Forward Clinical Ltd / Pando App Data Protection Policy

1. Data Protection, Confidentiality & Disclosure

As a business that processes sensitive personal data, relating to patients as well as users, the proper management of data is critical to all operations carried out by Forward Clinical Ltd. Systems, processes and policies that ensure we maintain the confidentiality of each patient and user's personal and sensitive information must therefore be an integral part of Forward Clinical's management structure in order to maintain continuity of its business, legal compliance and adhere to NHS information security and information governance regulations and policies. It is the responsibility of all Forward Clinical Ltd staff without exception to safeguard the confidentiality and security of all personal data.

1.1 What is personal and sensitive information?

According to the Data Protection Act 2018 and the EU General Data Protection Regulation (2016), data is information that:

"(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)."

Personal data is further classified by GDPR as:

"data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

GDPR also has special provision and conditions for the management and processing of sensitive personal data, referred to as special categories of data. These special categories include:

"personal data revealing 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.

Every use of personal identifiable information must be lawful and additional safeguards must be put in place when collecting, storing, sharing, and destroying sensitive personal data.

1.2 Data Protection Impact Assessments (DPIAs)

Privacy Impact Assessments are now referred to as Data Protection Impact Assessments under GDPR. This policy mandates the use of DPIAs, which are to be used to ensure that any new or amended policy, processes, procedure, or activity that involves the use of

personal information, sensitive personal information, is appropriately assessed to establish and record how this impacts on the data subjects and to recommend appropriate action to mitigate this impact.

DPIAs are now mandatory in England (United Kingdom) for new systems (IT or otherwise), processes, projects, policies or technologies which involves the processing of personal and/ or sensitive data.

1.3 Legal and professional obligations

Forward Clinical Ltd is required to meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within this policy are primarily based upon the Data Protection Act 2018 (DPA), EU General Data Protection (2016) and the NHS Code of Practice: Confidentiality (Code of Confidentiality) as well as requirements set by the NHS Information Governance Toolkit, now known as the Data Security & Protection (DSP) toolkit. These key standards cover the security and confidentiality of personal information within the NHS, United Kingdom and the European Economic Area.

Forward Clinical Ltd holds and processes information about its employees, users, their patients and other individuals for various purposes (e.g. the effective management of patient healthcare data or; for administrative purposes such as our staff payroll). To comply with the Data Protection Act 2018 (DPA) and the EU GDPR personal identifiable information must be collected and used fairly, stored safely and not disclosed to unauthorised persons. The DPA and Code of Confidentiality apply to both manual and electronic data.

Our organisation also has a duty to comply with additional guidance issued by the Department of Health, the NHS Executive, Monitor, and other professional bodies. All NHS providers and employees have a duty of confidence to patients and colleagues under common law.

The failure of our organisation, and/or employees or subcontractors to comply with relevant legislation could potentially result in investigation by the Information Commissioner's Office, with the possible risk of significant fines. Compliance with the policy will provide assurance to the our senior management, healthcare providers such as NHS Trusts and to individual patients that all personal and sensitive information processed by Forward Clinical is dealt with legally, securely, effectively and efficiently, in order to help our users deliver the best possible care to their patients.

Forward Clinical Ltd will establish and maintain policies and procedures to ensure compliance with the requirements contained in the NHS DSP Toolkit and the equivalent to be released in line with GDPR.

2. Scope

This Policy applies to Forward Clinical and all employees, senior managers, directors, contractors, third party partner organisations, and suppliers.

This policy covers records held and processed by Forward Clinical in any medium. Our organisation is responsible for its own records under the terms of the DPA/GDPR and it has registered itself as a Data Controller to the Information Commissioner.

This policy covers all aspects of information within the organisation, including (but not limited to):

- Patient/staff/client/service user information
- Personal information
- Organisational information

This policy covers all aspects of handling information, including (but not limited to):

- Structured and unstructured information record systems – both paper and digital
- Transmission of information – email, post, fax and telephone
- Information systems managed and/or developed by, or used by Forward Clinical

This policy covers all information systems purchased, developed and managed by, or on behalf of, the organisation and any individual, directly or otherwise engaged by the organisation.

3. Employee Responsibilities

As an employee of Forward Clinical Ltd you are subject to an obligation of confidentiality to all personal, sensitive and commercial patient information processed by the organisation and as such you must adhere to the DPA, NHS Caldicott Guidelines and NHS Information Security Procedures, which form part of all employee Terms and Conditions of Employment. All staff must sign a copy of the organisation's Data Protection, Confidentiality and Information Security Declaration without exception.

Subcontractors and employees of external organisations who are provided with access to any personal, sensitive or commercial information processed by Forward Clinical Ltd must agree and sign this declaration and a suitable contractual arrangement must be in place to protect and indemnify the organisation against improper use.

Although technical safeguards are in place to prevent Forward Clinical Ltd employees accessing any readable end-customer patient information – while you are at work you may occasionally have access to information about users, colleagues and/or the business. You may come in to contact

with this type of information during the course of your work or simply see, hear or read something while you are working or providing technical support to a clinician using our Pando App.

Circumstances may occur where you believe that a duty of care, either to the patient or to the staff member overrides the duty of confidentiality. In these circumstances you must discuss the matter with your supervisor/line manager in the first instance, or escalate it to the next senior manager and/or, where practicable, obtain advice from the organisation's Information Governance Manager. The discussion and outcome must be thoroughly documented and retained for future reference.

A copy of these documents must be provided to the Information Governance Manager for audit purposes. Otherwise, you must keep this information confidential.

Any unauthorised disclosure of personal or sensitive information by a member of staff may be considered as a disciplinary offence and could be subject to a disciplinary procedure.

This policy, and its supporting standards and work instructions, are fully endorsed by the Senior Management team through the production of these documents and their approval.

4. Management Responsibilities

4.1 The Joint CEOs (Chief Executive Officers)

The Joint Chief Executive Officers (CEOs) have ultimate responsibility for the Data Protection, Confidentiality & Disclosure Policy within the organisation. Implementation of, and compliance with this policy is delegated to Head of Information and overseen by the members of the Information Security Advisory Group (ISAG).

4.2 SIRO (Senior Information Risk Owner)

The SIRO is a board level individual responsible for the strategic management of information security and, specifically, to represent information governance and data security to the rest of the board and to provide advice and guidance to the Senior Management Team on the implementation of this policy.

The current SIRO is Philip Mundy who is also a co-CEO.

4.3 IG (Information Governance) Manager and Data Protection Officer

The Informatics Lead is designated as the organisation's Data Protection Officer and is responsible for supporting the day to day IG function and works closely with the SIRO on confidentiality and Data Protection matters such as, training, investigations and IG Compliance. The present IG Manager and Data Protection officer is Claire Robinson.

The Data Protection Officer can be contacted at ***dpo@hellopando.com***

4.4 ISAG (Information Security Advisory Group)

The Information Security Advisory Group (ISAG) is a team that comprises representatives from all relevant sections of Forward Clinical Ltd.'s Senior Management Team, in-house IT staff and NHS employees – and is responsible for identifying and assessing security requirements and risks.

4.5 Senior Management Team

Data Protection procedures will vary from department to department and across disciplines. It is the responsibility of Senior Managers to ensure adequate and compliant procedures are developed to handle personal data and sensitive personal data.

This includes the responsibility to ensure that new systems or procedures used for the processing of personal and sensitive personal data are carried out with reference to the ICO's DPIA Code of Practice.

Senior Managers may delegate the day to day running of operational procedures, but may not delegate overall responsibility for the handling of personal data and sensitive personal data within their departments.

4.6 Information Asset Owners (IAO)

Each Senior Manager is identified as an organisational IAO. IAO's assume particular responsibility for the digital information systems (information assets) which process personal, sensitive or commercially sensitive information for our end-customers.

The IAO will ensure each information asset 'owned' by them, has an assigned IAA (Information Asset Administrator). The IAO must identify an appropriate member of staff as the IAA for any new electronic systems before the procurement, development or introduction of the new system commences.

4.7 Information Asset Administrators (IAA)

The IAA's role is to either procure, develop, deploy or manage a digital information system and this person's job function is typically technical or IT-related in nature.

The IAA will assume responsibility for the compliance with the DPA (Data Protection Act) and this policy of the information asset for which they are the nominated IAA. However all employees involved in the procurement, development or introduction of such information assets, including customer health information systems, must ensure that best practice principles are incorporated during the procurement and design stage. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

Where for whatever reason an IAA has not been identified, the manager of the team procuring or developing the information assets must inform their IAO and the Information Governance Manager of the team introducing the new asset.

The IAA will also be responsible for ensuring that the information asset is audited against this policy before implementation and on a regular basis; at least annually. These audits must be provided to the IAO for approval.

5. Regulatory Compliance

Forward Clinical has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It is essential that patient identifiable information (PID) is handled, processed and released in a strictly controlled manner. This document sets out the organisations policy for the management of confidential information.

5.1 The Data Protection Act 2018 and EU General Data Protection Regulation 2016

The lawful and correct treatment of personal information is vital to the successful operation of, and maintaining the confidence with the organisation and the end-customer individuals with whom it deals with. Therefore, Forward Clinical Ltd will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair processing of patient and user information by our systems
- Meet its legal obligations to specify the purposes for which information is used by our users
- Collect and process appropriate information and only to the extent that it is needed;
- Use compliant process to fulfil operational needs to comply with any legal requirements;
- Ensure the quality of information management systems provided to end-users is 100% accurate;
- Apply strict record management techniques to help users determine the length of time patient information is held and help our customers establish a compliant disposal process where necessary;
- Audit compliance with legislation and appropriate standards and escalate findings to the IAO and ISAG.
- Ensure that the rights of people (users and patients) about whom information is held can be fully exercised
- Take appropriate technical and organisational security measures to safeguard personal and sensitive personal information;
- Ensure that personal information is not transferred outside the UK (United Kingdom) or EEA (European Economic Area) without suitable safeguards, such as data encryption in transit and at rest.

5.2 Notification to the Information Commissioner

Forward Clinical Ltd is a notified 'controller' of data. The Data Protection Act 2018 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence.

Forward Clinical's ICO registration number is ZA237861.

Personal information may be processed by Forward Clinical to enable it to provide a service in which we design, test and demonstrate software; promote our services; maintain our accounts and records and to manage our staff. We process information relevant to the above reasons/purposes. This may include:

- Personal details
- Family details
- Lifestyle and social circumstances
- Goods and services
- Employment and education details
- Financial details
- Information necessary for the development and test of software

We also process sensitive classes of information that may include physical or mental health details; racial or ethnic origin; religious or other beliefs. We process personal information about our clients, employees, suppliers and individuals necessary for software development.

We sometimes need to share the personal information we process with the individual them self and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act/GDPR. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

- Family, associates and representatives of the person whose personal data we are processing
- Suppliers and service providers
- Professional advisers and consultants
- Financial organisations
- Credit reference agencies
- Debt collection and tracing agencies
- Employment and recruitment agencies
- Central government

The responsibility of maintaining the organisation's ICO registration lies with the Data Protection Officer who will ensure that all uses and disclosures of personal data are specified within the registration.

It is also, essential that the organisation's registration is kept up to date, Managers and all staff are responsible for informing the Information Governance Manager of any new uses of

personal identifiable information or sensitive information. For further guidance on the type of personal data the organisation collects and the use and sharing of information refer to our Data Processing Policy.

5.3 Confidentiality: NHS Code of Practice & the Caldicott Committee Report

In 1997 the Caldicott Committee introduced stringent guidelines in the recording, access and use of personal data within the NHS. This document was called the Confidentiality: NHS Code of Practice. This Code mandated Each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012. The mandate covers all organisations that have access to patient records.

5.4 Caldicott 2 Report

The original Caldicott Report, established six principles for NHS bodies (and parties contracting with such bodies) to adhere to in order to protect patient information and confidentiality. Despite these principles, and the provisions of the Data Protection Act 1998 that followed, there were almost 200 serious data protection breaches reported to the Information Commissioner relating to NHS bodies in 2012. Against this background, it is acknowledged that NHS staff have become more reluctant to share information given the potential sanctions in doing so inappropriately.

Accordingly, the government commissioned Dame Fiona Caldicott to conduct a further Information Governance Review (the “Review”) which was published at the end of April 2013.

“The duty to share information can be as important as the duty to protect patient confidentiality”. The Review highlights that for health professionals to act in a patient’s best interest, they need to have all the available information about the patient to do so. However, it is acknowledged that current information governance provisions (or at least the interpretation of them) have led to information not being shared when it should be. Accordingly, Recommendation 2 of the Review specifically states that:

“for the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Further, the Review also recognises that there are certain situations when sharing of personal information is not just preferable, but vital. An example given of this is within public health medicine in order to identify people at risk during an outbreak of an infectious disease, or to carry out health improvement and research exercises.

5.5 Caldicott Guardian Registration

All NHS Trusts are required to maintain and update their Caldicott Guardian registration with NHS Digital. This registration function is carried out by an NHS Trust IG Manager. Forward Clinical recognises this NHS role as pivotal to the success of our Pando App roll-out within each NHS Trust and as part of our preliminary customer engagement and IG (Information Governance) assurance process this Data Privacy Policy document should be sent for review by the Caldicott Guardian.

5.6 Caldicott Principles

The Caldicott principles were recommended by the Caldicott Committee as a guide for the NHS for the use of, and transfer of patient identifiable information. A seventh principle was added following the Caldicott 2 Report. The seven principles provided by the Caldicott Report are the baseline for good practice:

1. Justify the purpose for using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect confidential information

6. Consent

In order for our Forward users (e.g. NHS health professionals) to be able to lawfully process the personal or sensitive personal information of an individual, they must first obtain freely given, informed consent from the subject. This is applicable to both NHS employees and patients. This is fairly straightforward to manage for NHS employees, but due to the very nature of healthcare this is not always that case when dealing with the information of patients. Therefore, where patients have consented to healthcare from an NHS provider, it is considered reasonable to argue that consent has been ‘implied’, similarly research has consistently shown that patients are normally content for information to be disclosed to other organisations in order to provide that healthcare.

GDPR raises the bar for consent and fair processing of data. Under GDPR, users data will be processed by Forward Clincial Ltd on the basis of consent, explicitly given by users on registering for the Pando app (sections 6(a) and 9(2)(a)).

For the processing of patients data, which is considered a special category of data, processing is based on sections 6(a) and 9(2) (h).

Notwithstanding this, it is still very important that reasonable efforts are made to ensure that our Forward users inform their patients – so patients understand how their information is to be used on systems to support their healthcare and that they have no objections.

Where this has been done effectively, consent can be implied, providing that the information is shared no more widely than absolutely necessary, only information that is adequate, relevant and not excessive is shared and that "need to know" principles are enforced.

Patients entrust our NHS Trust end-customers and us with, or allow us to gather extremely sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence with a legitimate expectation that NHS staff and any contracted information systems providers will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS and Forward Clinical Ltd, provides, and is seen to provide, a confidential service.

Personal or sensitive personal information that can identify any individual must not be used or disclosed for purposes other than for which it was provided without the individual's explicit consent, some other legal basis or where there is a robust public interest or legal justification to do so.

Anonymised information is not confidential and may be disclosed in some circumstances. Guidance contained in Confidentiality: NHS Code of Practice (November 2003) should be followed.

6.1 Consent & Compliance with the DPA 2018, GDPR and Code of Practice: Confidentiality

In order for our end-customers to promote a healthcare service which is open, transparent and sharing (ref. Caldicott Principle No. 7: "The duty to share information can be as important as the duty to protect confidential information") many healthcare providers are encouraged by the NHS to develop a series of leaflets, posters and website pages which provide patients with specific information about how their information will be collected, stored, used and shared with partner organisations for the provision of continued healthcare.

On the assumption that patient consent to data sharing continues to be 'implied' under NHS England's current practices (inc. NHS Mail) then Forward Clinical Ltd is satisfied that NHS England's existing patient awareness programmes are adequate for meeting the consent and compliance with the DPA, GDPR and Code of Practice: Confidentiality.

6.2 Individuals who prohibit the Sharing or Processing of Personal or Sensitive Information

In accordance with GDPR, data subjects have the right to object to the processing of their personal and/or sensitive data that is likely to cause or is causing damage or distress.

Where an NHS Trust receives written instruction from an individual patient that they hold records on that they wish to object to the processing of their personal data, this objection will be considered by the Trust's own IG (Information Governance) Manager and where appropriate, their Caldicott Guardian. We understand that NHS Trusts are obliged to comply with such requests from individual patients. Forward Clinical Ltd will take measures to comply with this cease request for any data currently held however Forward Clinical Ltd relies also on the user's responsibility for compliance to ensure no further data entry and processing is carried out.

6.2.1 Impact on the provision of health care

Most health and social care providers do not work in isolation and tend to collaborate with a number of other NHS organisations and independent treatment centres to provide their patients with the best possible care. In order to do this, patient information needs to be shared securely to provide care in local, central and peripheral locations.

If a Forward user's patient chooses to prohibit this information from being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided to them is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Again, Forward Clinical Ltd is not empowered as a data processor to handle processing 'cease' requests of this nature as it is the Forward user's responsibility for compliance.

6.2.2 Formal authority by the Courts

The law may require that our NHS customers and/or Forward end-users disclose or report certain types of personal or sensitive information, but that is only done after formal authority by the Courts or by a qualified health professional. Examples include reporting a serious crime which involves murder, manslaughter rape, treason, kidnapping, child abuse or infectious diseases that may endanger the safety of others, such as meningitis or measles, but not HIV/AIDS. On occasion our organisation may be legally required to comply with technically assisting in such information disclosure requests but only after consultation with our end-customer's IG (Information Governance) Manager, unless restricted by formal authority from the Courts.

7. Working and Sharing Information

In order for our NHS Trust end-customers to remain compliant with the Data Protection Act 2018, GDPR (2016), "Confidentiality: NHS Code of Practice and Information Security Regulations all 3rd Party Contractors, System Suppliers and Healthcare Partnership Agencies must formalise, document and sign legally binding agreements to permit the sharing of personal and sensitive personal information" – the following are examples of documents which can be supplied upon request:

- Contract between the healthcare provider and Forward Clinical Ltd
- Information/data sharing/data processing agreement between Forward Clinical Ltd and NHS Healthcare Partners

7.1 Data Protection Impact Assessment (DPIA)

Before entering into any agreement with Forward Clinical to process or share information on our platform, a draft Privacy Impact Assessment (PIA) can be supplied upon request.

There are a number of ways in which healthcare providers may have access to information or other information held in our systems, which will help determine how extensive our PIA needs to be. For example – accessing our infrastructure via an NHS Trust's or private healthcare provider's secure Wi-Fi network from the Forward will see different considerations to app connections over a standard 3G/4G/5G internet connection from a clinician's personal Smartphone device. It is essential that the nature and level of access is determined before the DPIA is formally conducted and before the information governance elements of the contract are completed.

7.2 Confidentiality and non-disclosure clauses

It is required that all contracts with Forward Clinical Ltd employees, third parties or sub-contractors contain appropriate confidentiality and non-disclosure clauses.

7.3 Security controls of private information

It is essential for our customers to be informed and know what security controls we have in place to protect the privacy of patient information, such as;

- Security controls, policies and training
- Staff screened prior to commencing employment
- Staff trained in Caldicott/confidentiality and data protection
- The customer's own Information Asset Administrator (IAA) responsible for the completion of the DPIA, which must be approved and sign off by their Information Asset Owner (IAO).

In order to protect our customers and mitigate any risks all contracts or protocols may contain the following:

- Ownership of information & arrangements for retention or destruction following any decommissioning of our service/system
- Releasing personal data within a statutory number of days to comply with subject access received by our customer
- The facility to extract personal data in an anonymised or pseudonymised format
- Audit of Systems, access, user account controls and reporting anomalies
- Overview of Technical Solutions
- Confidentiality
- Data Protection including parameters of disclosure of personal/corporate information
- Access control framework
- Error correction processes
- Secure transit and storage of patient identifiable Information
- Key contacts
- Liability
- Information security standards including statement of compliance
- Details of processing of data outside of the UK
- Incident reporting procedures
- Security transfer details
- Retention schedule for information

8. Ensuring safe transfer of private information

Every member of staff has an obligation to confirm the right to share information and where applicable, to request proof of the identity of the recipient, before confidential personal and or sensitive information is passed on. Every member of staff is personally responsible to take precautions to ensure and maintain the security of confidential personal information both whilst it is in their possession and when it is being transferred from one person or organisation to another.

The following is a list of recommended procedures to ensure the safe transfer of private information (note: The Forward encrypts all data transported between server and mobile app in transit and at rest on our servers). The following applies to all other types of private information handled by the organisation:

- Envelopes must be securely sealed, clearly addressed to a known contact and marked “Confidential” and “Addressee only”. A return postal code should also be marked on the envelope.
- Telephone validation or “call back” procedures must be followed before disclosing information to someone you do not know to confirm their identity and authorisation (even when receiving a call from someone claiming to be a fellow employee).
- Fax transfer is not safe and should be avoided wherever possible.
- Data held on disk or removable media of any type must be Bitlocker encrypted and the physical security of the device must be protected.
- E-mailing any confidential information is only permitted via the use of secure networks, or if it is appropriately encrypted. Refer to our Information Governance, IT & Communications Policy.
- Confidential information must not be transmitted via the Internet without it being encrypted, or where system-to- system networks are known to be insecure.
- When anonymised or pseudonymised information is shared, care must be taken to ensure that the method used is effective and individuals cannot be identified from the limited data set e.g. age and postcode together could be sufficient enough to reveal an individual’s identity. Refer to the Information Commissioner’s Anonymisation Code of Practice.

9. Private information use in testing & development

The Information Commissioner’s Office advises that the use of personal data and sensitive personal data for system testing must be avoided wherever possible. Our systems administrators and developers must develop alternative methods of system testing. Only where is has been proved that there is no practical alternative to using live data for this purpose, can live data be used. In this case, the use of this data must be fully risk assessed and approved by the IG (Information Governance) Manager and where patient data is included, also by the CISO (Chief Information Security Officer). This must be undertaken before commencement of any testing/development.

Should the Information Commissioner receive a complaint about the use of personal data for system testing or development, their first question to our organisation would be to ask why no alternative to the use of live data had been found. Compliance with the above will prove

assurance that appropriate steps will have been taken to establish if an alternative exists and if not, appropriate approval have been received before proceeding.

At present, Forward Clinical Ltd does not use live patient data for the purposes of development or testing.

9.1 Key Risks to Personal Data in System Testing & Development

There are a number of general risks that exist whenever system testing is undertaken using live data and/or a live environment. These are:

- Unauthorised disclosure of data
- Unauthorised access to data
- Intentional corruption of data
- Unintentional corruption of data
- Compromise of source system data
- Loss of data
- Inadequacy of data
- Objections or complaints from data subjects
- Potential clinical risk

Any of the above risks can also lead to financial loss to the organisation and/or the person the information relates to. Such action could significantly damage our reputation.

10. Consequences of a breach of this policy

10.1 Disciplinary

A deliberate breach of this Data Privacy Policy will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

- Unlawful disclosure of Personal Data and Sensitive Personal Data
- Inappropriate use of Personal Data and Sensitive Personal Data
- Accessing patient or staff personal data including medical records in the absence of a legitimate professional relationship
- Misuse of the Personal Data and Sensitive Personal Data which results in any claim being made against the organisation

10.2 Criminal Offence

Section 170 of the Data Protection Act 2018 builds on section 55 of the DPA 1998 which criminalised knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data. The provision was most typically/commonly used to prosecute those who had accessed healthcare and

financial records without a legitimate reason. Section 170 adds the offence of knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller. There are some exceptions: for example where such obtaining, disclosing, procuring or retaining was necessary for the purposes of preventing or detecting crime. Section 170 (2) and (3) set out the defences to Section 170 (1).

Under EU GDPR the maximum penalty has significantly increased to the greater of 20 million euro, or 4% global annual turnover.

11. Mandatory Training

All employees must complete both Information Governance and Security training annually. Data Protection, security and confidentiality will form a major part of the course content, which will be offered to all employees via one-to-one sessions with the Data Protection Officer and via a CBT (Computer Based Training) package. For any member of staff who for whatever reasons (such as disability) the CBT is not appropriate, alternative methods of training will be made available.

The organisation will ensure that training courses/presentations will support this policy. The training will ensure general awareness of Data Protection and NHS Caldicott Principles with more specific training for IAOs and IAAs and other staff groups.

11.1 Staff induction

All staff must complete annual training and assessment in data security and awareness relevant to their level of data access and responsibility. All staff will be provided with dedicated Information Security, Data Protection, NHS Caldicott and Confidentiality training.

11.2 Departmental Induction

Each new member of staff will be given appropriate training materials as part of their induction pack from their departmental manager. The information provided will be fully explained.

Managers and supervisory staff are responsible for ensuring that new staff and those returning after a significant period of absence are provided with a locally based information governance orientation training which should include but is not limited to:

- Postal procedures: internal and external post
- Destruction of confidential waste and data
- Using email to share information outside the organisation
- Leaving telephone messages
- Access to secure areas
- Safe and secure transportation of private data
- Appropriate access to confidential information

- Challenging visitors attempting to access our site
- Briefing new employees on business continuity plans

11.3 Data Security, Confidentiality & Protection Awareness

The Data Protection Officer will ensure all Forward staff are given appropriate training in data security and awareness, relevant to their role and their level of data access and responsibility.

12. Monitoring Compliance & Reviews

Compliance with this policy will be monitored through regular confidentiality audits carried out by the IAAs (Information Asset Administrators). Any incidents or potential concern will be raised with in the first instance with the IAOs (Information Asset Owners) and in the second instance the IG (Information Governance) Manager/ Data Protection Officer and/ or CISO (Chief Information Security Officer). All potential breaches will be investigated in line with the Information Security, IT and Telecommunications policy.

All audits will be carried out in accordance with the ICO Confidentiality Audit Guidance: ICO

12.1 Staff knowledge

Staff knowledge and awareness will be audited by the IG Manager annually using an automated questionnaire. The results will be collated to form a report to the CISO and the ISAG (Information Security Advisory Group) members.

12.2 Customer experience

Customer experience will also be monitored via a personal survey managed by the IG Manager/Data Protection Officer. This survey will also include the evaluation of promotional emails and Forward reviews.

Data from survey will be analysed and compiled by the IG Manager/Data Protection Officer and reports submitted to the Senior Management team.

12.3 Data Protection & Confidentiality Compliance Visits

The IG Manager/Data Protection Officer will carry out compliance visits throughout the organisation and with external service suppliers to be fed back to the Senior Managers, CISO and ISAG.

12.4 Communication & Implementation

This policy is to be made available to all Forward Clinical staff and observed by all members of staff – whether they are management, technical, clinical or administrative.

12.5 Review

This policy and associated documents will be reviewed annually by the IG Manager/Data Protection Officer, and every three years by the ISAG or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from NHS Digital, NHS England, NHS Scotland, NHS Wales and HSCNI (Health & Social Care Services in Northern Ireland).

This policy was last reviewed on 14th December 2019 by Forward Clinical's Data Protection Officer and was approved by the ISAG.