcards should follow the organisation's suite of information governance policies and procedures; adhere to the Data Protection and Caldicott Principles, and the Confidentiality Code of Practice and the Care Records Guarantee.
- Ensure that you return your smartcard if you leave the organisation and are not going to another NHS organisation.

17.7 Data Custodian / Information Asset Administrator Responsibilities (IAA)

- Data custodians / IAAs undertake to monitor appropriate smartcard usage (where applicable) by compliance audit checks, raising awareness of the importance of keeping cards secure, taking any remedial action advised by the IG manager and logging any necessary incidents. Where non-compliance is identified the head of information governance should be notified immediately.
- Data custodians should keep an up to date log of smartcards in use by their team / directorate as part of their team Information Asset Registers.
- A master list of CCG smartcard users is retained by Trudie Higby, CCG Business Manager. Kim Bryant, Senior Administrator, will keep a CHC register and this will feed into the CCG master register. Data custodians / IAAs should inform the RA sponsor if there are any changes to smartcard users within their teams.

17.8 Guidance on the process for management of smart cards can be found on the within the Registration Authority Policy on the CCG website.

18. INFORMATION GOVERNANCE STAFF HANDBOOK

18.1 Please ensure you sign the accompanying slip confirming you have read and understood the information provided and return to the CSU IG team.

18.2 Should you have any questions or queries regarding information governance, please do not hesitate to contact the CSU IG team:

Your CCG IG manager is:	Lucy Long Information Governance Manager
CSU IG Team Mailbox:	Scwcsu.igenquiries@nhs.net

19. EQUALITY AND DIVERSITY STATEMENT

19.1 NHS West Hampshire CCG is committed to equality of opportunity for all people and to eliminating unlawful discrimination, harassment and victimisation. In line with our commitment we have considered the equality impact of all information governance policies. Key impacts identified relate to fair implementation of all information governance policies, equalities monitoring and the confidentiality requirements defined in the Gender Recognition Act 2004. The handbook and associated policies have been amended to reduce any potential negative equality impacts. Refer to individual policies for guidance.

Health & Social Care Information Centre

Appendix A

CIS – Request Creation of New User (Sponsor Use Only)

- The information in this form must be entered in the Care Identity Service (CIS) in the event CIS is not being used to request the registration of a new Smartcard User.
- All mandatory fields must be completed to complete this process.

Please complete the following fields in BLOCK CAPITALS:

Applicant Details	**(Please complete all fields as fully as possible)**
Title (e.g. Dr, Mr, Mrs etc.):	
Given Name (Forename): (Mandatory)	
Middle Names:	
Family Name: (Mandatory)	
Preferred name:	
Previous family names:	
Applicant Contact Details	**(Please complete all fields as fully as possible)**
Telephone number:	
Mobile number:	
Email:	
Applicant Organisation	
Organisation name:	
Applicant Workplace Details	**(Please complete all fields as fully as possible)**
Workplace name:	
Workplace department:	
Workplace address: (Including Postcode)	

Sponsor's declaration (To be entered in the Notes field in CIS when entered by RA)

I confirm that the **Applicant** specified above should be issued a Smartcard.

Sponsor Name	
Sponsor UUID	
Date	

Once completed in full please email (or post) the completed form to your local Registration Authority.

NHS
West Hampshire
Clinical Commissioning Group

Information Governance Staff Handbook Confirmation Slip

I confirm that:

I have received my copy of the information governance staff handbook and I understand my responsibilities.

Name ……………………………………………………………………………………

Signature…………………………………………………………………………….

Job title……………………………………………………………………..…….

Workplace………………………………………………………………………….

Date…………………………………………………………………………..……..

Please return to:

Information Governance Team
NHS South, Central & West Commissioning Support Unit
Omega House
112 Southampton Road
Eastleigh
SO50 5BP

Scwcsu.igenquiries@nhs.net

West Hampshire CCG IG Staff Handbook v9.04 March 2018