South East Staffordshire and Seisdon Peninsular CCG

All Staff Information Governance Briefing

Introduction

To ensure compliance with legislation and to meet the CCGs corporate responsibilities we are required to adopt a range of information governance policies and procedures. This staff briefing has been developed to ensure you are aware of how to access these policies and some of your key responsibilities.

We have produced a high level IG Policy that details how the CCG will implement Information Governance. This includes the IG Management Framework and IG Improvement Plan.

We have developed an IG Handbook that covers all the IG Procedures required within the CCG.

These documents will be made available to you at the following links:

http://sesandspccg.nhs.uk/about/information-governance

Please make sure you familiarise yourself with the contents of this briefing note as well as the Policy and Handbook.

Key Responsibilities for IG within the CCG

All staff should be aware of who fulfils the key roles within the CCG.

Accountable Officer	**Rita Symons**
Senior Information Risk Owner (SIRO)	**Tim Tebbs**
Caldicott Guardian	**Heather Johnstone**
Information Governance Lead	**Rob Boland**

Support provided by Midlands & Lancashire Commissioning Support Unit IG Team:

Information Governance Support Officer	**William Hill**
Information Security Manager	**Emma Styles**
Information Governance Manager	**Hayley Gidman**

If you have any queries about this briefing or any other Information Governance issues, please contact your Information Governance Support Officer:

William Hill
william.hill@staffordshirecss.nhs.uk
07712302113

Communicating IG Responsibilities

As a CCG, we have a responsibility to ensure that everybody who works for us is aware of the expectations placed upon them regarding how they use the confidential information they come in to contact with as part of their work for the CCG. This may be information which identifies individuals, or which would be commercially sensitive and would be detrimental to the organisation if its confidentiality was breached.
Therefore, the CCG has put policies and procedures in place which cover all aspects of Information Governance and will provide you with guidance and direction on how we expect you to work with confidential information, and in doing so, ensure that you are compliant with all relevant legislation.

It is particularly important that every effort is made to follow this guidance as the Information Commissioner's Office (the body who regulate compliance with the Data Protection Act and Freedom of Information Act in England) has the power to fine organisations and individuals up to £500,000 if a serious enough breach of the Data Protection Act occurs.

In addition to this, at an organisational level, any breaches of these policies and procedures may result in disciplinary procedures.

However, it is really important that when you read and use the policies and procedures, if there is anything which after careful consideration is just not workable or is impractical for you to be able to implement, please let your IG Support Officer know.

If we aren't made aware of any issues, then we can't provide alternative solutions.

Use of Personal Information within the CCG

Where the CCG has access to person confidential data relating to patients, it should only be for the purpose of direct care or where explicit consent has been provided. This is the basic requirements of the Data Protection Act to ensure that the CCG is compliant with principle 1.

If the CCG wishes to use patient information for any other purpose, they must obtain explicit consent from each patient.

Information Security

The Information Security principles are detailed throughout the IG Handbook and set out the minimum requirements for using, communicating and managing information within the organisation. These procedures are applicable to all staff within the CCG, including temporary staff and contractors.

These procedures provide the processes which support the framework set out within the Information Governance Policy and need to be read, understood and adhered to.

This procedure, correctly adhered to, will achieve a comprehensive and consistent approach to the secure management of information throughout the organisation, ensure continuous business

capability and minimise the likelihood of occurrence and the impacts of any information security incidents.

The CCG needs robust information security management arrangements for the protection of personal and confidential information to meet the statutory requirements set out within the Data Protection Act 1998.

The Information Security Procedures cover a range of issues including:

- Network Access
- Storage of Information
- Password Management
- Smartcard Security
- Software and Equipment
- Use of Portable Equipment
- Clear Screen & Clear Desk Procedure
- Internet, Intranet and Email
- Safe Haven Procedures
- Sending Person Identifiable Information outside the Organisation
- Acceptable Use of Social Media & Social Networks
- Mobile or Home Working
- Information Governance Incident Reporting
- Temporary Staff Confidentiality & Compliance

Confidentiality and Data Protection

Much of our work involves us, in one way or another having access to confidential information.

If you are required to handle person confidential data (whether staff or patients), we trust our staff to respect this confidence. The **Confidentiality and Data Protection** section of the handbook explains not only to you but to others who work on behalf of the organisation, how seriously we treat this matter.

The section aims to:

- Inform staff of the need and reasons for keeping information confidential
- Inform staff about what is expected of them
- Protect the CCG as an employer and as a user of confidential information

Personal information about individuals is routinely collected by the CCG as part of its work. The CCGs staff and those authorised to use that information are bound by common law obligations of confidentiality, contracts of employment and the requirements of the Data Protection Act 1998. Staff/client information is also the subject to the Caldicott guidelines.

A general duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

All staff working within the NHS are bound by a legal duty of confidence to protect person confidential data that they may come into contact with during the course of their duties.

The Health and Social Care Information Centre (HSCIC) has published a detailed
Guide to Confidentiality in Health and Social Care

Information collected by the CCG about its staff is subject to the same duty of confidentiality and the requirements of the Data Protection Act 1998. If confidentiality is broken, then this breach may result in an unauthorised disclosure of information, a breach of the Data Protection Act and a loss of trust between an individual and the CCG.

A principle of the IG Policy and Handbook is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the CCGs security systems or controls in order to do so.

The handbook has been written to meet the requirements of:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- The NHS Code of Confidentiality 2003

The handbook has been produced to protect staff by making you aware of the correct procedures so that you do not inadvertently breach any of these requirements.

If principles of the Policy or Handbook are breached then this may result in legal action against the individual and/or the CCG after investigation in accordance with the CCGs disciplinary procedures.

Privacy Impact Assessments

All organisations need to ensure that when new projects, processes, services or systems are introduced, or changes made to existing ones, the implementation does not breach information security, confidentiality or data protection requirements.

To assist with this, the Information Commissioners Office (ICO) has developed a framework called a **Privacy Impact Assessment (PIA)** for organisations to use when developing and introducing projects and processes that may have an impact on how we use patient and staff information. This process enables organisations to anticipate and address the likely impacts of new initiatives on an individual's privacy.

A PIA is a process whereby a projects potential privacy issues and risks are identified and examined from the perspectives of all stakeholders and a search is undertaken for ways to avoid or minimise privacy concerns. Systems, projects, etc., can then be designed to avoid unnecessary intrusion in to

people's privacy wherever possible, and features can be built in from the outset that reduce the likelihood of privacy intrusion.

As an organisation, we need to ensure that **all** new or changed projects or processes that use person confidential data go through the PIA screening process.

Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. By carrying out a PIA, it will increase public confidence in our data collection and the services we provide.

Not every new or changed process will require a PIA. The CCG has developed a Privacy Impact Assessment Guidance document, based on the national ICO guidance, which explains when a PIA should be undertaken and provides templates and guidance to complete a PIA should it be found one is required. This guidance can be found in the IG Handbook.

Responsibility to support Subject Access Requests and where to direct requests

Patients and employees have a right under the Data Protection Act 1998 to access personal data about themselves which is held in either electronic or manual form by the organisation. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 (except for records relating to deceased patients). This type of request is known as a Subject Access Request.

All Subject Access Requests must be made in writing. Within all applications for access to records the applicant will need to prove their identity.

As per the Department of Health's "Guidance for Access To Health Records Requests"
Although the DPA states 40 days to comply, a Government commitment requires that for health records requests should normally be handled within 21 days.

The administration of requests for access to records (subject access requests) will be undertaken by a trained Subject Access administrator. Clinically trained leads will review records prior to release under the Data Protection and Access to Records Acts. The CSU Information Governance Team are responsible for training Subject Access administrators and will provide advice and guidance on all aspects of Data Protection and Access to Records Acts. Additional guidance can also be provided by the Caldicott Guardian.

All Subject Access Requests will be dealt with following standard operating procedures set out by the CSU Information Governance Team, ensuring that NHS England is made aware of all requests received and the outcome/completion of each request.

If you receive a request for access to records, or any queries regarding access to records, the request/query should be **immediately** forwarded to the CCG's operational IG Lead to ensure the request is processed and responded to within the time frame specified by the relevant Act.

Fair Processing Notice

Individuals must be informed, in general terms, how their information may be used by the CCG and the organisation or types of organisations it may be disclosed to. To achieve this, the CCG has produced a **Fair Processing Notice** which will be displayed wherever members of the public may access the organisation, e.g. in reception areas of buildings, on the CCG website.

The Fair Processing Notice explains why the CCG may collect information about service users, how we will keep it secure, who we may share the information with, and the individual's rights under the Data Protection Act.

It is important that all staff familiarise themselves with the notice, so that you understand its content and know that any queries from the public or service users about their information should be directed to the CSU information governance team.

Confidentiality Audits

All staff have access to confidential information that is relevant to the role that you are employed to do. The organisation has a responsibility to actively monitor and audit access to confidential information. You should be aware that your role based access will be monitored and subject to audit.

If as a result of audit, it is found that staff have access to information that they shouldn't, the access rights will be revoked immediately. If it is identified that any staff member has inappropriately accessed information then action could be taken against them in line with the CCGs disciplinary procedures.

Smartcards

Access to confidential information is restricted based on your role within the CCG. If you have been provided with a Smartcard that provides you with access to person confidential data then you should be aware of your personal responsibilities when using your smartcard. On completing your smartcard application form you signed an RA01 form, which provides you with the terms and conditions of use.

Under no circumstances should you ever share your smartcard pin number or stick it to the front of your card. Smartcards should be removed from keyboards when not in use.

Lost smartcards should be reported as an IG incident at the earliest possible opportunity.

Full information on the use and security of smart cards can be found in the IG Handbook.

Business Continuity

Business continuity management describes an organisations attempt to predict, assess and counteract threats and risks that may cause or lead to significant disruption of all or part of the organisations business functions. It examines the likelihood and impact of such disruptive events occurring, determines what the organisation can do to prevent or minimise the level of disruption and develop plans to effect systematic and timely recovery.

All staff members should be aware of the organisations Business Continuity Plan and understand your own responsibilities in relation to its implementation.

All Information Asset Owners, should have identified their critical information assets and ensured they have been included within the business continuity plan. The responsible manager for the management and implementation of the business continuity plan should also ensure that the plan itself is listed as a key information asset on the CCGs information asset register.

Incident Management

All IG incidents should be recorded at the point at which the organisation becomes aware of the issue and risk assessed in line with the Information Governance Toolkit Incident reporting tool. The IG team should be notified to allow any mitigating actions to be completed and incident support to be provided to the CCG.