Weobley & Staunton on Wye Surgeries

CONFIDENTIALITY (DISCLOSURE & SHARING OF INFORMATION) POLICY

INTRODUCTION

The Data Protection Act 1998/ Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) impose obligations on the use of all personal data held by Weobley & Staunton on Wye Surgeries whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation. This has implications for every part of the organisation. The Practice also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, NHS Digital and the NHS Information Governance Alliance the specific requirements of the NHS Digital Data Security and Protections Assurance Toolkit and guidance issued by professional bodies.

The Practice and its employees are bound by a legal duty of confidentiality to all patients which can only be set aside to meet an overriding public interest, legal obligation, or similar duty. The DPA and GDPR apply to all staff, contractors and volunteers working for the Practice. Weobley & Staunton on Wye Surgeries are the Data Controller, as defined in Article 3 (7) of the GDPR and Section 1 of the DPA and is obliged to ensure that all the Data Protection requirements are implemented. The requirements of Article 5 (1) of the GDPR and be able to demonstrate compliance with those requirements Article 5(2).

This policy sets out how the Practice meets its legal obligations and requirements under confidentiality, Data Protection and information security standards. The chief requirements outlined in this Policy are based upon the DPA/GDPR, which is the central piece of legislation covering security and confidentiality of personal information.

As a principle, seeking the consent of a patient to the disclosure of their information shows respect, and is part of good communication between doctors and patients.

Most patients understand and accept that information must be shared within the healthcare team in order to provide their care. The Practice will make sure that information is readily available to patients, explaining that (unless they object) personal information about them will be shared within the healthcare team, including administrative and other staff who support the provision of their care.

The Practice will respect the wishes of any patient who objects to particular information being shared within the healthcare team or with others providing care, unless disclosure would be justified in the public interest.

- All patients can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when somebody is at grave risk of serious harm).
- All information held at the Practice about patients is confidential, whether held electronically or in hard copy;
- Other information about the Practice (e.g. staff records and financial matters) is confidential;
- All staff are aware of their responsibilities for safeguarding confidentiality and preserving information security
- All staff understand their responsibilities when sharing information with both NHS and non-NHS organisations

Should a patient object to a disclosure that is considered essential to the provision of safe care, it will be explained to them that they cannot be referred (or cannot otherwise arrange for their treatment) without also disclosing that information.

The Practice will make every effort to ensure that anyone to whom we disclosure personal information understands that it is being given to them in confidence, which they must respect.

POLICY AIMS

This Policy aims to ensure that Weobley & Staunton on Wye Surgeries (the Practice) meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the General Data Protection Regulation (GDPR) that is the key piece of legislation covering security and confidentiality of personal information.

POLICY SCOPE

This policy covers all forms of information held by the Practice, including (but not limited to):

- Information about members of the Public
- Non-practice employees on Practice premises
- Staff and Personnel information
- Organisational, business and operational information

This Policy applies to all Practice employees and third parties responsible for the delivery of contracted NHS services on behalf of the Practice.

DEFINITIONS

- **Information Governance** (IG) – IG is the organisational practice of managing information from its creation to final disposal in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that Practice information is managed securely, compliant with legislation and available for access by both staff and external parties, including the public and regulators.

- **Data Security and Protections Toolkit (DSP)** – The assessment toolkit is supported by both NHS Digital and NHS England and is a self-assessment tool for Practices which incorporates a knowledge base and guidance all aspects of IG. The DS&P is updated annually to reflect new NHS guidance, legislation and NHS Codes of Practice.

- **Senior Information Risk Owner (SIRO)** – The SIRO takes ownership of the Practice's Information Risk Policy and acts as an advocate for information risk on behalf of the Practice who is also the Senior Information Risk Officer. The SIRO for the Practice is the Practice Manager.

- **Caldicott Guardian** – The Practice's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is Dr. Tom Moore.

- **Data Controller** – means the natural or legal person, public authority (Weobley & Staunton on Wye Surgeries), 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; Article 4(7) GDPR

APPLICABILITY

The policy applies to all Practice Employees and Partners, and also applies to other people who work at the Practice e.g. Locum GPs, Non-employed nursing staff, Temporary staff and Contractors (referred to as "Staff" throughout this document).

PRINCIPLES OF CONFIDENTIALITY STANDARDS

To meet the vision for managing DPC standards there are three key interlinked aims to the policy which will ensure the delivery of an effective policy framework:

Legal Compliance - The Practice aims to meet and exceed all compliance requirements relating to DPC. The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements through the Appropriate IG Toolkit and demonstrating compliance to all relevant healthcare standards, the policy will also demonstrate that the Practice has adopted the Accountability for demonstrating compliance with the GDPR as required by Article 5(2).

Information Security - The Practice will promote effective confidentiality and security practice to its staff through an Information Security Management Systems (ISMS) which includes policies, procedures and training. The Practice has established and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Openness - Non-confidential information on the Practice and its services should be available to the public through a variety of media. The Practice will undertake or commission annual assessments and audits of its policies and arrangements for openness through the IG Toolkit.

STAFF CONFIDENTIALITY

All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications must be conducted in a confidential manner.

Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager. Staff must not process any personal information in contravention of the GDPR 2016 or DPA2018.

Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

All staff have a confidentiality clause in their contract of employment. The practice has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

PATIENT CONFIDENTIALITY

The Confidentiality NHS Code of Practice has been published by NHS England. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators.

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

On first contact with the Practice, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

In the event a person lacks capacity to consent to information being shared staff should check if a person is authorised by a Lasting Power of Attorney (health and welfare) or been appointed by the court of protection to make that decision. The document must be seen. This person can consent on their behalf but must act in the person's best interest. If they have not, then no one can consent on behalf of that person. A professional in the care team must assess if it is in the best interest of the person to share the information. The person's wishes and feeling, although not determinative, should be the starting point in this assessment

OVERVIEW - PATIENTS' RIGHT TO CONFIDENTIALITY

Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care.

- All information about patients is confidential: from the most sensitive diagnosis, to the fact of having visited the surgery or being registered at the Practice. This includes information about patients' families or others associated with them.
- Confidential information may not be health-related. It can include anything that is private and not public knowledge.
- Workers should limit any discussion about confidential information to only those who need to know within the practice.
- Only the minimum amount of necessary information should be disclosed.
- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person.
- Workers must not, under any circumstances, disclose patient information to anyone outside the Practice, except to other health professionals on a need-to-know basis, or where the patient has provided written consent.
- Workers must not, under any circumstances, disclose confidential information about the Practice to anyone outside the Practice unless with the express consent of the Practice Manager and/or Partners.
- All patients can expect their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when a person is at grave risk of serious harm).
- Where disclosure of information is required which is non-routine in nature the patient will, where possible, be fully informed of the nature of the disclosure prior to this being released.
- Where the decision is made to disclose information, the decision to do so must be justified and documented.
- Person-identifiable information must not be used unless absolutely necessary – anonymised data should be used wherever possible.
- Workers must be aware of and conform to the requirements of the Caldicott recommendations and GDPR principles.
- Electronic transfer of any confidential information, once approved by the Practice Manager and/or a Partner must be transmitted by NHS net using agreed encryption methods. Workers must take particular care that confidential information is not transmitted in error by email or over the internet.
- Workers must not take data from the Practice's computer systems (eg. on a memory stick or removable drive) off the premises unless authorised to do so by the Practice Manager and/or a Partner.
- Where this is the case, the information must be kept on the worker's person at all times while travelling and kept in a secure, lockable location when taken home or to another location.
- Workers who suspect a breach of confidentiality must inform the Practice Manager and/or a Partner immediately.
- Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal.

- Workers remain bound by a requirement to keep information confidential even if they are no longer employed at the Practice. Any breach, or suspected breach, of confidentiality after the worker has left the Practice's employment will be passed to the Practice's lawyers for action.

All Staff will be required to sign the Practices Confidentiality Statement, as detailed overleaf.

PROTECTING INFORMATION

When you are responsible for personal information about patients you must make sure that it is effectively protected against improper disclosure at all times

Many improper disclosures are unintentional. You should not discuss patients where you can be overheard or leave patients' records, either on paper or on screen, where they can be seen by other patients, unauthorised health care staff or the public. You should take all reasonable steps to ensure that your consultations with patients are private.

SHARING INFORMATION WITH PATIENTS

Patients have a right to information about the health care services available to them, presented in a way that is easy to follow, understand and use

Patients also have a right to information about any condition or disease from which they are suffering. This should be presented in a manner easy to follow, understand and use, and include information about:

- Diagnosis
- Prognosis
- Treatment options
- Outcomes of treatment
- Common and / or serious side-effects of treatment
- Likely time-scale of treatments and
- Costs where relevant

You must always give patients basic information about treatment you propose to provide, but you should respect the wishes of any patient who asks you not to give them detailed information. This places a considerable onus upon health professionals, yet, without such information, patients cannot make proper choices as partners in the health care process

You should tell patients how information about them may be used to protect public health, to undertake research and audit, to teach or train clinical staff and students and to plan and organise health care services. See Section "Disclosing Information for Clinical Audit" for further information.

RESPONSIBILITIES OF PRACTICE STAFF/WORKERS

All Practice employees whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All health professionals must follow their professional codes of practice and the law. This means that they must make every effort to protect confidentiality. It also means that no identifiable information about a patient is passed to anyone or any agency without the express permission of that patient, except when this is essential for providing care or necessary to protect somebody's health, safety or well-being.

All health professionals are individually accountable for their own actions. They should, however, also work together as a team to ensure that standards of confidentiality are upheld, and that improper disclosures are avoided.

Additionally, The Weobley and Staunton-on-Wye Surgeries, as employers:

- are responsible for ensuring that everybody employed by the practice understands the need for, and maintains, confidentiality
- have overall responsibility for ensuring that systems and mechanisms are in place to protect confidentiality
- have vicarious liability for the actions of those working in the practice – including health professionals and non-clinical staff (i.e. those not employed directly by the practice but who work in the surgery)

Standards of confidentiality apply to all health professionals, administrative and ancillary staff – including receptionists, secretaries, practice manager, cleaners and maintenance staff who are bound by contracts of employment to maintain confidentiality. They must not reveal, to anybody outside the practice, personal information they learn in the course of their work, or due to their presence in the surgery, without the patient's consent. Nor will they discuss with colleagues any aspect of a patient's attendance at the surgery in a way that might allow identification of the patient unless to do so is necessary for the patient's care.

All staff are required to undertake regular Practice mandatory training in information governance to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance.

Practice Management Team

The Practice Management Team has overall responsibility for the Practice's ability to meet the policy requirements. The Management Team is responsible for:

- Receiving, considering and approving regular reports and briefings
- Signing off the Practice's Privacy Strategy and annual DS&P Toolkit returns

Executive Lead

The Senior Partner has overall responsibility for information governance in the Practice. As Accountable officer he/she is responsible for the management of information governance within the Practice and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The Practice has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Caldicott Guardian

The Practice Caldicott Guardian has Management Team level responsibilities for the Practice's Caldicott Function and enables a direct reporting line to the Practice Management Team. The Caldicott Guardian is responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to information governance (IG) and will require an IG Lead to liaise directly with the Caldicott Guardian

Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) has Management Team level responsibilities and takes overall ownership of the Practice's IG processes and provides written advice to the Senior Partner on the content of the Practice's Annual Governance Statement in regard to information risk.

IG Lead

The IG Lead is the Practice Manager. The IG Lead has responsibility for project managing the overall co-ordination, publicising and monitoring of the Practice IG Framework. The Practice IG Lead has specific responsibility for the development of this policy, producing performance monitoring reports and producing the DSP Toolkit returns on behalf of the Practice.

Data Protection Officer

Paul Couldrey of PCIG Consulting Limited will act as the Data Protection Officer (DPO) for Practice. This role is key to ensuring that the Practice complies and can demonstrate that they comply with the GDPR.

EDUCATION AND TRAINING REQUIREMENTS

The Practice is committed to the provision of IG training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery.

The Practice has a mandatory training programme which includes maintaining awareness of IG, data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:

- personal responsibilities;
- confidentiality of personal information;
- relevant IG Policies and Procedures;
- general good practice guidelines covering security and confidentiality;
- records management.

All staff will be required to complete annual IG training (including data protection and confidentiality training) commensurate with their duties and responsibilities. All new starters will be given IG training as part of the Practice Mandatory Induction process.

LEGAL LIABILITY

The Practice will generally assume vicarious liability for the acts of its staff, including those on Honorary contracts. However, it is incumbent on staff to ensure that they;

- Have undergone any suitable training identified as necessary under the terms of this policy or otherwise.
- Have been fully authorised by their Line Manager to undertake the activity.
- Fully comply with the terms of any relevant Practice policies and/or procedures at all times.
- Only depart from any relevant Practice guidelines providing always that such departure is confined to the specific needs of individual circumstances. In healthcare delivery such departure shall only be undertaken where, in the judgement of the responsible clinician it is fully appropriate and justifiable – such decision to be fully recorded in the patient's notes.

Staff Contracts of Employment are produced and monitored by the Practice. All Contracts of Employment include a data protection and general confidentiality clause as part of controls to enhance privacy and information governance. Agency and contract staff are subject to the same rules.

DISCLOSING INFORMATION ABOUT PATIENTS

When Practice staff manages any business information then they are required to comply with the requirements of the procedures and requirements. This policy requires all staff to manage information to the highest standards to ensure compliance with appropriate standards, to secure all Practice information and to promote appropriate information access.

The Practice fully endorses the six principles set out in the GDPR 2016. The Practice and all staff who process personal information must ensure these principles are followed. In summary these state that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

- (processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Furthermore, the Practice is committed to implementing the seven Caldicott principles for handling patient-identifiable information, namely:

- Justify the purpose of using patient identifiable information.

- Only use patient identifiable information when absolutely necessary.

- Use the minimum necessary patient identifiable information.

- Access patient identifiable information on a strict need to know basis.

- Everyone should be aware of their responsibilities.

- Understand and comply with the law.

- The duty to share information can be as important as the duty to protect patient confidentiality

Seeking patients' consent to disclosure of information is part of good communication between doctors, Practice staff and patients. When asked to provide information you must follow the guidance in this document.

SHARING INFORMATION WITHIN THE HEALTH CARE TEAM OR WITH OTHERS PROVIDING CARE

Circumstances Where Patients May Give Implied Consent To Disclosure

Most people understand and accept that information must be shared within health care teams in order to provide their care.

You should make sure that patients are aware that personal information about them will be shared within the health care team, unless they object, and of the reasons for this.

It is particularly important to check that patients understand what will be disclosed if you need to share identifiable information with anyone employed by another organisation or agency who is contributing to their care.

You must respect the wishes of any patient who objects to particular information being shared with others providing care, except where this would put others at risk of death or serious harm

You must make sure that anyone to whom you disclose personal information understands that it is given to them in confidence, which they must respect. All staff members receiving personal information in order to provide or support care are bound by a legal duty of confidence, whether or not they have contractual or professional obligations to protect confidentiality

Circumstances may arise where a patient cannot be informed about the sharing of information, for example because of a medical emergency. In these cases you must pass relevant information promptly to those providing the patient's care.

DISCLOSING INFORMATION FOR CLINICAL AUDIT

Clinical audit is essential to the provision of good care. All doctors in clinical Practice have a duty to participate in clinical audit. Where an audit is to be undertaken by the team which provided care, or those working to support them, such as clinical audit staff, you may disclose identifiable information, provided you are satisfied that patients:

- Have been informed that their data may be disclosed for clinical audit, and their right to object to the disclosure; and
- Have not objected

If a patient does object, you should explain why information is needed and how this may benefit their care. If it is not possible to provide safe care without disclosing information for audit, you should explain this to the patient and the options open to them.

Where clinical audit is to be undertaken by another organisation, information should be anonymised wherever that is practicable. In any case, where it is not practicable to anonymise data, or anonymised data will not fulfil the requirements of the audit, express consent must be obtained before identifiable data is disclosed.

DISCLOSURES WHERE EXPRESS CONSENT MUST BE SOUGHT

Express consent is usually needed before the disclosure of identifiable information for purposes such as research, epidemiology, financial audit or administration.

When seeking express consent to disclosure you must make sure that patients are given enough information on which to base their decision, the reasons for the disclosure and the likely consequences of the disclosure. You should also explain how much information will be disclosed and to whom it will be given.

If the patient withholds consent, or consent cannot be obtained, disclosures may be made only where they are required by law or can be justified in the public interest.

Where the purpose is covered by a regulation made under section 60 of the Health and Social Care Act 2001, disclosures may also be made without patients' consent.

You should make a record of the patient's decision, and whether and why you have disclosed information

Where doctors have contractual obligations to third parties, such as companies or organisations, they must obtain patients' consent before undertaking any examination or writing a report for that organisation. Doctors should offer to show patients the report, or give them copies, whether or not this is required by law.

EMERGENCY SUMMARY CARE RECORD

All patients have been contacted by the PCT in order to provide them with the opportunity to opt out of the Emergency Summary Care Record. Patients (ESCR) who do not respond to the letter will be tagged as giving assumed consent for the upload of their ESCR.

Patients who reply stating they do not want their ESCR uploaded to the national spine will have the appropriate code applied to their clinical record.

Patients who opt to upload all or opt to decline upload can change their mind by informing the practice who will add or delete the appropriate code from their medical record.

DISCLOSURE IN CONNECTION WITH JUDICIAL OR OTHER STATUTORY PROCEEDINGS

Disclosures Required by Law

You must disclose information to satisfy a specific statutory requirement, such as notification of a known or suspected communicable disease. You should inform patients about such disclosures, wherever that is practicable, but their consent is not required

Disclosures to Courts or in Connection with Litigation

You must also disclose information if ordered to do so by a judge or presiding officer of a court. You should object to the judge or the presiding officer if attempts are made to compel you to disclose what appear to you to be irrelevant matters, for example matters relating to relatives or partners of the patient, who are not parties to the proceedings

You must not disclose personal information to a third party such as a solicitor, police officer or officer of a court without the patient's express consent, except in the circumstances described below.

Disclosures to Statutory Regulatory Bodies

Patient records or other patient information may be needed by a statutory regulatory body for investigation into a health professional's fitness to Practice.

If you are referring concerns about a health professional to a regulatory body, you must seek the patient's consent before disclosing identifiable information, wherever that is practicable.

Where patients withhold consent or it is not practicable to seek their consent, you should contact the GMC, or other appropriate regulatory body, which will advise you on whether the disclosure of identifiable information would be justified in the public interest or for the protection of other patients.

Wherever practicable you should discuss this with the patient. There may be exceptional cases where, even though the patient objects, disclosure is justified.

THE PUBLIC INTEREST

Disclosures in The Public Interest

Personal information may be disclosed in the public interest, without the patient's consent, and in exceptional cases where patients have withheld consent, where the benefits to an individual or to society of the disclosure outweigh the public and the patient's interest in keeping the information confidential.

In all cases where you consider disclosing information without consent from the patient, you must weigh the possible harm (both to the patient, and the overall trust between doctors and patients) against the benefits which are likely to arise from the release of information

Before considering whether a disclosure of personal information 'in the public interest' would be justified, you must be satisfied that identifiable data are necessary for the purpose, or that it is not practicable to anonymise the data.

In such cases you should still try to seek patients' consent, unless it is not practicable to do so, for example because:

- The patients are not competent to give consent; or
- The records are of such age and / or number that reasonable efforts to trace patients are unlikely to be successful; or
- The patient has been, or may be violent; or obtaining consent would undermine the purpose of the disclosure (e.g. Disclosures in relation to crime); or
- Action must be taken quickly (for example in the detection or control of outbreaks of some communicable diseases) and there is insufficient time to contact patients

In cases where there is a serious risk to the patient or others, disclosures may be justified even where patients have been asked to agree to a disclosure, but have withheld consent.

You should inform patients that a disclosure will be made, wherever it is practicable to do so. You must document in the patient's record any steps you have taken to seek or obtain consent and your reasons for disclosing information without consent

Ultimately, the 'public interest' can be determined only by the courts; but the GMC may also require you to justify your actions if a complaint is made about the disclosure of identifiable information without a patient's consent.

The potential benefits and harms of disclosures made without consent are also considered by the Patient Information Advisory Group in considering applications for Regulations under the Health and Social Care Act 2001.

Disclosures of data covered by a Regulation 4 are not in breach of the common law duty of confidentiality.

Disclosures to Protect the Patient or Others

Disclosure of personal information without consent may be justified in the public interest where failure to do so may expose the patient or others to risk of death or serious harm.

Where the patient or others are exposed to a risk so serious that it outweighs the patient's privacy interest, you should seek consent to disclosure where practicable. If it is not practicable to seek consent, you should disclose information promptly to an appropriate person or authority.

You should generally inform the patient before disclosing the information. If you seek consent and the patient withholds it you should consider the reasons for this, if any are provided by the patient.

If you remain of the view that disclosure is necessary to protect a third party from death or serious harm, you should disclose information promptly to an appropriate person or authority. Such situations arise, for example, where a disclosure may assist in the prevention, detection or prosecution of a serious crime, especially crimes against the person, such as abuse of children.

CHILDREN AND OTHER PATIENTS WHO MAY LACK COMPETENCE TO GIVE CONSENT

Disclosures in Relation to the Treatment Sought by Children Or Others Who Lack Capacity to Give Consent

Problems may arise if you consider that a patient lacks capacity to give consent to treatment or disclosure.

If such patients ask you not to disclose information about their condition or treatment to a third party, you should try to persuade them to allow an appropriate person to be involved in the consultation.

If they refuse and you are convinced that it is essential, in their medical interests, you may disclose relevant information to an appropriate person or authority. In such cases you should tell the patient before disclosing any information, and where appropriate, seek and carefully consider the views of an advocate or carer. You should document in the patient's record your discussions with the patient and the reasons for deciding to disclose information

Disclosures Where A Patient May Be A Victim of Neglect or Abuse

If you believe a patient to be a victim of neglect or physical, sexual or emotional abuse and that the patient cannot give or withhold consent to disclosure, you must give information promptly to an appropriate responsible person or statutory agency, where you believe that the disclosure is in the patient's best interests.

If, for any reason, you believe that disclosure of information is not in the best interests of an abused or neglected patient, you should discuss the issues with an experienced colleague. If you decide not to disclose information, you must be prepared to justify your decision.

Disclosure after a Patient's Death

You still have an obligation to keep personal information confidential after a patient dies.

The extent to which confidential information may be disclosed after a patient's death will depend on the circumstances. If the patient had asked for information to remain confidential, his or her views should be respected.

- Where you are unaware of any directions from the patient, you should consider requests for information taking into account:
- Whether the disclosure of information may cause distress to, or be of benefit to, the patient's partner or family;
- Whether disclosure of information about the patient will in effect disclose information about the patient's family or other people;
- Whether the information is already public knowledge or can be anonymised;
- The purpose of the disclosure

If you decide to disclose confidential information you must be prepared to explain and justify your decision

BREACH OF THE DATA PROTECTION LEGISLATION

Any breach of the Data Protection legislation with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Practice Policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal.

GLOSSARY

This defines the terms used within this document. These definitions have no wider or legal significance.

Anonymised Data	Data from which the patient cannot be identified by the recipient of the information. The name, address, and full post code must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the patient. Unique numbers may be included only if recipients of the data do not have access to the 'key' to trace the identity of the patient
Clinical Audit	Evaluation of clinical performance against standards or through comparative analysis, to inform the management of services. Studies that aim to derive, scientifically confirm and publish generalizable knowledge constitute research and are not encompassed within the definition of clinical audit in this document
Consent	Agreement to an action based on knowledge of what the action involves and its likely consequences
Express Consent	Consent which is expressed orally or in writing (except where patients cannot write or speak, when other forms of communication may be sufficient)
Identifiable Data	Data from which a patient can be identified. Name, address and full postcode will identify patients; combinations of data may also do so, even where name and address are not included
Implied Consent	Agreement to disclosure where patients have been informed about the information to be disclosed, the purpose of the disclosure, and that they have a right to object to the disclosure, but have not done so
Health Care Team	The health care team comprises the people providing clinical services for each patient and the administrative staff who directly support those services
Patients	Used throughout the guidance to mean competent patients. Parents of, or those with parental responsibility for, children who lack maturity to make decisions for themselves, are generally entitled to make decisions about disclosures on behalf of their children
Personal Information	Information about people which doctors learn in a professional capacity and from which individuals can be identified
Public Interest	The interests of the community as a whole, or a group within the community or individuals

CONFIDENTIALITY AUDIT PROCEDURES

With advances in the electronic management of both health and employment information within the NHS brought about by the advent of the NHS Care Record Service, Electronic Prescribing, Choose and Book and the Electronic Staff Record, the requirement to monitor access to such confidential information has become increasingly important.

With the large number of staff using these systems, it is imperative that access is strictly monitored and controlled. Furthermore, with the increased use of electronic communications, the movement of confidential information via these methods poses the threat of information falling into the hands of individuals who do not have a legitimate right of access to it.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purposes may result in a breach of that confidentiality, therefore contravening the requirements of:

- Caldicott
- Data Protection Act 1998/2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality

These procedures provide an assurance mechanism by which the effectiveness of controls implemented within the Practice are audited, areas for improvement and concern highlighted and recommendations for improved control and management of confidentiality within the Practice are made.

Monitoring Confidential Information

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

Monitoring should be carried out by the Practice Manager in order that irregularities regarding access to confidential information can be identified and reported to the Caldicott Guardian and action taken to address the situation, either through Disciplinary action, the implementation of additional controls or other remedial action as necessary.

Actual or potential breaches of confidentiality should be reported using the Practice's reporting systems.

Auditing Access to Confidential Information

The Caldicott Guardian and/or the Practice Manager will ensure that audits of security and access arrangements within each area are conducted on a regular basis. Areas to be audited include:

- Security applied to manual files eg. storage in locked cabinets/locked rooms
- Arrangements for recording access to manual files eg. tracking cards, access requests by solicitors, police and data subjects etc
- Evidence that checks have been carried out to ensure that the person requesting access has a legitimate right to do so
- The existence and location of whiteboards containing confidential information
- The use of and disposal arrangements for post it notes, notebooks, other temporary recording material
- Retention and disposal arrangements
- Confidential information sent or received via email, security applied and email system used
- Information removed from the workplace – has authorisation been gained either for long term or short term removal
- Security arrangements applied ie. transportation in secure containers
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information

- Security applied to laptops and compliance with the Practice's Remote Working Policy
- Verbal conversations with personal data exchange
- Passwords being used within the area being audited

Audit Method

Audit should be carried out using the attached Information Governance Spot Check Questionnaire at least twice per annum (see Appendix B) and ad-hoc instances can be recorded using Appendix C.

Pre-set questions will establish:

- Roles and responsibilities
- Awareness of general confidentiality issues
- Understanding of Data Protection Principles directly relating to their job
- Understanding the requirements of policies, protocols and procedures relation to confidentiality
- Training received

Reporting

A formal outcome report should be provided to the Partners for review at the Friday Partners Business meeting.

Non-Compliance

Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, including all the facts and referring to any relevant evidence. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered to be non-compliant.

Each non-compliance observed should have an associated recommendation which should be discussed and agreed with the Partners and/or Practice Manager.

Non-compliance can fall into one of two categories:

- Major Non-Compliance – this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences
- Minor Non-Compliance – these could include one off occurrences of non-compliance, there is little risk of the non-compliance causing more than a minor irritation

Where a number of minor instances of non-compliance are observed by the same person or the same functional area, this may indicate a more serious problem within that area. If this is the case, these instances of non-compliance should be combined into a major non-compliance.

Failure to comply with the standards and appropriate governance of information as detailed in this procedure and supporting documents can result in disciplinary action. All staff are reminded that this procedure covers several aspects of legal compliance that as individuals they are responsible for.

Failure to maintain these standards can also result in criminal proceedings against the individual.

Audit Follow-Up

Once the audit process is complete, arrangements should be made for follow-up where non-compliance has been observed, this will allow the Practice to confirm that the recommended corrective action has been implemented.

LEGISLATION

Access by Patients

Two pieces of legislation give patients, or their authorised representatives, access to information about themselves:

Data Protection Act 1998
Rights of access for patients to their medical records
Right to know about what data is used for

Advice on how the guidance applies in clinical care and in research, epidemiology etc. is available from the Office of the Information Commissioner (http://www.dataprotection.gov.uk/). The Data Protection Act 1998 also places a duty on those who process data to do so lawfully (in accordance with relevant legislation or case law) and fairly (keeping people informed about how their personal information is being used)

Access to Medical Reports Act 1988
Provides for patients to see reports written about them for insurance or education purposes by a doctor who has provided their clinical care

Access by Others

Gender Recognition Act 2004
The 2004 Gender Recognition Act (GRA) makes it a criminal offence to disclose an individual's transgender history to a third party without their written consent if that individual holds a Gender Recognition Certificate (GRC).

Patients do not need to show a GRC or birth certificate in order for the GRA 2004 to be in effect, so it is best practice to act as though every trans patient has one. This means always obtaining a trans patient's written consent before sharing details about their social or medical transition, sometimes also called gender reassignment, with other services or individuals.

This includes information such as whether a patient is currently taking hormones or whether they have had any genital surgery, as well as information about previous names or the gender they were given at birth. Consent should always be obtained before information relating to the patient being trans is shared in referrals and this information should only be shared where it is clinically relevant, e.g. it would be appropriate when referring a trans man for a pelvic ultrasound but not when referring him to ENT.

Disclosure In Relation To A Court Order
The courts, both civil and criminal, have power by virtue of the various pieces of legislation that govern their operation, to order disclosure of information. A court order will generally explain the basis on which disclosure is being ordered, so we have not listed the legislation here

Access to Health Records Act 1990
Access to records of deceased persons

Abortion Act 1967 and Abortion Regulations 1991 (SI 1991 No 499)
Disclosure of information on abortion for purposes specified in the Regulations

Audit Commission Act 1998
Information required to allow the Audit Commission to carry out its functions under the Act

Criminal Appeal Act 1995
Information required by the Criminal Cases Review Commission to assist in the exercise of their functions

Health and Social Care Act 2001
Gives the Secretary of State for Health the power to make Regulations specifying information to be disclosed in the public interest, or in the interest of improving patient care, for England and Wales only

Health (Community Health and Standards) Act 2003
Gives Commission for Healthcare Audit and Inspection right of access to fulfil its statutory functions

Human Fertilisation and Embryology Act 1990 (as amended by the Human Fertilisation (Disclosure of Information) Act 1992)
Disclosure of information to the HFEA

Medical Act 1983
Disclosure of information to the GMC in respect of its powers to investigate complaints

NHS (Venereal Diseases) Regulations 1974 (SI 1974 No 29)
Emphasises the importance of confidentiality but provides for limited sharing of information between doctors

Police and Criminal Evidence Act 1984
Gives power to the police to apply to a court for access to records to assist in an investigation

Prevention of Terrorism (Temporary Provisions) Act 1989
Requires anyone to inform the police of information about terrorist activity

Public Health (Control of Disease) Act 1984 and SI 1988 No 1546
Notification of specified diseases and food poisoning incidents

Road Traffic Act 1988
Gives powers to police to require doctors to provide information which might identify a driver alleged to have committed a traffic offence

SUPPORTING REFERENCES, EVIDENCE BASE & RELATED POLICIES

The Senior Information Risk Owner (SIRO) will direct the IG Lead to take actions as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies in particular:

- The NHS Confidentiality Code of Practice
- Care Record Guarantee
- NHS Records Management Code of Practice Part 2
- NHS IGA GDPR Guidance
- Information Security Management: NHS Code of Practice

Confidentiality Notice

This document and the information contained therein is the property of **The Weobley & Staunton-On-Wye Surgeries**. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from **The Weobley & Staunton-On-Wye Surgeries**.

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.0	01.01.13	Michele Petrie	Michele Petrie	
1.0	30.12.15	Michele Petrie	Michele Petrie	Reviewed – no updates
2.0	23.08.17	Michele Petrie	Michele Petrie	Reviewed – updated legislation
3.0	10.10.18	Michele Petrie	Michele Petrie	Reviewed - updated legislation & practice
3.0	25.09.19	Michele Petrie	Michele Petrie	Reviewed – no updates
4.0	22.10.19	Michele Petrie	Michele Petrie	Updated legislation
5.0	20.11.19	Michele Petrie	Michele Petrie	Reviewed appropriate terminology for LGBT
5.0	1.03.24	Suzi Prince	Suzi Prince	Reviewed – no updates

Appendix A

Weobley & Staunton on Wye Surgeries

CONFIDENTIALITY AGREEMENT FOR STAFF

In the course of your employment or associated work with the Practice, you may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised officer within the Practice, on no account should such information be divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of computer data, will result in disciplinary action, which may lead to your dismissal.

You should also be aware that regardless of any action taken by the Practice, a breach of confidence could result in a civil action against you for damages.

You must ensure that all records, including computer screens and computer printouts of patient data, are never left in such a manner that unauthorised persons can obtain access to them. Computer screens must always be cleared when left unattended and you must ensure that you log out of computer systems, removing your password. All passwords to practice systems must be kept confidential.

No unauthorised use of the internet or email is allowed.

Information concerning patients of staff is strictly confidential and must not be disclosed to unauthorised persons. This obligation shall continue in perpetuity.

Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the Data Protection Act 1998 or an action for civil damages under the same Act in addition to any disciplinary action taken by the Practice.

I have read, understand and agree to the terms and conditions set out above

Signature	
Name	
Date	

Appendix B

Weobley & Staunton on Wye Surgeries

INFORMATION GOVERNANCE SPOT CHECK QUESTIONNAIRE

Location		Date		Auditor	

ICT Security

ICT Security	Comments	Results
How many PCs are within the public area?		
How many are secured against theft?		
How are they secured against inappropriate access?		
How many of these computers are currently unattended and unlocked?		
How many Smartcards were left in the keyboard when desks are currently unattended?		
Is the screen viewable to the public?		

Random check of C drives for confidential information		
Passwords written down or visible?		
How many staff are currently in date with their IG training?		
How many staff are due to undertake their annual IG training in the next month?		

Communication

Communication	Comments	Results
Is the Clear Desk Policy being implemented?		
Is there facility for calls to be taken in privacy?		
Check to see if calls can be heard from the public area		
Is there an answerphone in the public area?		
Is this listened to whilst the public are present?		

Check to see if there is any confidential material left in view		

Physical Security

Physical Security	Comments	Results
Is access to staff only areas restricted by a security device?		
Are there any public areas which are closed for any period eg. lunch?		
Is the area secured against entry during these periods?		

Security of Confidential Information

Security of Confidential Information	Comments	Results
Is confidential information used in a public area?		
What security is used to protect this information?		
Are locked cabinets available?		

Check the reception area, walls and desks to see if confidential information is clearly on view		
Within staff only areas – is confidential information kept secure?		
Can confidential information be seen from outside of the area?		
Have information asset owners and information asset administrators been identified and are they aware of their responsibility?		
Has the Information Risk Management Tool and Information Asset Register been updated to take into account the system and information flows?		
Any other observations?		

Records Security

Records Security	Comments	Results
How are records stored?		

Where are other records stored?		
Where are records archived?		

Disposal of Confidential Information

Disposal of Confidential Information	Comments	Results
Is there any shredding stored in boxes?		
Any other additional information?		

NON-COMPLIANCE OBSERVATION & RECOMMENDATIONS

Detail of Non-Compliance		
Extent of Non-Compliance	Major ☐	Minor ☐
Recommendations		

Detail of Non-Compliance		
Extent of Non-Compliance	Major ☐	Minor ☐
Recommendations		

Detail of Non-Compliance		
Extent of Non-Compliance	Major ☐	Minor ☐
Recommendations		

Detail of Non-Compliance		
Extent of Non-Compliance	Major ☐	Minor ☐
Recommendations		

Appendix C

Weobley & Staunton on Wye Surgeries

INFORMATION GOVERNANCE - NON-COMPLIANCE OBSERVATION & RECOMMENDATIONS

Location		**Date**		**Auditor**	

Detail of Non-Compliance		
Extent of Non-Compliance	Major ☐	Minor ☐
Recommendations		