QMS2301 - Security Policy

Process Owner

Name:	Michael Pennington
Position:	Head of Operations and Security
Signature	

Authorisation and Approval

Name:	Phil Kirby
Position:	Manager Director
Signature	

Summary of Changes since Last Version

Full review of format and content for GDPR

Related Documents

QMS2302	Security Incident Process
QMS2303	Security Incident Report Form
QMS2306	Data Security Agreement
QMS2308	IG Framework Policy
QMS2321	Laptop, Mobile Phone and Portable Media Policy

1 Introduction

Health Intelligence operates almost exclusively within the area of healthcare and operates within the UK. The Company's philosophy is to ensure the delivery of tangible patient care benefits and effective support to NHS organisations and others to this end. A small, but quality Company, the skills and experience of our personnel are key.

Security is of utmost importance within the National Health Service and it is company policy to operate at all times within the guidelines set out within this security policy.

Please note that this policy is also provided to all third-party consultants who will adopt the same working practice as Health Intelligence Ltd.

Why this Policy Exists

This data protection policy ensures Health Intelligence:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) describes how organisations — including Health Intelligence — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2 People, Risks and Responsibilities

Policy Scope

All assets, processes and staff (including remote workers) involved in the provision of Diabetic Retinal Screening, Childhood Health Information Services and Informatics Services (Including but not limited to Childhood Immunisations, Health Checks, Population Based Risk Stratification and Long Term Conditions Intelligence) to the NHS from all of the Health Intelligence offices.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018 and GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals such as healthcare data.

Policy Objectives

The objective of this Policy is to establish and maintain both the physical and information security of Health Intelligence, including sensitive and confidential information, by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other documents
- Introducing a consistent approach to security and ensuring that all members of staff understand their responsibilities
- Creating and maintaining within the Company a level of awareness of the need for information security as an integral part of the day to day business.

Data Protection Risks

This policy helps to protect Health Intelligence from very real data security risks, including:

- **Breaches of confidentiality** - For instance, information being given out inappropriately.
- **Failing to offer choice** - For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage** - For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Health Intelligence has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Health Intelligence meets its legal obligations by setting and endorsing the Information Governance (IG) Strategy and to formally review the agreed policies and procedures to ensure continued compliance.

- The **Managing Director, Phil Kirby,** is Health Intelligence's Caldicott Guardian and has overall responsibility for Health Intelligence's compliance with IG and is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.

- The **Head of Operations and Security, Michael Pennington**, is responsible for:
    - Arranging data protection training and advice for the people covered by this policy
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Health Intelligence holds about them (also called 'Subject Access Requests')
    - Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.

- The **IT Manager, Chris Sagar**, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services the Company is considering using to store or process data. For instance, cloud computing services.

- The **Marketing Manager, Alexandra Richardson**, is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets e.g. newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- **All managers** are responsible for:
    - Building the IG Strategy 'where applicable' into day to day working practices
    - Ensuring compliance with the IG Strategy is ongoing on a day to day basis
    - Ensuring that all security breaches or perceived security breaches are referred to the Head of Operations & Security for immediate investigation.

- **All staff** are responsible for:
  - Ensuring that they have reviewed and understood all the relevant IG policies and procedures
  - Ensuring that they use this security understanding and awareness and build into their daily work
  - Informing the Head of Operations & Security of all security issues or risks in relation to the best practice guidance that is provided
  - Completing in a timely manner the IG Training Toolkit Assessment modules.

3 General Staff Guidelines

1. The only people able to access data covered by this policy should be those who **need it for their work**
2. Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line manager.
3. **Health Intelligence will provide training** to all employees to help them understand their responsibilities when handling data.
4. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
5. In particular, **strong passwords must be used,** and they should never be shared.
6. Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
7. Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
8. Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.
9. Laptop screens are sited to minimise the **risk of being overlooked.**
10. Laptops and PCs must either **be logged out or have their screens locked** when the user is away from their desk.
11. Conversations and phone calls are kept discreet to reduce the chances of eavesdropping.

4 Data Protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Head of Operations and Security.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. Where the paper contains **Patient Identifiable Data (PID)** it should be printed on **blue paper**.

These guidelines also apply to data that is **usually stored electronically but has been printed out** for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them, e.g. on a printer**
- **All data printouts should be placed into the 'Shred-it'** and therefore disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Where applicable, data should be **protected by strong passwords** that are changed regularly and never shared between employees
- No **patient identifiable data shall be stored by users on laptops, notebooks and USB storage devices at any time**. For further clarification, please see section 4 of QMS2321 - Laptop, Mobile Phone and Portable Media Policy.
- Data should only be stored on **designated drives and servers** and should not be uploaded to any cloud computing services
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures
- **PID should never be saved directly to laptops** or other mobile devices like tablets or smart phones.

Data Use

Personal data is of no value to Health Intelligence unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT Manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data Accuracy

The law requires Health Intelligence to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Health Intelligence should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a patients / customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a patient / customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject Access Requests

All individuals who are the subject of personal data held by Health Intelligence are entitled to:

- Ask **what information** the company holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the company is **meeting its data protection obligations**.

The process is managed by Document 'QMS2609 - Process - Access Request for Personal Data' and by using the form 'QMS2608 - Subject Access Request Form - v1.4'.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Health Intelligence will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board and from the Company's legal advisers where necessary.

Providing Information

Health Intelligence aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights.

To these ends, the Company has a privacy statement, setting out how data relating to individuals is used by the Company. This is available on request and on our websites, for example: http://www.eadesp.co.uk/diabetic-eye-screening/privacy-notice/

5 Information Classification Handling and Exchange

Classification

Health Intelligence classifies information into four levels of classification:

- **Confidential (PID)**
- **Confidential**
- **Internal**
- **Public**

Information that is classified as restricted (Internal Board only or Internal Management Team only, etc.) must, in addition, identify the individuals or roles to which the information is restricted to.

Information received from outside Health Intelligence is re-classified by its recipient so that, within Health Intelligence, it complies with this classification.

Information sent and received internally that is not marked with a classification level is treated as confidential. Information that is sent externally unmarked is classified as public. If any confidential or restricted information is sent externally without the correct classification marking, then that action is classed as breaching the Company regulations and may be considered as misconduct.

Confidential PID: This restricted classification is reserved for patient identifiable data (PID).

- This data should only be sent via either NHS secure mail or via Secure FTP over N3 and be stored only on encrypted media
- Examples: This covers any information which relates to patient's personal details (administrative and/or clinical).

Confidential: This classification covers all information assets that have value, but which do not need to fall within the restricted category.

- This information should be only communicated, to employees for whom it is meant for and access to this information is allocated on a "need to know" basis only
- Confidential information is restricted for release to employees on specific grade levels and third party contractors whose contracts with the Health Intelligence authorise such access to confidential information
- Information should not be distributed freely internally or externally with any organisation. Inappropriate disclosure could cause embarrassment to the Company and/or individual(s), but not cause serious damage.
- Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine
- Examples: Contracts, planning documents, specifications, system administration guides, network diagrams, drafts of internal documents, staff appraisals, personnel records, expense reports, individual salary letters, pay slips, client contracts, third party contracts, new patent submissions, data falling under Data Protection Act, Business Continuity Plan.

Internal: Everyone on a permanent employment contract with Health Intelligence is entitled to access information with this classification, as are third party contractors whose contracts with Health Intelligence authorises such access.

- This information has no restrictions in terms of how it is communicated, other than that it is cleared for release outside Health Intelligence or to those individuals and/or organisations who sub-contract with Health Intelligence other than where it is has been specifically authorised in advance and contractually documented with that third party.
- This information is intended for internal disclosure only but would cause no measurable damage to the company if disclosed externally.
- Examples: Internal memos, routine reports, monthly reports, corporate policies, company procedures, incident reporting, general HR forms, training materials, internal telephone directory.

Public: This is information which can be released outside of Health Intelligence and includes documents or information intended for public disclosure.

- Examples: Information widely available in the public domain, public facing website pages, marketing materials, demonstration software.

Labelling

Electronic documents are labelled as set out above, with the classification set out in the document footer. Documents that do not have footers are marked accordingly. Unmarked documents are automatically treated as public documents.

Removable and storage media (CD-ROMS, USB sticks, tapes, etc.) may not be used for the storage of Confidential (PID) or any patient level data unless it is has been authorised by the Head of Operations and Security and is encrypted.

Storage

Media should be stored in a proper heat and humidity-free, clean storage environment.

Asset owners should take proper care in handling data media, as these are very sensitive.

All paper media that have been declared Confidential (PID) or Confidential should be stored in lockable filing cabinets with owners identified.

Other types of printed or paper media have to be stored by the owners under lock and key in their drawers or cupboards and files; forms have to be stored safely.

Electronic Confidential reports or files should be stored in a secured directory / folder with strict access restrictions. Wherever possible files should be password protected. Backup copies of all such files / reports should be taken in a secured folder / directory.

Other forms of electronic reports should also have access rights based on need and it is the individual responsibility to store is securely in their workstations.

Communication & Transmission

Electronic or paper information classified as Confidential (PID) or Confidential, if there is a requirement for communication, must be done on 'Need-To-Know' basis only through a secure mode. Care must be taken to ensure that in the TO field and CC list, only authorised people have been added while sending emails.

Electronic or paper information classified as Confidential must be communicated to suitable recipients only. Care should be taken to ensure that unauthorised recipients do not get to know the contents of such information.

Confidential (PID) or Confidential information should not be discussed in non-secure environments.

Handling & Processing

The Asset Register will indicate the designated personnel who are authorised to handle paper & electronic assets that carry a classification level as Confidential (PID) or Confidential; only these personnel are authorised to handle these assets.

Care should be taken to ensure that whilst processing Confidential (PID) data; it is not revealed by mistake to unauthorised personnel.

Secure post (registered post) should be used for the transmission of personal information between Health Intelligence and the named addressee requested to acknowledge receipt of the information. Secure packaging, that will clearly show if it has been tampered with, should be used.

Patient clinical data on paper should be placed in a locked filing cabinet when not being worked on

Internal post containing personal information transported within and between Health Intelligence's sites should be carried in lockable satchels to protect it from loss or accidental viewing.

Encrypted electronic media transported between sites or organisations should be properly packaged and clearly labelled to ensure they are handled correctly and not corrupted by magnetic fields.

A fax machine used to receive person identifiable or sensitive information must be located in a secure environment. Additionally, the fax should be removed from the machine on receipt and appropriately dealt with and safely stored. Where appropriate, the sender should be contacted to confirm receipt.

Patient digital images (still or moving) are being used more often. If digital/video images are part of the patient record, they must be transferred and retained in accordance with the Caldicott Principles and stored securely.

Audio recordings of patients should be treated in a similar manner to digital images.

Recorded telephone messages may contain sensitive personal information, for example, the names and addresses of applicants phoning for a job. Therefore, they need to be properly secured so that only those entitled to listen to the message may do so. Telephone and other messages taken in another's absence should be recorded by a dedicated method that is kept secure and confidential.

Health Intelligence should ensure that when personal or sensitive information is received it is stored securely with access only by those with a legitimate right to the information. The type of storage that is appropriate will depend on the media on which the information is received.

Destruction

Confidential paper documents for destruction are shredded for secure disposal.

Electronic assets should be permanently deleted, by firstly formatting the disk and then deleting the contents of the disk.

Hard drives, removable media and any similar items are checked for any confidential or restricted information and such information removed and/or the item put beyond use (i.e. destroyed).

Control of Records

All records should have appropriate version control applied which includes:

- The version number
- Date of creation/amendments
- Verification signature(s) where appropriate

All records must be classified in accordance with Health Intelligence's classification guidelines

All changes to records must go through an appropriate approval process (wherever one has been agreed).

A record will be maintained, to record all business forms and logs in use by Health Intelligence. 'QMS0308 - Control of Records List' is this log and it specifies the following requirements for each form/log: department, type of record, naming convention, and the stored location of the document, along with the retention period and any protection applied.

All records must have electronic versions which are made available on Health Intelligence's network and which can be backed up in line with Health Intelligence's Information Backup and Restore Policy.

Records must be maintained and stored in line with relevant retention policies, legal regulations and/or statutory requirements.

Where there is no longer a requirement to retain records, appropriate document disposal and removal procedures must be carried out in accordance with Health Intelligence's Information Destruction Policy (8.3.3.10).

All records of security incidents must be kept as part of Health Intelligence's Information Security Management System.

All information security records should be reviewed and controlled by Health Intelligence's IG Steering Group.

Information Transfer

Transport of information and system documentation Confidential (PI.D) and Confidential information is protected from unauthorised use by the controls established within Health Intelligence. Any information transmitted externally to Health Intelligence is protected from unauthorised access by either being sent only to the intended recipient or if physically sent by sealing the protective container or being hand carried by a member of staff. System documentation is similarly protected from unauthorised access by password management and privilege control.

Emails have a disclaimer attached indicating that the information contained in the mail is for the recipient only and that any unintentional recipient should not act upon the information apart from notification to sender or recipient that the message has been inadvertently diverted.

Email is not a secure system. All staff using email should be made aware of this during their induction training and during any training provided for use of the email system. Therefore, patient identifiable and other sensitive information should not be sent by email unless it has been encrypted to standards approved by the NHS.

NHSmail accounts are encrypted to NHS-approved standards and may be used for sending patient identifiable data to recipients that also have an NHSmail account. There is still a need to be certain about the identity of the recipient. It is imperative that all users are aware that the data is encrypted only between NHSmail accounts.

Emails containing patient identifiable data should not be sent to non-NHSmail accounts, as they are not encrypted, even if sent from an NHSmail account. All users must be fully trained in the use of email and NHSmail accounts.

Emails containing patient identifiable data must be stored appropriately on receipt, e.g. incorporated within the individual's record, and deleted from the email system when no longer needed.

Email attachments are one of the most common methods for transmitting viruses.

All users should be aware of the dangers posed by opening attachments, especially those they were not expecting. Up-to-date anti-virus software is used to check attachments and lock particular file types.

Documented Information Retention Policy

The required retention periods, by record type, are below:

Record Type	Retention Period	Responsible
Human Resources (HR) Records	Six years	HR Manager
Finance Data	Six years	Directors
Customer Data	Six years	Head of Operations and Security

Record Type	Retention Period	Responsible
Incident Documents	Three years	Head of Operations and Security
Property Lease Documents	Two years	Directors
Third Party contracts and agreements	Six years	Directors
Tax Records	Six years	Directors
Audit Records	Three years	Head of Operations and Security
Management System Records	Three years	Head of Operations and Security

The Head of Operations and Security is responsible for the destruction of the data once it has reached the end of the retention period specified in table above. Destruction must be completed within 90 days of the planned retention period.

6 Personal Security

All members of staff and agents are obliged to read and sign the Health Intelligence Security Policy at least every twelve months or upon any alterations to the policy. Records will be maintained.

- Reference to the need to maintain a high standard of confidentiality. Signature of the document commits the individual to abide by the Data Protection Act, the General Data Protection Act, the European Data Protection Directive, the Computer Misuse Act and the Health Intelligence Security Policy. Disclosure or misuse of personal data will be treated as a serious disciplinary offence, which may result in disciplinary action.
- IG security requirements form part of the recruitment process, it is included in all job advertisements and job descriptions. As part of the recruitment process, security and confidentiality clauses are part of the employment contract and completion of a Disclosure and Barring Service check (formally known as CRB checks) forms part of the employment offer for all relevant staff.
- HR shall always take up previous work references for all new employees. This procedure does not however, guarantee that all employees shall behave impeccably during their employment. Line management should always be vigilant for signs of staff disgruntlement or significant personality changes or even a more affluent lifestyle of any employee.
- It is the responsibility of each member of staff to be aware of the full nature of their responsibilities and in particular the limits of those responsibilities. This is best achieved through discussion with their line manager who should then document the results of such discussions. Ideally, where appropriate, members of staff shall have a current written job description.

- It is the intention of Health Intelligence that all members of staff receive appropriate training to enable them to carry out their work effectively. It is the responsibility of the line manager, in conjunction with the employees and/or the agents, to ensure that any member of staff who uses an information system is competent to do so. They must also appreciate the importance of providing correct information and fully understand the status of the output received.
- To support efficient and knowledgeable working practices, each member of staff or agent shall have access to appropriate documentation. However, it must be recognised that such documentation may also be of help to an individual who may wish to attempt to gain unauthorised access to the system(s), and it must, therefore be held securely at all times.
- Any employee or agent who becomes aware of errors that may have been made by the information system(s) must formally report such errors to their line manager and/or the Head of Operations and Security. The seriousness of an error is not the main issue; even minor errors may be symptomatic of a deeper and much more serious issue.
- Health Intelligence management regard the preservation of the security of information systems as of vital importance. Any breach in security shall be properly investigated and, where appropriate, disciplinary action shall be taken.

7 Equipment Security

All computer and related equipment shall, where practicable, be located in rooms where all windows and doors can be and shall be locked when staff are not present.

If equipment cannot be located within a room as described above, it shall, wherever practical and possible, be sited in an area which is always supervised and where members of the public have no cause to enter unless accompanied by a member of staff.

Equipment, which through necessity must be located in an area that is accessible to the public and that may be unsupervised for prolonged periods, shall be physically protected against theft. In addition, technical access to such equipment shall require the use of a physical token as well as a password.

All portable equipment shall be clearly and indelibly marked to indicate that it is the property of Health Intelligence. Where possible such equipment shall be locked away when not in use.

Portable equipment shall not be removed from the premises of Health Intelligence without written authority from a senior manager. This will only be granted on the understanding that:

- The employee assumes (where applicable) full responsibility and liability for any loss or damage
- No item(s) of equipment is left in an unattended vehicle
- Equipment shall only be used for 'bona fide'' Health Intelligence business
- Equipment shall only be used by Health Intelligence employees
- Equipment shall not be removed beyond the borders of the UK without written consent.

All equipment, including portable, shall be recorded on an asset register. The register shall record the individual to whom it is allocated or, in the case of non-portable equipment, the physical location of that equipment. All changes to allocation or location and any additional equipment details shall be recorded in the asset register.

Where members of the public are able to view the output on a screen, whether as a passer-by or by invitation, staff shall exercise great care to ensure that unauthorised disclosure does not occur. Care must also be exercised to ensure that passwords are not disclosed to other staff or members of the public who may be able to observe the entry of such passwords onto the system(s).

8 Mobile Computing and Teleworking

Scope

All the users of the Health Intelligence's wireless laptop computers, mobile access devices and endpoints are within the scope of this procedure. This includes laptops and mobiles.

All teleworkers who use Health Intelligence's or their own resources to connect to the Health Intelligence's facilities are subject to the requirements of this procedure.

Note – supplementary guidance is provided in QMS2321 - Laptop, Mobile Phone and Portable Media Policy.

Responsibilities

The IT Manager is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure.

The IT Manager is responsible for the configuration of required computing equipment.

The IT Manager is responsible for network configuration and, where agreed, for providing remote network connectivity and user support.

Procedure

Health Intelligence requires specified firewalls (Windows and Cisco firewalls), anti-malware software, and automatic updating facilities to be enabled, up to date and meet the corporate minimum standards on all laptops and computers.

Health Intelligence requires mobile devices (laptops, mobile phones, USB sticks and other similar memory devices) to have a password protection where appropriate/possible and to be encrypted following industry standards.

Health Intelligence requires that laptops are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft this is reported immediately as in Section 6.9.

Health Intelligence requires users to ensure that all the most recent operating system and application security-related patches, fixes and updates have been installed.

Health Intelligence requires users to comply with the Company's requirements on the means of connecting to public access points and accessing the Health Intelligence's information.

Health Intelligence requires users to act with care in public places so as to avoid the risk of screens and confidential computer activity being overlooked by unauthorised persons.

Health Intelligence provides users with appropriate training and awareness to ensure that they understand the risks of wireless computing and that they understand and can carry out their agreed security obligations.

All remote workers and teleworkers working from home must use a security enabled wireless configuration where that is the preferred connection method and a secure connection (VPN) to the Health Intelligence's network. The IT Department supplies the necessary software and security settings.

Teleworker Security

Teleworkers must abide by the same principles outlined above. Any necessary changes to the network are made to ensure that the Health Intelligence's Access Control Policy is not breached by the teleworker.

The teleworker undergoes necessary training.

All teleworkers should be formally signed off.

9 Security Incidents

The process for managing Security Incidents is contained in QMS2302 - Security Incident Process and QMS2303 - Security Incident Form. This includes the procedure to be followed in the event of an actual or perceived security incident.

It is advised that you talk directly to your line manager or the Head of Operations and Security if you are aware of an actual or potential incident.

10 Social Networking and Blogging Policy

Advice on the use of social networking and blogging can be found in the document **'QMS4135 - Social Networking and Blogging Policy'**.

11 Corrective Action Procedure

Health Intelligence has a formal Corrective Action Procedure to log and deal with non-conformities or problems with processes, procedures and products. This can be found in Section 8.1 of the Document **'QMS2308 - Information Governance Framework Policy'**.

12 Commitment to Security Policy

I _____ confirm that:

- I have received a copy of 'QMS2301 - Security Policy – v20.0' dated 30th June 2018.
- I understand my obligations in securing patient privacy and in maintaining appropriate security in relation to the data and information which commute through my activities.
- I will inform the Head of Operations & Security of any query, point of concern or risk which may come to my attention whilst undertaking my duties.

Signature _____

Date _____