Basildon Road Surgery

Data Security and Protection policy

Reviewed by: Practice manager
Reviewed: March 20
Re-review: March 21

Data security and protection policy

1 Introduction and purpose

1.1 Basildon Road Surgery has a legal obligation to comply with all appropriate legislation in respect of personal and confidential information. The GP practice and staff understand the importance of data protection and confidentiality and the responsibility owed to patients, families, staff and business partners with regards to the way in which we process, store, share and dispose of information.

1.2 The Data Protection Act 2018, General Data Protection Regulations 2018 provide a framework for the management of all data from which individuals can be identified. It is essential that all staff are fully aware of their responsibilities for information they may come into contact with.

1.3 This policy supports the National Data Guardian, 10 data security standards for the submission of the NHS Digital Data Security and Protection Toolkit (DSPT).

1.4 From this point of the policy all personal, sensitive (Including special categories of data) and business confidential information will be referred to as personal and confidential data.

2. Scope

2.1 This policy applies to all staff at Basildon Road Surgery, including contractors, agency staff, locums, bank, voluntary or work experience staff.

2.2 This is inclusive of staff working at or for Basildon Road Surgery, including remote working.

3. Principles relating to processing of personal data

3.1 General Data Protection Regulations 2018/Data Protection Act (DPA) 2018 came into force on 25th May 2018 and sets out the principles that the practice, as a data controller, must adhere to when

processing personal information.

3.2 Pauline Clelland will take all reasonable measures to ensure full compliance with legal responsibilities for processing and handling personal data.

As a data controller of personal data Basildon Road Surgery shall register the practice processing activities with the Information Commissioners Office (ICO) and pay the annual fee for registration

Data Protection Act and General Data Protection Regulations (GDPR) 2018

Below are the principles of the Data Protection Act and GDPR.

Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation – data must be collected only for specified, explicit and legitimate purposes
Data minimisation – data must be adequate, relevant and limited to what is necessary
Accuracy – data must be accurate and, kept up to date. Inaccurate data must be erased
Storage limitation – data must only be retained for as long as is necessary in accordance with NHS England retention schedules
Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Integrity and confidentiality – data must be processed in a secure manner in line with cyber security principles laid out in the new data legislation
Accountability - the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles

Types of data

The Data Protection legislation defines personal data as information which relates to natural persons who;

- can be identified or who are identifiable, directly from the information in question; or
- Who can be indirectly identified from that information in combination with other information.

Personal data may include special categories of personal data or

criminal convictions and offences data.

Lawful basis for processing

Processing of personal data may only be carried out where there is a lawful basis for processing. The GP practice shall ensure that any personal data is processed in line with the lawful conditions.

Other legislation

There is a variety of legislation and information governance standards that apply to organisations that handle and manage personal data. These include, but are not limited to;

- NHS Code of practice
- Common law of duty of Confidentiality
- Caldicott Principles
- NHS Code of conduct
- NHS Code of practice records management
- Care Act 2014
- Mental Health Act 1983
- Computer misuse Act 1990
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- National Data Guardian Review for consent and opt-out

4. Accountability and governance

Having the right people engaged in data security and protection roles can make a significant difference and support the organisation and staff meet its legal obligations. The details below provide an overview of the roles and responsibilities within the GP practice.

Data Protection Officer (DPO)

It is a mandatory duty of the General Data Protection Regulations to appoint a Data Protection Officer (DPO) for public authority or body that carries out core activity includes large scale processing of special categories of data (which includes information relating to an individual's

health).

A Data Protection Officer (DPO) is required to operate independently and report to the highest level of management within the GP practice.

In line with the NHS National GP contract, Bexley Clinical Commissioning Group Data Protection Officer will provide a supporting role to GP practices across Bexley.

Data Protection Lead

The GP practice has an appointed Data Protection Lead. This role will oversee the day to day running of the practice data protection and security including, but not limited to;

- Monitoring compliance with GDPR and other data protection laws, relating to policies, awareness- raising, training and audits
- Advise on and monitor Data Protection Impact Assessments when implementing changes, new systems or projects relating to the GP practice
- Act as a point of contact for individuals relating to subject access requests, individual's rights or any other data protection related issues
- Act as the point of contact for the Information Commissioners Office
- Give due regards to any risks associated with processing operations and takes into account the nature, scope, context and purposes for processing
- Maintain the GP practice information asset register, data flow mapping register
- To review, development any processes to support data protection and security
- To review, update and publish the annual Data Security and Protection Toolkit
- Ensure fees and registration of the GP practice data processing activities are completed and remain up to date.
- Liaise with the nominated Data Protection Officer for the GP practice

The role of the Data Protection Lead GP practice has been appointed to Pauline Clelland. The Data Protection Lead will liaise with NHS Bexley CCG DPO for support and advice when it is necessary to do so.

Caldicott Guardian

Appointment of a Caldicott Guardian is a mandatory requirement for NHS organisations and GP practices. This individual plays a key role in ensuring that the GP practice and staff satisfies the highest practical standards for managing personal, sensitive and confidential information.

This role has the responsibility of ensuring that the data protection principles are fully embedded with the practice and will support staff to deliver these principles.

Basildon Road Surgery shall register the organisations Caldicott Guardian on the NHS Digital website so that the information is made available on the public register of Caldicott Guardians.

The Caldicott Guardian has responsibilities which include, but not are not limited to;

- Sign off of information sharing agreements, or protocols
- Overview and sign off of the GP practice Information Asset Register and Data Flow mapping
- Review and sign off any Data Protection Impact Assessments involving any projects, changes or new systems that impact on personal, sensitive or confidential information
- Review and sign off of any contracts or service level agreements that involve personal, sensitive and confidential information

Staff

All staff (including temporary, contractors, voluntary, locums and bank) shall understand the principles of the data protection laws to undertake their work in a manner that protects the confidential, personal and sensitive information they work with.

All staff shall acknowledge these responsibilities by signing a staff confidentiality agreement/contract.

All staff are responsible for the records they create and maintain in the course of their duties and are designated Information Asset Administrators (IAA). (See further guidance below regarding Information Assets)

All staff shall ensure that access to personal data and other information assets is appropriately controlled.

The GP practice shall maintain a record of staff and their current roles.

5. Data Security and Protection (DSP) Toolkit

5.1 The Data Security and Protection (DSP) Toolkit is an online self-assessment tool that allows the GP practice and other health care providers to measure their performance against the National Data security standards.

5.2 As an organisation that has access to NHS patient data and systems, the GP practice shall complete the DSP toolkit to provide assurance that they are practising good data security and personal information is handled correctly.

5.3 The GP practice shall submit this assessment prior to the 31st March each year. The submission of the annual DSP Toolkit supports the Care Quality Commission (CQC) 'Well Led' inspection framework.

5.4 Staff shall support the GP practice, by ensuring that they remain up to date with the relevant data protection and security guidance and complete the mandatory information governance training each year between 1st April – 31st March. (Data Security Awareness – Level one)

6 Data Protection Impact Assessments (DPIA)

The General Data Protection Regulations 2018 (GDPR) makes privacy by design an expressed legal requirement, under the term 'data protection by design and by default'. It refers to this process as a 'Data Protection Impact Assessments' (DPIA).

The GP practice has a Data Protection Impact Assessments (DPIA) guidance and template, which provides an effective way to comply with data protection obligations and meet individuals' expectations of privacy. It also allows the GP practice to identify any privacy risks, overcome problems at an early stage of implementing new systems, projects or change.

Staff responsible for implementing change shall ensure that a DPIA is completed to address any risks to privacy of personal data at the start of any changes introduced.

The DPIA assessments that are completed shall be reviewed and signed off by the GP Practice Data Protection Lead and Caldicott Guardian. Once DPIA has been signed by the practice, they must be reviewed by the NHS Bexley CCG DPO.

7. Training and awareness

Staff shall be provided with information in order to understand the principles and importance of data security and confidentiality. It is a mandatory requirement that all staff remain up to date with the current legislation and are asked to complete a mandatory on-line training module on a yearly basis. The GP practice manager shall maintain a record of staff roles and the training completed.

Staff Induction

Staffs that commence employment at the practice will be given an induction, which includes guidance on data protection and security.

Annual mandatory training

Mandatory data security awareness training shall be completed by all staff within each year (01 April – 31 March). This training is made available on the E-Learning for Health online training portal and supports the standards of the Data Security and Protection Toolkit.

Enhanced training

Learning opportunities for leaders and key data security roles should be appropriate to their role and accountability. Additional training should be carried out to enhance knowledge and understanding of data protection and security responsibilities.

Additional awareness

The GP practice will provide staff with additional information and awareness through policies, guides, bulletins and team meetings.

8. Security measures and access controls

Network and physical security measures exist to support the secure handling and storage of the personal and confidential data that are created and handled at the GP practice.

These security measures in place guard against:

- Unauthorised access to alternation, disclosure, destruction of data
- Accidental loss or destruction of data

Protection is needed against both external threats such as theft and internal threats such as inappropriate access by staff.

Access controls

Staff will be provided with access to the GP ICT network and clinical system which are appropriate to their level and roles of responsibility. The GP practice shall be responsible for ensuring that access controls and roles to the relevant systems are kept up to date.

Staff shall understand their responsibilities for the use of these systems by ensuring that passwords and smartcards are kept safe and not shared.

All ICT equipment shall be password protected and mobile devices must be encrypted.

Backups of systems and data shall be taken at regular, pre-determined intervals in accordance with the written procedures for each system.

NHS Bexley CCG will ensure that appropriate ICT disaster recovery plans are in place, tested and reviewed regularly, to enable PC desktop and clinical system access at the practice are restored as quickly as possible. The GP practice also has its own business continuity plan which provides further details of processes and actions that must be put in place in the event of an incident where normal GP practice service may not be possible.

The copying of personal or confidential data to any other form of portable media devices is strictly prohibited. Where this cannot be avoided, for example if it is necessary to take records on visits to patients home, procedures for safeguarding the information are in place through password protection and encryption.

Authorisation for taking records of site must be obtained from the GP practice Caldicott Guardian.

Staff must not rely on the screen saver function of the PC when leaving their workstation. The PC must be locked when being left unattended by using CTRL-Alt and Delete (or Windows symbol and L). PCs must be locked at the end of the day, unless there is specific agreement from the NHS Bexley CCG ICT department for specified ICT equipment to remain logged on.

Physical security

There must be physical controls that exist in the practice to support data protection. This includes lockable doors, windows cupboards,

clear desks and key coded locks in order to prevent access to personal and confidential data.

The practice must ensure that cabinets that contain confidential information are not in public areas and are always kept locked and offices are locked. Offices must be locked at the end of each day.

Staff shall ensure that any documents that are scanned or printed are not left unattended on the device.

Staff shall remain vigilant to ensure that personal and sensitive information remains secure at all times.

Cyber security

A cyber-attack is a malicious act by hackers/criminals to damage or destroy a computer infrastructure network or personal computer device. Cyber-attacks against organisations are a constant occurrence and the impact and sophistication of these acts continues to grow.

Staff must remain vigilant to cyber-security threats and take steps to avoid problems or information breaches occurring. Staffs that suspect they have received an email which may contain malicious content or viruses should contact NHS Bexley CCG, ICT Department immediately on 020 8 298 6166.

Staff must ensure that the do not send or forward the email on to the ICT department or other members of staff.

GP practice desktop cyber and anti-virus services are supported by NHS Bexley CCG ICT department who are registered members of CareCERT and Window Anti Threat Protection (ATP)

Passwords

Passwords shall be used to ensure that access to IT systems and devices and information is controlled and restricted to approved and authorised users only.

Unique passwords shall be created and used by staff for each system to which they require access.

Passwords must be kept secure at all times and must not be shared, unless a specific joint administrative system password has been authorised by the Practice Manager or NHS Bexley CCG ICT department.

Default passwords changes are set on the GP practice clinical system

every 40 days and NHS Mail default password is every 365 days. Further information regarding NHS Mail passwords can be found on the NHS Mail website.

Registration Authority (Smartcards)

To enable healthcare professionals and authorised personnel to gain access to clinical IT applications; staff are required to register for a Smartcard.

Authorisation for a Smartcard shall be granted by the Practice Manager or Lead GP who is an authorised sponsor for the GP Practice. Staff will be designated with the level of access appropriate to their role and duties.

Registered users will be provided with a Smartcard which will have a unique ID pass-code. All staff have a duty to keep their Smartcard and ID pass-code secure at all times.

The registration process for Bexley GP practices is operated at a local level by NHS Bexley CCGs ICT department who are authorised registration authority agents and who shall conform to the national registration policy and guidance.

Staff shall read and acknowledge the Terms and Conditions for Smartcard usage when registering for the Registration Authority service. Failure to adhere to these terms may result in access to the system being revoked or disciplinary proceedings and/or criminal prosecution.

Mobile devices

Staff with the responsibility for mobile devices which includes, laptops, iPads, VPN tokens/access, and USB sticks shall ensure they are aware of their responsibilities for the use of the equipment, along with the security and any health and safety issues related to such devices.

Any purchase of mobile devices for GP practice use will be made through the NHS Bexley CCG ICT department to ensure the appropriate security measures are in place.

Unsupported systems and devices

NHS Bexley CCG will fulfil its obligations in line with the CCG practice agreements to ensure that no IT systems deployed and supported by NHS Bexley CCG are unsupported. The ICT support service ensures the appropriate anti-virus, patch management, system upgrades and access controls are in place meet data security and protection

standards.

Basildon Road Surgery must ensure that they have no unsupported IT systems or devices. Practices should always consult the NHS Bexley CCG ICT Department if in any doubt.

E-mail

Staff members of Basildon Road Surgery will be provided with an NHS Mail email mail account or access to an NHS Mail shared mailbox. All emails transmitted should be encrypted.

NHS Mail provides a secure method of exchanging personal data with other NHS Mail email account users or other NHS Mail secure domain user accounts. (a full list of secure domain accounts is available on the NHS Mail website)

NHS Mail users also have the ability to send secure encrypted emails to non-NHS users by using the NHS Mail [SECURE] encryption functionality. Further guidance to support this process shall be sought via the NHS Mail website.

When exchanging personal data by email, practice staff must be vigilant to its security. Ensuring that the correct safe haven processes are carried out and only the minimum amount of data is shared is critical.

Staff shall ensure that the exchange of personal data via NHS Mail is done so in line with NHS Mail guidelines.

Personal notes

All notations taken during the official work undertaken on behalf of the GP practice regarding personal data is subject to access under the Data Protection Act/GDPR. Staff shall ensure that notations in relation to personal data or business related information is appropriately stored.

Post

Ensure correspondence containing personal data is

- Marked private and confidential
- Marked with the name of the recipient and the sender
- Are delivered in a secure manner
- When sending by secure delivery, are confirmed received

Telephone

All staff shall be vigilant when using the phone to discuss personal information. Care should be taken to restrict the ability to be overheard.

Care should be extended to messages on answering machines; both the security of the message on the machine and the playback of the message should not reveal any confidential information or details that may breach individual's privacy.

Social Media

Social media can be a resource for doctors and staff; however staff should always consider protecting themself and other privacy on-line.

There are many benefits to using social media, but the legal consequences or improper use can be serious. Inappropriate or unintentional disclosure of information will be seen as a data breach and can result legal action or penalties by the Information Commissioner's Office (ICO).

Instant messaging software

Instant messaging is a useful tool in supporting the delivery of direct care, however there are some important data protection considerations surrounding the use of these systems.

The security features of an app can help ensure that your message stays private between you and the intended recipient or recipients. Security features are particularly important if your message contains a patient's identity or information that could potentially be used to identify a patient.

NHS England has released guidance 'Information governance considerations for staff on the use of instant messaging software in acute clinical settings' which supports staff when choosing instant messaging applications.

Video conferencing

With the advances in technology and the use of video conferencing for managing consultations being more widely used, staff must always consider security and privacy when using these facilities.

Fax

NHS England guidance supports the disbanding of fax machines and should therefore not be used with effect from April 2020. (Department of Health and Social Care Secretary bans fax machines in NHS)

Monitoring and audits

The Data Protection 2018 states that "*personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

To protect the integrity and confidentiality of personal data, Basildon Road Surgery has the capabilities and capacity for activity within the practice and systems to be monitored and recorded.

Monitoring and audit checks can include the following;

- Inappropriate access to clinical and practice systems
- The security of smartcards (i.e. smartcards left unattended/shared)
- Premises audits (Security of windows, doors, cabinets)
- Computer desktop/C Drive audits (maintaining personal data unsecure on staff PC desktop or hard drive)

The GP Practice will from time to time carry out security audits and spot checks in line with this legal requirement.

Unauthorised access or misuse of personal data is seen as breach of the data protection principles and can lead to disciplinary action or prosecution.

Individuals rights/Subject Access Requests

Within the General Data Protection Regulations 2018/Data Protection Act 2018, individuals have the right to access their personal data held at the practice. These requests are known as Subject Access Requests (SAR) and can be made to the GP Practice verbally or in writing.

There are also a number of individual's rights that can be submitted to the practice. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification

- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The GP practice provides a documented protocol on handling subject access requests and individual rights, which includes template forms and guidance for patients and staff.

Applications for subject access requests or individuals rights shall be made to the Basildon Road Surgery and must be responded to within 30 days. An extension of a further two months can be provided with valid justification and notification to the data subject.

As data controller, the practice shall ensure that ID verification is requested and must be satisfied that the person requesting the information is the data subject to whom the data applies.

Further guidance can be found on the GP Practice Subject Access Requests and individual's rights protocol or on the Information Commissioners Office Website https://ico.org.uk/

Requests by individual's representative, legal organisations and law enforcement agencies

When a request is made on behalf of an individual by someone such as a legal representative, law enforcement or advocate (friend, parent, and guardian) the person/organisation representing the individual must be asked to produce evidence of authorisation that they have approved the request on their behalf.

Staff shall refer to guidance or obtain further support from the practice manager or GP lead (Caldicott Guardian) prior to the release of any such requests.

Access to health records – deceased patients

Access to health records of deceased patients fall under the Access to Health records Act 1990 and as therefore further guidance shall be obtained prior to the release of any information requested.
(BMA Access to Health Records)

Freedom of Information Act 2000

The Freedom of Information Act applies to all NHS bodies, including hospitals, as well as doctors, dentists, pharmacists and opticians. It specifically includes any person providing general medical or personal

medical services under the National Health Service Act.

The Freedom of Information Act permits individuals (known as requesters) to ask for information about the GP practice activities. The request must be made in writing and include the requesters name and correspondence address.

Written or email Freedom of Information requests must be responded to within 20 working days (commencing the day after the practice receive the request).
Generally Freedom of Information requests must be produced free of charge, but there are cases where request for fees can be made. The requester will be contacted in writing prior to proceeding with the request.

The Freedom of Information has certain exemptions, which are prevented by law which allow the practice to withhold information from the requester. Any requests received at the practice must be dealt with by the Practice Manager to ensure that the request meets the criteria for a valid Freedom of Information Request.

Transparency (Privacy notice)

The GP practice has a legal duty to ensure that individuals are informed about the collection and use of their personal data, along with information regarding their individual's rights. Basildon Road Surgery ensures that a 'Privacy notice' in made available on the GP practice website and further information is also made available through posters and a summary document.

Staff shall familiarise themselves with this information, in order to respond to any requests or contacts made from patients.

A South East London wide (Our Healthier South East London) privacy notice is also made available through the GP website to support awareness of data processing activities across South East London health and care organisations.

Data sharing

Health and care professionals should have the confidence to share information in the best interest of their patients. Personal and confidential information must only be shared when it is legally permissible.

When it is necessary to share personal and confidential information, staff shall ensure that it is done so securely and ensure individual's privacy is respected at all times.

Data sharing in the NHS is governed by the Caldicott Principles.

Caldicott Principles

Staff shall consider the Caldicott Principles when sharing information and ensure that there is a lawful basis for doing so.

1. Justify the purpose for using confidential information
2. Do not use personal data unless it is absolutely necessary
3. Use the minimum necessary personal data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data 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 protection patient confidentiality

Technical systems, controls and secure transfer processes exist to support the secure transfer of personal or confidential data.

South East London Data Sharing Framework

Health Care professionals already share information for many different purposes. To formalise this data sharing, a formal data sharing framework has been developed across south east London.

This data sharing framework provides a consistent and transparent approach across all health and care partners and ensures compliance with the Data Protection Act 2018 and General Data Protection Regulations.

These formal Data sharing agreements for health and care providers are maintained on the NHS England Data Controller Console (DCC).

Basildon Road Surgery is a registered member of the DCC and as such shall ensure that any new and updated documents are reviewed and appropriately approved.

National data opt-out

The national data opt-out is an NHS service that allows patients to opt out of their confidential patient information being used for research and

planning.

Patients who decide they do not want their personal identifiable data used for planning and research can set their national opt out preferences online, by phone or post.

A website link to the National data opt-out shall be made available on the GP Practice website.

Transfer of information

All transfers of information within and outside the GP practice must be managed, comply with information security and follow clear process.

All staff will be made aware of the processes in place for the secure handling of personal and confidential information.

When transferring information involving personal and confidential information staff must ensure;

- there is a valid purpose and justification for transferring the information
- security standards are met for the method of transfer

Further guidance must be sought for the protection of personal and confidential information transferred outside the European Economic Area.

Clinical system data sharing

The GP practice utilise IT systems and services allocated under the GP system of choice (GPSoC). This provides the GP practice with approved and secure systems for the storage and transfer of personal data.

Records of processing activities

Information Assets

Information assets are records that are created on a day to day basis, that are central to the efficient running of the GP practice, i.e. patient document/records, finance, business records. Assets will also include documents, computer systems, network hardware and software which

are used to process this data. This includes non-computerised systems holding information (hardcopy records)

Information asset register

To maintain appropriate protection of the GP practice information assets, the practice shall maintain an information asset register.

The information asset register shall include details of;

- information assets
- the legal basis for processing
- details of systems that hold information assets
- categories of recipients and transfer (data flows)
- details of asset which may be transferred overseas
- retention information

The Practice Manager (Data Protection Lead) ensures that the items are recorded on the register and reviews the practice information asset register at least annually to ensure that it is maintained up to date.

On reviewing the information assets and data flows, the GP practice shall address any risks which may be identified regarding the controls and security of the assets.

Any risks that cannot be controlled or mitigated shall be reported to the GP Practice Caldicott Guardian and when necessary further advice and guidance should be sought from the NHS Bexley DPO or Information Commissioners Office.

Data flow mapping

Routine data flows of inward and outward personal data (information assets) shall be captured on the GP information asset register. The register aims to ensure that the method of transfer is done so securely and no personal data is not transferred outside the European Economic Area (EAA). *(Subject to change 2019 – Refer further guidance)*

The data flow mapping registered shall be reviewed in line with the information assets at least annually. Any new data flows identified as part of the Data Protection Impact Assessment will be added to the register as they take place.

Any potential or highlighted risks identified as part of the data flow mapping review will be addressed to ensure the privacy and transfer method is secure.

Information Asset Owners

Information Asset Owners are members of staff who are senior enough to make decisions concerning the information assets at the highest level.

The IAO can assign day to day responsibility for each information asset to an administrator or manager. Their role is also to understand and assess risks to the information assets they "own" and to provide assurance to the Caldicott Guardian regarding the security and use of those assets.

Information Asset Administrators

All staff are responsible for the records they create and maintain in the course of their duties and are designated Information Asset Administrators (IAA), ensuring efficient records management through the lifecycle information assets (records) they process.

Records management

The GP practice shall adhere to the records management Code of Practice for Health and Social Care 2016 and British Medical Association Retention of health records guidance.

This guidance provides a framework for the management and retention and Basildon Road Surgery shall promote good records management processes to staff.

Lifecycle

The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved.

Records, both hardcopy and electronic which are created and maintained by the practice shall be maintained efficiently and securely.

Retention

Basildon Road Surgery shall adhere to the NHS Records management code of practice regarding the minimum retention periods of personal data and other organisational related records that are created.

Although the guidance refers to minimum periods for which records must be retained, there are may be occasions when records need to be kept for longer. Decisions to retain records for longer than the recommended retention period will reside with the Caldicott Guardian.

The GP practice provides a local records retention schedule, which has been developed in line with the records management code of practice and BMA retention guidance.

Destruction

As a health professional, the GP practice is responsible for destroying personal and confidential information so that the information is not compromised. Personal and confidential data that has not been selected for retention of permanent preservation are destroyed by means of shredding by an accredited external provider.

Data quality

Basildon Road Surgery recognises that all of its decisions, whether patient care, managerial or financial need to be based on information which is of the highest standard. Data quality is crucial and the availability of complete, accurate, relevant and timely data is important in supporting patient care and business management.

Health records must be clear, accurate, factual, legible and timely. They must include all relevant clinical findings, the decisions made, information given to patients, and drugs or treatment prescribed.

Personal views about the patient's behaviour or temperament should **not** be included unless they have a potential bearing on treatment or it is necessary for the protection of staff or other patients.

Health records should not be altered or tampered with, other than to remove or correct inaccurate or misleading information. Any such amendments must be made in a way that makes it clear what has been altered, who made the alteration and when it took place.

Staff shall ensure that their manner of keeping records facilitates access by patients if requested. Information that should not be disclosed should be flagged or highlighted so that when access is given, any information is not be disclosed, (such as those which identify third parties) is readily identifiable.

Clinical coding

Read codes and Snomed codes are a coded thesaurus of clinical terms by which clinician's record patients finding and procedures in health care IT systems across primary and secondary care. Consistent data formats and the use of appropriate coding systems are key to effective electronic healthcare records in the NHS.

The GP practice shall use and promote the appropriate use of coding in line with national NHS guidance. *(NHS Digital - National clinical coding standards)*

Data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes

All staff at the practice will be made aware of;

- how to recognise a personal data breach
- who to notify within the practice for managing breaches (a dedicated person or team)
- what action is required to support the reporting of the personal data breach

Reporting a data breach

Any data breach that is likely is to result in a high risk of adversely affecting individuals' rights and freedoms must be reported to the Information Commissioners Office (ICO) within 72 hours.

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The DPO , Pauline Clelland will seek further guidance from the ICO supporting guidance and take the appropriate measures to ensure that the data breach is acted upon.

A data breach that requires reporting to the ICO, shall be reported through the NHS Digital Data Security and Protection Toolkit.

The GP practice will take steps to also register details of the event and actions taken in line with the GP practice significant events policy.

Not all data breaches require reporting to the ICO. Any other data breaches must be reported, investigated and action taken to address any future occurrence.

Data breaches or incidents (large or small) must be registered and maintained on a local file, providing details of the breach and any subsequent investigation and outcomes. Care should be taken not to include any personal data on the register.

When it is necessary to do so, the Practice Manager will ensure that

any individuals involved in the personal data breach are notified.

The Data Protection Lead will take responsibility for notifying the Information Commissioners Office and act as the liaison officer when dealing with any investigations arising from the data breach.

Business continuity planning

The GP practice business continuity plan enables staff at the practice to plan and respond to a range of emergencies and incidents that could affect health or safety of patients. This document is controlled and reviewed by Pauline Clelland and is made available to staff in practice Shared P drive and printed hard copy available in reception.

The business continuity plan shall include a list of staff contact telephone numbers, to enable the responsible officers to make contact with staff. This list will be kept accessible to all staff in the event of an emergency.

Incidents that occur that affect the IT infrastructure such as a cyber-security breach or electrical down time event shall be reported to the NHS SE London Clinical Commissioning Group (Bexley) ICT support service immediately on 020 8 298 6166 or the out of hours 0208 298 6111

Accountable suppliers

As a data controller, the GP practice shall be responsible for knowing what service providers are handling personal data on behalf of the practice.

Details of the organisations, the services they provide and contract details shall be registered by the practice manager on the information asset register.

Due diligence involving the research of suppliers Data Security Standards will be completed and registered along with the detailed list of suppliers.

Full guidance is made available on the NHS Digital, Data Security and Protection Toolkit NDG standard 10.

Dissemination and review

This policy will be available to staff in the shared P drive and will be reviewed every two years or when there are changes in national guidance

Associated GP practice documents

- Data Protection Impact Assessment
- Subject access requests and individuals rights protocols
- Information breach incident reporting guide
- Staff contracts/confidentiality agreement
- Staff handbook
- Staff leavers form
- Monitoring and spot checks template

Definitions

BMA – British Medical Association
DPA – Data Protection Act (2018)
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
DSPT – Data Security and Protection Toolkit
ELfH – E- Learning for Health
GDPR – General Data Protection Regulations
ICO – Information Commissioners Office

Guidance and resources

BMA – Social Media guidance for doctors
BMA – Access to health records guidance
CQC – Well Led inspection
Information Commissioners Office
NHS England – Information governance and instant messaging
NHS Digital Data Security and Protection Toolkit
NHS Digital clinical coding
Quality Outcome Framework
Records management NHS Code of Practice 2016
Bexley IT contract

Appendix to Bexley GP practice Data Security and protection policy
Glossary

Access to Health Act 1990	The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased individual. The individuals are defined under Section 3 (1) (f) of the Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.
British Medical Association (BMA)	BMA are the trade union and professional association for doctors and medical students across the UK. The BMA support doctors throughout their training and careers. We are the trade union and professional association for doctors and medical students across the UK
Caldicott Guardian	A Caldicott Guardian is a senior person (normally a health or social care professional) in every NHS and social services organisation who champions patient confidentiality, acting as the 'conscience' of the organisation to help ensure that patient information is protected and shared appropriately.
Caldicott Principles	The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to adult social care records in 2000.
Care Act 2014	The **Care Act 2014** sets out in one place, local authorities' duties in relation to assessing people's needs and their eligibility for publicly funded **care** and support. To make provision about safeguarding adults from abuse or neglect, to make provision about care standards, to establish and make provision about Health Education England, to establish and make provision about the Health Research Authority, and for connected purposes.
CareCERT	NHS Digital has been commissioned by the Department of Health to develop a Care Computer Emergency Response Team (CareCERT). CareCERT offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats

Computer misuse Act	The Computer Misuse Act is designed to protect computer users against wilful attacks and theft of information. Offences under the act include hacking, unauthorised access to computer systems and purposefully spreading malicious and damaging software (malware), such as viruses
Common law of duty of confidentiality	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is generally accepted that information provided by patients or service users to a health or social care service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. This is an important point, as once information is effectively anonymised it is no longer confidential. Under English common law, information given in circumstances where it is expected that a duty of confidence applies (such as within the relationship between a patient and their health and social care professional) cannot normally be disclosed without that person's explicit consent. Confidential information may be shared within the care team where necessary for the direct care of that individual patient - which is the reason the information is held. Any disclosure outside the care team must have one of the following in order to be lawful: o The explicit, informed and freely-given consent of the patient. o A legal duty to disclose (such as a statutory obligation or court order). o A statutory basis to permit disclosure (such as Section 251 support). o Exceptionally, an overriding public interest in disclosure which outweighs both the individual's own rights and freedoms and the public interest in a confidential health service (such as safeguarding disclosures).
Criminal offences data	“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.
Cyber Essentials	Cyber Essentials is a Government and industry-backed standard which protects your business against cyber threats.
Data controller	Data controller is the natural or legal person, public

	authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. Data processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data processor	**"Data processor"**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Obtaining recording or holding the information or data.
Data flow	Data flows are inward and outward transfer (flows) of personal data.
Data flow mapping	Routine data flows are captured on a register to ensure that the method of transfer is recorded and remains secure. This helps assess the level of risk associated with the data flow.
Encryption	Encryption is an effective way to achieve data security. It is a process which converts computer data and messages into something incomprehensible. The process generates cipher text that can only be viewed in its original form if decrypted with the correct key, by systems and organisations that are authorised to view the information in its original form.
Information Commissioners Office (ICO)	The ICO is an independent organisation that has been established to uphold information rights in the public interest. They have the power to conduct compulsory audits and to issue monetary penalty notices for serious data breaches. They also provide guidance and support for the public and organisations about protecting personal information. https://ico.org.uk/
Lawful bases for processing	The Data Protection Act 2018/General Data Protection Regulations set out a series of lawful basis conditions for processing personal data. Organisations that handle personal data must determine the lawful basis for

	processing in line with the legal requirements to ensure they met these legal requirements.
Mental Health Act (1983)	The **Mental Health Act** (1983) is the main piece of legislation that covers the assessment, treatment and rights of people with a **mental health disorder**. People detained under the **Mental Health Act** need urgent treatment for a **mental health disorder** and are at risk of harm to themselves or others.
National Data Opt-Out	The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.
NHS Code of practice	The '**Confidentiality**: **NHS Code of Practice**' sets out what health and care organisations have to do to meet their responsibilities around **confidentiality** and patients' consent to use their health records. It's based on legal requirements and best **practice**. e '**Confidentiality**: **NHS Code of Practice**' sets out what health and care organisations have to do to meet their responsibilities around **confidentiality** and patients' consent to use their health records. It's based on legal requirements and best **practice**.
NHS Digital **Register for Caldicott Guardians**	NHS Digital website to complete the registration form at: https://digital.nhs.uk/services/organisation-dataservice/our-services#CG.
Personal data	"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier..
personal data breach	A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.
Special categories of personal data	"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).
The National Cyber	Provides UK Government advice and guidance on a wide

Security Centre (NCSC).	range of Security and Cyber Security Threats and Solutions, including archived guidance from CESG. This archived guidance, although no longer mandated, does still provide guidance on best practice. https
Unsupported systems	Hardware and software systems that do not support the latest version controls, upgrades or protection.
Your Data: Better Security, Better Choice, Better Care	A Government response document in response to the National Data Guardian For health and Care review of Data Security and Opt-Outs
Health and Social Care Act	Indirect care/Secondary purposes The term 'indirect care' is defined as activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of indirect care activities include risk prediction and stratification, service evaluation, needs assessment, and financial audit.
Information Commissioners Office	The Information Commissioner's Office (ICO) is the UK regulator of the Data Protection. This ICO is the UK's independent body set up to uphold information rights.
Mental Health Act 1983	The Mental Health Act (1983) is the main piece of legislation that covers the assessment, treatment and rights of people with a mental health disorder. People detained under the Mental Health Act need urgent treatment for a mental health disorder and are at risk of harm to themselves or others.
National Data Guardian for Health and Care's review of Data Security and Opt-Outs	A review by the National Data Guardian for Health and Care (NDG), Dame Fiona Caldicott, which makes recommendations to the Secretary of State for Health. These are aimed at strengthening the safeguards for keeping health and care information secure and ensuring the public can make informed choices about how their data is used.
Records management NHS Code of practice for health and social care	Records management NHS code of practice for health and social care. The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. This includes records of staff, complaints, corporate records and any other records held in any format including both paper and digital records. The

	guidelines also apply to Adult Social Care records where these are integrated with NHS patient records. This code defines roles and responsibilities within the organisation, including the responsibility of individuals to document their actions and decisions in the organisation's records and to dispose of records appropriately when they are no longer required in line with the records retention framework.