Policy

Data Protection & IG Policy

Classification	Confidential	Title	Data Protection & IG Policy	Version	2
Release Date	July 2020	Owner	Exemplar Health Care Services Ltd	Page	1 of 19

Policy

CONTENTS

Policy

ACRONYMS AND ABBREVIATIONS

BC	Business Continuity
CQC	Care Quality Commission
DFM	Data Flow Mapping
DH	Department of Health
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit
EEA	European Economic Area
FOI	Freedom of Information Act 2000
HSCIC	Health and Social Care Information Centre
IAM	Information Asset Management
IAO	Information Asset Owner
IAR	Information Asset Register
ICO	Information Commissioner's Office
IG	Information Governance
IGC	Information Governance Committee
IGT	Information Governance Toolkit
InfoSec	Information Security
IRM	Information Risk Management
ISA	Information Sharing Agreement
LDR	Local Digital Roadmap
NHSD	NHS Digital
PCD	Personal Confidential Data
RA	Registration Authority
SIRO	Senior Information Risk Owner
STP	Sustainability and Transformation Partnership

Policy

1. EXECUTIVE SUMMARY

This policy sets out the strategic IG agenda for Exemplar Health Care.

The Data Protection Act 2018 has six principles, that Personal Confidential Data (PCD) must be processed:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.

Furthermore, Data Subjects have increased rights, to:

1. Information about how their information is being processed.
2. Access to their information.
3. Rectification when information is wrong.
4. Be forgotten; when it is appropriate to do so.
5. Restrict processing.
6. Data portability.
7. Object to processing.
8. Appropriate decision-making.

In health and social care, the Caldicott Principles reflect these, that when using PCD:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect service user confidentiality.

Everyone within Exemplar Health Care has IG responsibility:

- **Directors:** Have ultimate responsibility for IG.
- **Senior Information Risk Owner:** The SIRO has overall responsibility for the Exemplar Health Care's information risk policy and advises the Board on its effectiveness. The Legal Director is the SIRO for the Exemplar Health Care Group.
- **Caldicott Guardian:** Has an advisory role to protect the confidentiality of service user information and ensure it is shared appropriately and securely.
- **Data Protection Officer:** Has the Organisations leadership function for IG, maintaining confidence of service users, staff and the public.
- **CIO:** Provides advice on maintaining the Confidentiality, Integrity and Availability of service user and staff information.
- **Information Asset Owners:** Support the SIRO, and have the function to understand what information is held in their work area, who has access to it and why. (Governance Champions)
- **Information Governance Committee:** IGC is chaired by the SIRO and is responsible for overseeing the implementation of IG policy and the annual IG assessment.
- **All staff:** Have responsibilities to abide by good IG practice as defined in this and other policies, and the Staff Handbook (see Appendix 1).

To ensure good practice across Exemplar Health Care there are robust IG processes in place:

- An annual IG audit.
- Oversight by the healthcare regulator, the Care Quality Commission (CQC).
- A mandatory annual training and awareness programme.
- A staff Confidentiality Code of Conduct, distributed to all staff.
- A robust plan to communicate Confidentiality and DP to Data Subjects.
- An IAM and Business Continuity (BC) programme.
- An Information Risk Management (IRM) programme.
- DP Impact Assessments (DPIA) for new projects and proposals.
- Robust Information Security (InfoSec), Cyber Security and User Access Controls.
- Safe Haven processes to ensure data is safely transmitted and received.
- Systematic Records Management processes.
- Robust IG clauses in third party contracts.
- Clarity on the legalities of processing data and the use of consent.
- Robust Information Sharing processes.
- Assurance on the transfer of PCD outside the UK.
- Data Quality Assurance.
- Subject Access Requests (SAR), allowing subjects to view and check their information.
- Clarity on the disclosure of information to the police, funders, CQC, Coroners etc.
- Robust processes for the reporting and analysis of information-related incidents.

2. INTRODUCTION AND AIM

Information is a vital asset clinically and for the efficient management of services, resources and performance. It is therefore important that an appropriately robust policy framework is in place. IG stipulates the way in which information, particularly in a health care environment, should use and handle PCD. PCD is:

- Personal information about identifiable individuals, which should be kept private.
- The DP legislation definition of personal and special categories of data, adapted to include those who have passed away (see next two paragraphs for definitions).
- Information 'given in confidence' and 'that which is owed a duty of confidence'.[1]

Under the DPA **Personal Data is defined** as:

> *Any information relating to an identified or identifiable natural i.e. living person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*[2]

And Special Categories of Personal Data is defined as:

Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation […].[3]

[1] Independent Information Governance Oversight Panel (2013), *Information: To Share or Not to Share*, p.130.
[2] General Data Protection Regulation, Article 4(1).
[3] General Data Protection Regulation, Article 9(1).

IG also enables Exemplar Health Care to ensure that all confidential information is dealt with legally, securely and efficiently, in order to deliver the best possible care to its service users.

This policy has been developed to locally implement national legislation and guidance including, though not limited to, that listed on pages 1-2.

3. SCOPE

This policy applies to and must be adhered to by all employees of Exemplar Health Care, regardless of grade or profession and any other iteration of personnel that could legitimately be considered staff. Its application is to any person who has been treated as a service user or employee by Exemplar Health Care in any way.

4. ROLES AND RESPONSIBILITIES

- **Directors:** Directors are ultimately responsible for ensuring the IG function is addressed.

- **Senior Information Risk Owner:** The SIRO is a Director-level member of staff with overall responsibility for the organisation's Information Risk Management. The SIRO also leads and implements the IG risk assessment and advises the Board on the effectiveness of IRM across the organisation. See Appendix 2. The Legal Director is the SIRO for the Exemplar Health Care Group.

- **Caldicott Guardian:** The Caldicott Guardian is the person within the Organisation with advisory responsibility for protecting the confidentiality of service user information and ensuring it is shared appropriately and securely.

- **Data Protection Officer:** The DPO has the leadership function for IG, maintaining the confidence of service users, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle PCD. This includes ensuring that the Organisation is fully compliant with all IG-related legislation and that the Organisation meets statutory and mandatory obligations for IG through development of strategy and implementation of IG policies.

- **CIO:** Provides advice on all aspects of information security. Their assessment of information security risks, threats and advice on controls.

- **Information Asset Owners:** The SIRO is supported by IAOs. The role of an IAO is to understand what information is held, how it is used, who has access and why for information systems under their responsibility.

- **All staff:** Staff have responsibility to abide by their legal, professional ethical and contractual responsibilities for IG related issues, regardless of their position, and whether directly employed or not. They must also comply with the most up-to-date version of this policy and other Organisation IG guidance, particularly the Staff Handbook and completion of the annual IG mandatory training.

5. OVERARCHING LEGISLATION AND PRINCIPLES

A range of components fall under IG as it overlaps Clinical Governance and is a subset of Corporate Governance. The overarching NHS framework is outlined in the Data Security and Protection Toolkit (DSPT), which replaced the IG Toolkit (IGT) in April 2018. Known as the National Data Security Standards, they are drawn from the 2016 Caldicott 3 Report and are outlined in Appendix 5.

In its management of PCD, Exemplar Health Care complies with DPA and Caldicott Principles. Under the new law, PCD must be processed in line with six principles:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.[4]

Data Subjects also have rights under the new legislation to:

1. **Information about how their information is being processed.** Exemplar Health Care addresses this by ensuring a layered approach to informing data subjects how their information is used, including posters, pamphlets and service-level leaflets.

2. **Access to their information.** See Section 6.0.

3. **Rectification when information is wrong.** Any request for rectification will be assessed on a case by case basis using the precedent of Exemplar Health Care's developing experience of the new legislation, along with relevant case law.
4. **Be forgotten, when it is appropriate.** In healthcare information needs to be retained for care and medicolegal purposes, rendering this right largely exempt. Any request to be forgotten will be assessed on a case by case basis using the precedent of Exemplar Health Care's developing experience of the new legislation, along with relevant case law.

5. **Restrict processing.** Data Subjects may request that Exemplar Health Care hold only sufficient Personal Data about them, but not process it any further. Any request for restriction of processing will be assessed on a case by case basis using the precedent of Exemplar Health Care's developing experience of the new legislation, along with relevant case law.

6. **Data portability.** This allows Data Subjects to obtain and reuse their information across different services. In healthcare there are not expected to be many requests, as much information is available as a SAR. Any request for portability of data will be assessed on a case by case basis using the precedent of Exemplar Health Care's developing experience of the new legislation, along with relevant case law.

7. **Object to processing.** This allows the Data Subject to object if they do not believe the use of their information is legitimate. Any request to object will be assessed on a case by case basis using the precedent of Exemplar Health Care's developing experience of the new legislation, along with relevant case law.

8. **Appropriate decision-making.** Exemplar Health Care is required to demonstrate that it has a lawful basis to carry out profiling and / or automated decision-making. This is undertaken by an annual organisation-wide assessment, led by the IG Team.

All requests from Data Subjects to exercise their rights must normally be responded to within 30 days, unless there are extenuating circumstances, in which case there are some rights to extension under the legislation.

[4] General Data Protection Regulation, Article 5(2) (a-f).

In the NHS, the Caldicott Principles are equally as important; when using PCD:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect service user confidentiality.

Full detail about Caldicott is in *Information: To Share or Not to Share* (2013).[5]

6. EFFECTIVE INFORMATION GOVERNANCE MANAGEMENT

a. Annual Information Governance Audit

From April 2018 Exemplar Health Care's IG compliance will be measured via a self-assessment process of compliance against standards set out in the DSPT (see Appendix 5). Once it is released Exemplar Health Care will utilise it to assess its IG practice in broadly the same manner as its IG Toolkit (IGT) predecessor to assess its compliance against national standards.

b. Care Quality Commission Oversight

CQC, as outlined in *Safe Data, Safe Care* (2016),[6] have powers to inspect Exemplar Health Care's IG as part of its inspection round. To this end Exemplar Health Care must ensure that robust IG practices are in place. CQC specifically requires that Medical Records are accurate, fit for purpose, held securely and held confidential.

c. Mandatory Training and Awareness

Fundamental to the success of delivering a robust IG agenda across Exemplar Health Care is the development of an IG-aware culture. Training is provided to all staff to promote this ethos.

In addition to formal IG training, a layered approach to awareness is employed, acknowledging a broader understanding of training to encapsulate awareness raising.[7]

Some roles, such as SIRO, Caldicott Guardian, and IAOs are required to undertake regular training to remain current in their role.

d. Confidentiality Code of Conduct

All staff must be aware of their individual responsibilities for the maintenance of confidentiality, DPA, InfoSec management and data quality. They are given the tools for this through attending annual mandatory IG training and all staff receiving a Confidentiality Code of Conduct. All new staff are issued the latter at recruitment, and all staff are annually directed to it in the Staff Handbook.

[5] See Independent Information Governance Oversight Panel (2013).
[6] Care Quality Commission (2016), *Safe Data, Safe Care*.
[7] Among others these include Global emails, articles in Headlines newsletter, active IG Team participation in the staff conference; bespoke advice; IG Team attendance at departmental meetings; StaffNet news articles; monthly Organisation Brief articles and the Information Governance Staff Handbook.

It is made clear in both of these documents that failure to maintain confidentiality may lead to disciplinary action, including dismissal.

e. Communicating Confidentiality and Data Protection

Exemplar Health Care maintains a Information Governance and Information Security Improvement Plan. This includes actions to ensure that service users and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as Data Subjects, in particular how they may access their Personal Data and how they may exercise those rights.

f. Information Asset Management and Business Continuity

A core IG objective is that IAs and the use of information in them are identified and that the business importance of those assets is established.

IAs are those that are central to the efficient running of Exemplar Health Care and specific departments, e.g. service user, finance, stock control etc. They also include, but are not limited to the following examples:

- **Information** – system documentation and procedures, archive media and data.
- **Software** – databases, application programs, systems, development tools and utilities.
- **Physical** – infrastructure, equipment, furniture and accommodation used for data processing.
- **Paper Records** – Service users' records, employee HR records, corporate records
- **Services** – computing and communications, heating, lighting, power, air conditioning used for data processing.
- **People** – qualifications, skills and experience in the use of information systems.
- **Intangible** – Exemplar Health Care's reputation.

Essentially, it is information in any format that is of value to the organisation and would be problematic if it were not accessible.

Exemplar Health Care has clear lines of accountability for IRM that lead directly to the Directors through the SIRO.

The SIRO has the final decision on approving identified risk mitigation plans as part of the Service Level Agreement (SLA) with Exemplar Health Care. Serious risks must be entered onto the Risk Register.

All information and assets associated with information processing facilities must be owned by a designated part of Exemplar Health Care, for example HR, Finance. The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and reviewing access restrictions, classifications, and BC arrangements taking into account applicable access control policies.

In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

All changes to IA, such as system upgrades, should follow an established change control procedure, such as a DPIA (formerly known as a Privacy Impact Assessment / PIA, see Section 6.h)

.

g. Information Risk Management

Exemplar Health Care is committed to making the best use of the information it holds to provide efficient healthcare and services to its service users and the local health economy while ensuring that adequate safeguards are in place to keep information secure and to protect Data Subjects' right to privacy.

Exemplar Health Care recognises that information handling represents a significant corporate risk in that failures to protect information properly or use it appropriately can have a damaging impact on its reputation. Furthermore, failure to protect information adequately can attract the attention of the Information Commissioner's Office (ICO), which regulates DP and has access to a range of sanctions including significant fines.

Information risk is intrinsic in all administrative and business activities and all staff must continuously manage it. Exemplar Health Care recognises that the aim of IRM is not to eliminate risk, but to provide the structural means to manage it, by balancing its treatments with anticipated benefits that maybe derived.

Exemplar Health Care acknowledges that IRM is an essential element of broader IG and InfoSec arrangements and is an integral part of good management practice; it should not be seen as an additional requirement.

The risk management framework is dependent on allocating clear organisational responsibilities, identifying all the IAs, assessing the associated risks and managing any incidents arising from them. This will:

- Protect the Organisation, its staff and its service users from information risks where the likelihood of occurrence and the impact is significant.
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
- Encourage proactive rather than reactive risk management.
- Inform decision making throughout the Organisation.
- Meet legal and statutory requirements.
- Assist in safeguarding the Organisation's IAs.

Information Risk Assessments are performed for all information systems and critical IAs.

Information incident reporting is in line with Exemplar Health Care's overall risk management incident reporting processes. Additional guidance is drawn from NHS Digital's (NHSD) Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Indicators that IRM is being positively enacted include, but are not limited to successful completion of the DSPT and there having been no involvement from the ICO as a result of significant DP breaches.

h. Data Protection Impact Assessments

In line with ICOs guidance, a DPIA must be undertaken for any project, procurement, business case, transfer of Personal Data or departmental / team initiative where there is a potential impact upon the privacy of individuals.[8]
DPIAs are a Risk Assessment tool to analyse how a particular project or system will affect the privacy of the individuals involved.[9] Projects are not formally defined by the Organisation, but must be understood be any plan or proposal,[10] including potentially any proposal, procurement, business case and / or departmental / team initiative that include transfers of Personal Data and / or potential sensitive business information.

[8] See Information Commissioner's Office (2014), *Conducting Privacy Impact Assessments Code of Practice*.
[9] Information Commissioner's Office (2014), p.5.
[10] Information Commissioner's Officer (2014), p.5.

The DPIA process must be an integral to conventional project management techniques, and be started from the very earliest stages of the project's initiation, often as a result of the A3 business case process being invoked.

DPIAs are chiefly concerned with an individual's ability to manage their information; the Organisation's processes are therefore aligned to DP and Caldicott principles, with specific concentration being given to the minimising of harm arising from intrusion into privacy, as defined by those principles.

An effective DPIA allows the organisation to identify and resolve any such problems at an early stage, minimising costs and reputational damage which might otherwise occur.

For further procedural detail see Appendix 6.

i. InfoSec, Cyber Security and User Access Controls

Exemplar Health Care's Cyber and InfoSec Management System is as promoted in the Information Security Code of Practice, based on industry standards, providing a comprehensive and coherent approach to identify and manage IAs, whether electronic or manual.

Exemplar Health Care ensures that PCD is protected by encryption in accordance with DH directives.

To prevent unauthorised access to information systems, formal procedures are in place to control the allocation of access rights to information systems and services, which cover all stages in the lifecycle of system access. This is supported by the IAO and IAM processes outlined in Section 6.f and 6.g.

Users are made aware of their responsibilities for maintaining effective access controls through the inclusion of InfoSec in IG training, particularly with regard to the use of passwords and the security of equipment.

Security facilities at the operating system level should be used to restrict access to computer resources, including terminal identification, access records, authentication mechanisms and access time restrictions.

j. Safe Haven

All transfers of PCD, for whatever reasons, must wherever possible, be undertaken within a Safe Haven environment, to ensure it adheres to the legal restrictions that govern transfer of such information.

Safe Havens are arrangements in place to ensure that PCD can be transmitted safely and securely, for example a physical location, such as a lockable room where personal faxes are received, or a virtual network of staff that are authorised to receive or send PCD and may do this by any method of communication. Exemplar Health Care fully endorses and promotes the use of such processes when sending or receiving PCD for any purpose.

Detailed operational guidance, which must be followed, is available for staff within the Staff Handbook (see Appendix 1).

k. Records Management

Exemplar Health Care is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposition. Exemplar Health Care ensures it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of the information efficiently and securely when it is no longer required.

Care Records are managed in accordance with the Records Management Code of Practice for Health and Social Care, as set out in Exemplar Health Care's **Records Management Policy.**

l. Third Party Contracts

It is not unusual to have third parties undertaking tasks and services on behalf of the Organisation. It is possible that as a result of access to Information Assets, third party staff may have significant access to service user or staff PCD.

Without exception contracts must be in place for any activity where third parties have access to service users, their PCD, or staff PCD on behalf of Exemplar Health Care.

It is the joint responsibility of the Legal Department and the owning Manager of the contract to ensure this Checklist is completed and the contract is IG compliant.

The SIRO and IAOs must take all reasonable steps to ensure that contractors and support organisations to whom PCD is disclosed comply with their contractual obligations to keep PCD secure and confidential.

An accurate register of all third party contracts must be maintained by Exemplar Health Care, and is managed by the Legal Team.

m. Processing Data, the Use of Consent and Information Sharing

Sharing and use of information about an individual between within and between partner agencies is vital to the provision of co-ordinated and seamless provision of care and services. Exemplar Health Care keenly recognises the need for shared information and robust InfoSec to support the implementation of joint working arrangements. The uses and sharing of clinical data can be divided into two broad categories.

The first of these is immediate **Direct Care**, which the Independent IG Oversight panel defines as:

> *A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.*[11]

For such use service user consent is not generally required under new legislation. However, practitioners must maintain an awareness of the Common Law Duty of Confidentiality, that if the service user disclosed information in circumstances where it was expected that a duty of confidence applied, it should not normally be further disclosed without that Data Subject's consent. If this has not been obtained it is beholden on the member of staff intending to share personal information to make an appropriate decision based on whether disclosure is essential to safeguard either the Data Subject or a third party and is considered to be in the public interest. There may also be a legal obligation to share the information, such as a Court Order.

[11] Independent Information Governance Oversight Panel (2013), p.128.

The second category is **Secondary Uses**, which the National IG Board defines:

> *Any purpose which does not "directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided" to the individual'.*[12]

For such use service user consent is generally required. This is defined as 'freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of Personal Data relating to him or her, such as by a written statement, including by electronic means, or an oral statement'.[13]

However, under the DPA legislation consent is not required where there is another condition for processing. There are specific legal gateways for sharing PCD for the planning of services and management of health and social care systems and services. For such uses a DPIA must be completed where identifiable Special Categories of Data are present and formal advice must be sought from the Legal Department. A documented Information Sharing Agreement (ISA) is highly likely to be required .

An ISA is good practice and can be a useful way of providing transparency for organisations needing to exchange information, providing assurance in respect of the standards that each party agrees to adopt.

Beyond sharing for immediate Direct Care and Secondary Uses, an ISA is required for **large-scale regular / permanent sharing**, such as giving access to a clinical system.

n. Data Quality Assurance

The quality of information acquired and used within Exemplar Health Care is a key component to its effective use and management. As such, IAOs and managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

Exemplar Health Care promotes Data Quality through the use of policies and procedures including the **Records Management Policy**, and associated statutory professional requirements to ensure that wherever possible, information quality will be assured at the point of collection.

The IAM process encourages that Data Quality audits are undertaken annually.

o. Subject Access Requests

All living individuals, whether service users or staff, have a right to verify the lawfulness of the processing by:

- Having it confirmed to them that their data is being processed.
- Being given access to their Personal Data.
- Being given supplementary information, akin to that given in a Privacy Notice, explaining why the data is being processed.

Staff must be aware that anything they record about service users or colleagues, wherever it is stored, legally could and should in principle be released when a request is received, as all information technically forms part of the data subjects' wider HR or Medical Record. Subject Access Requests should be processed in accordance with Exemplar Health Care's Subject Request Policy and procedure.

[12] National Information Governance Board (2011), *Information Governance for Transition*, p.42.
[13] General Data Protection Regulation, Recital 32.

Any requests should be sent to infosec@exemplarhc.com who will respond to the request.

p. Disclosure of Information to the Police

Under the law the Police and other law enforcement agencies do not have automatic right to see PCD about service users or staff. However, Exemplar Health Care will cooperate with them as much as possible, when it is legal to do so.

When requests are received, even with a Police Officer in attendance, each one must be considered individually on its own merit. PCD will not be released without careful consideration.

Requests from the Police were formerly considered under Section 29(3) of the Data Protection Act 1998, so it is likely that colloquially such requests may continue to be known as a Section 29(3). This should not prevent them being actioned in line with the new legislation, which allows for the release of personal and special categories of data for 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.[14]

Exemplar Health Care requires any request to release personal or sensitive data about service users or staff to be signed or countersigned by a police officer of at least Inspector rank.

The types of scenarios where requests are likely to be considered appropriate are based on those outlined in the Confidentiality: NHS Code of Practice and include, but are not limited to, murder, manslaughter, rape, treason, kidnapping, child abuse, serious harm to state security, serious harm to public order, as well as crimes involving substantial financial gain.[15]

Any requests should be sent to infosec@exemplarhc.com who will assess the decision to release to the Police.

However, unless there is a legal basis to do so Exemplar Health Care is not obliged to make a release, and will make decisions based on a public interest test.

Any requests for information received from Coroners, funders, CQC, safeguarding or third party solicitors should also be sent to infosec@exemplarhc.com who will assess the decision to release to the requesting party.

7. INFORMATION GOVERNANCE, INFOSEC AND CYBER SECURITY INCIDENTS

InfoSec must be informed immediately of all IG, InfoSec and Cyber Security incidents. These include, but are not limited to, NHSD's classifications:

- Lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Disclosed in error
- Uploaded to website in error
- Non-secure disposal – hardware
- Non-secure disposal – paperwork

[14] General Data Protection Regulation, Article 23(1)(d). At time of writing, an exemption to allow such releases is expected to be written into the Data Protection Act 2018.
[15] Department of Health (2003), *Confidentiality NHS Code of Practice*, p.35.

- Technical security failing (including hacking)
- Unauthorised access/disclosure

IG incident reporting is undertaken in accordance the Exemplar Health Care's incident reporting process. Notification of incidents should be sent to infosec@exemplarhc.com.

8. MONITORING AND MEASUREMENT

The effectiveness of this policy is monitored on a quarterly basis.

APPENDIX 1 – STAFF HANDBOOK

Exemplar Health Care maintains and distributes to all staff a Staff Handbook which includes guidance linked to Data Protection. This is updated annually in the autumn. This has operational guidance regarding good information practice.

APPENDIX 2 – SENIOR INFORMATION RISK OWNER ROLE DESCRIPTION[16]

1. The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the Board (or equivalent senior management group/committee)

2. The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a Board member already leading on risk management or information governance.

3. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

4. The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management Strategy and processes. He/she will provide leadership and guidance to a number of Information Asset Owners.

5. The key responsibilities of the SIRO are to:

    a. Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
    b. Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
    c. Review and agree action in respect of identified information risks.
    d. Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
    e. Provide a focal point for the resolution and/or discussion of information risk issues.
    f. Ensure the Board is adequately briefed on information risk issues.
    g. Ensure that all care systems information assets have an assigned Information Asset Owner.

[16] Information Governance Toolkit v14.1 Requirement 307.

APPENDIX 3 – CALDICOTT GUARDIAN ROLE DESCRIPTION[17]

1. A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

2. The Caldicott Guardian should play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information. Their main concern is information relating to service users, 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 service user information.

3. Caldicott Guardians should apply the seven principles wisely, using common sense and an understanding of the law. 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 the impartiality and independence of their advice.

APPENDIX 4 – INFORMATION ASSET OWNERS ROLE DESCRIPTION[18]

1. For information risk, IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. In large organisations IAOs will be assisted in their roles by staff acting as Information Asset Administrators (or persons with equivalent responsibilities) who have day to day responsibility for management of information risks affecting one or more assets.

2. It is particularly important that each IAO (or equivalent) should be aware of what information is held and the nature of and justification for information flows to and from the assets for which they are responsible.

3. The role of the IAO is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result, they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The IAO will also be responsible for providing or informing regular written reports to the SIRO (or equivalent), a minimum of annually on the assurance and usage of their asset.

4. It is important that "ownership" of Information Assets is linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.

5. It is the responsibility of Information Asset Owners to ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.

[17] UK Caldicott Guardian Council (2017), *A Manual for Caldicott Guardians*, p.3.
[18] Information Governance Toolkit v14.1 Requirement 307.

APPENDIX 5 – NATIONAL DATA SECURITY STANDARDS

The National Data Security Standards are from the National Data Guardian's *Review of Data Security, Consent and Opt-Outs* (2016) (Caldicott 3), and form the structural basis of the Data Security and Protection Toolkit, which replaces the IGT in April 2018.

	Leadership Obligation 1: ***People:*** *Ensure staff are equipped to handle information respectfully And safely, according to the Caldicott Principles.*
1.	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2.	All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3.	All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
	Leadership Obligation 2: ***Process:*** *Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.*
4.	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5.	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6.	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7.	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
	Leadership Obligation 3: **Technology:** Ensure technology is secure and up-to-date.
8.	No unsupported operating systems, software or internet browsers are used within the IT estate.
9.	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10.	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.

.

APPENDIX 6 – DATA PROTECTION IMPACT ASSESSMENT PROCESS

A non-exhaustive list of projects that would require a Data Protection Impact Assessment (DPIA) includes:

- A new IT system for storing and accessing Personal Confidential Data (PCD).
- A data sharing initiative where multiple organisations seek to link sets of PCD.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing PCD for a new, unexpected or more intrusive purpose.
- A new surveillance system, especially one which monitors members of the public, or the application of new technology to an existing system, for example adding number plate recognition capabilities to existing CCTV.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- Use of data that appears to be pseudonymised or anonymised, but could be identifiable if combined with other information. Pseudonymisation is '[t]he process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity', and anonymisation '[t]he process of rendering data into a form which does not identify individuals and where identification is not likely to take place'.[19]

Answering a set of screening questions within the DPIA document will identify if there is any potential impact on privacy. A positive answer to **any** of the questions confirms that a DPIA is required.

If so, the Project Manager or Board (however these are defined, depending on the size of the project) must proactively consider how project management activity can address privacy issues. These must also be discussed with all appropriate stakeholders.

DPIAs must be conducted by someone that is introducing a new or significantly changed project, procurement, business case or departmental/team initiative that involves PCD. The responsibility for carrying out the DPIA must be formally recorded and assigned by the Project Board / appropriately senior Manager.

The selection must be allocated to a member of the project team, with a strong understanding of the project or process itself.

Privacy implications must be considered at each phase of the life-cycle of a project. This may result in several DPIAs being completed or updated. It is for the Project Manager or Board to ensure this is effectively managed.

Not all DPIAs will relate to changes that require the production of a business case. Where a business case will be required by the Organisation the approved DPIA (or nil return) should be appended to the case in line with the business case process. When a DPIA is completed it must first be reviewed by the appropriate Project Board, and then be submitted to the Legal Department by email for triage.

For service user-based DPIAs, the IG Team will make a recommendation to the Caldicott Guardian, who acts as the Organisation's conscience with regard to use of service user information and has ultimate sign-off for the processes using their information. For similar non-service user based DPIAs, such as (but not limited to) Human

[19] Information Commissioner's Office (2012) *Anonymisation: Managing Data Protection Risk Code of Practice*, pp.48-49.

Resources, the sign-off will be undertaken by the Organisation's SIRO. The recommendations will be either Approved, or Declined.

Once approved by the IG Team DPIA Panel and passed to the SIRO (as applicable), who will Approve or Decline it.

This process will continue cyclically until such time as the IG Team and SIRO (as applicable) are in agreement with the project's proposals.

DPIAs must be retained by the Project Board / appropriate Senior Manager and form part of official Project Documentation where applicable.

The outcomes of a DPIA include:

- The identification of the project's privacy impacts.
- Appreciation of those impacts from the perspectives of all stakeholders.
- An understanding of the acceptability of the project and its features by the organisations and people that will be affected by it.
- Identification and assessment of less privacy-invasive alternatives.
- Identification of ways in which negative impacts on privacy can be avoided.
- Identification of ways to lessen negative impacts on privacy.
- Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them.
- Documentation of the outcomes.

Compliance with the DPIA requirement is monitored by the Legal Team, which regularly reviews incidents reported to establish if they have been caused in whole or part by DPIAs not being appropriately completed. To ensure projects appropriate complete DPIAs this will be reviewed by the Information Governance Committee.