DATA PROTECTION AND ACCESS POLICY

Context and overview

Introduction

Wyndham House Surgery needs to gather and use certain information about individuals.
These can include patients, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet the surgery's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures **Wyndham House Surgery:**

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

Data protection law

The Data Protection Act 1998 describes how organisations — including Wyndham House Surgery — must collect, handle and store personal information.

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

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- All staff and volunteers of Wyndham House Surgery
- All contractors, suppliers and other people working on behalf of Wyndham House Surgery

It applies to all data that the surgery holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect Wyndham House Surgery from some very real data security risks, including:

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

Responsibilities

Everyone who works for or with Wyndham House Surgery has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Partners are ultimately responsible for ensuring that Wyndham House Surgery meets its legal obligations.
- The data protection officer, Rebekah Lovewell, is responsible for:
- Keeping the practice updated about data protection responsibilities, risks and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Checking and approving any contracts or agreements with third parties that may handle the surgery's sensitive data.
- Evaluating any third-party services the surgery is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The Practice Manager has responsibility for dealing with the following:
- Dealing with requests from individuals to see the data Wyndham House Surgery holds about them (also called 'subject access requests').

- Delt (the IT provider) is responsible for the following:
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Wyndham House Surgery will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the surgery or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the practice manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

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

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the surgery's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

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

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Wyndham House Surgery to take reasonable steps to ensure data is kept accurate and up to date.

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

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

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Wyndham House Surgery will make it easy for data subjects to update the information Wyndham House Surgery holds about them. For instance, via the surgery website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by Wyndham House Surgery are entitled to:

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

If an individual contacts the practice requesting this information, this is called a subject access request.

Subject access requests from individuals should be made in writing, addressed to the Practice Manager or by email, addressed to the data controller, at

wyndhamhouse.surgery@nhs.net. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for a first subject access request. The data controller will aim to provide the relevant data within 30 days. Subsequent requests will provide data collected since the last request free of charge. Requests to provide data already supplied previously will incur a cost as noted on the process guide at Annex 1 The data controller will always verify the identity of anyone making a subject access request before handing over any information, and will obtain a signed acknowledgement of receipt (annex 2).

Where a subject access request is made by a third party on behalf of a patient, (legal advisor etc.) and an appropriate signed consent has been provided, the request will be treated as having been received directly from the patient. The patient will be sent an appropriately completed template letter (annex 4) followed by the provision of the data in the normal manner.

On occasion a third party request for data will be made on behalf of the patient that is not a Subject Access Request and is therefore chargeable. These typically request only a partial disclosure of the medical record. On receipt of these requests the reception staff will verify that the consent given is comprehensive and appropriate, if not they will send the patient a consent verification letter. They will then invoice the requesting organisation for the chargeable amount (which may be updated from time to time) and send the request to the practice manager for action. The practice manager will copy the appropriate portion of the record to an encrypted USB drive and pass this to reception when completed, for sending on

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Wyndham House Surgery will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Partners and from the surgery's legal advisers where necessary.

Providing information

Wyndham House Surgery aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends, the surgery has a privacy statement, setting out how data relating to individuals is used by the surgery (annex 3).

Annex 1

Subject Access Requests

Request arrives from a patient for a copy of their record

Identity of the patient is verified by front desk staff and check made for previous requests (check read code Xalg4)

Front desk staff check to ensure that all available data is in the record (old paper records obtained from Imagestor and scanned)

Task sent to Practice Manager

Practice Manager accesses Pt record on System 1

'Patient – Print – Print Record' then save to desktop

Task sent to usual GP to view record and approve release

On approval from GP

Move all files to USB drive and verify transfer complete

Password protect USB Drive with patient surname plus six digit DOB

Add read code to Patient record Xalg4 and comment 'SAR (date)'

Front desk staff to contact patient and invite in to collect data

Identity to be verified and verifier to make entry in journal that data was collected and obtain signed receipt

Password format to be explained to the patient

Subsequent requests for data access if already carried out previously:

-Data from date of last request to now, to be provided as above free of charge

- Repeat of data already provided will be charged at 8ppp or 12ppp (double sided) for prints, or a single charge of £20 for electronic media.

Annex 2

WYNDHAM HOUSE SURGERY
SILVERTON EXETER DEVON EX5 4HZ
Tel: 01392 - 860024 (24 hrs) Fax: 01392 - 861165
www.wyndhamhousesurgery.co.uk

Dr Anthony O'Brien
Dr Catherine Burkill
Dr Jeffrey Solman

Practice Nurses:
Elaine Rolfe
Liz Huxtable

I, acknowledge receipt of a USB drive from Wyndham House Surgery on (date) containing all of my patient record, and have had the password requirements explained. I understand that a subsequent request for information already provided will incur reasonable charges from the surgery.

Signed _____

Wyndham House Surgery

Privacy Notice

The data that the surgery collects on each of its patients is necessary in order to support high quality healthcare, some examples of this are:

Consultations, test results, medications, allergies etc

Demographic data (address, phone number etc)

Personal data (height, weight, some lifestyle choices etc)

Historical data (past medical history, letters etc)

Some of the information held by us is shared with others:
Other health care providers (e.g. Devon Docs, SW ambulance trust etc) – If you have already consented to this then you need do nothing. You can provide or decline this consent at any time.
Other health care agencies (e.g. National diabetes association, secondary care referrals, etc) – where not a legal requirement we will ask for your consent before providing information. Where it is a legal requirement for us we will publish an information notice and you may dissent at any time
Commercial agencies (e.g. insurance companies etc) we will always seek your explicit consent.
If you have provided us with your e-mail address and/or your mobile phone number we will use these to contact you directly, to send you a text reminder of an appointment or to tell you about a health campaign specific to you. We will not use it for any other purpose.
You can provide or remove your consent at any time. Please speak to the Practice Manager if you have any concerns.

Annex 4

Name
Address

Date

Dear,

Subject Access Request

We recently received a request for your medical records from your legal /insurance advisor.

Increasingly, medical practitioners and the BMA are becoming concerned that insurance companies and the legal profession are using the provisions of the Data Protection Act inappropriately and requesting full access to medical histories when limited information will suffice. Patient records carry a lot of information that is deemed private and sensitive, and many do not realise that this is also provided to the advisor when it may not be relevant or appropriate. However, it is difficult to monitor this as the patient has signed a comprehensive release.

Because of this, we have taken the decision to provide Subject Access Data to the patient directly so that you have the choice to provide full access or not. This does not affect requests for reports directly from the Doctors at the surgery, as this is an established process that monitors that the information released is appropriate.

We will begin to put your record together on a memory stick, and a member of our staff will contact you once it is able to be collected.

I should also point out that, while an initial request for information is free of charge, subsequent requests for information already given will incur a cost. It is important that you retain or recover your information once provided to your advisor.

Yours sincerely

Wyndham House Surgery