Document name: Data Security and Protection Policy

Date created: 11 April 2020

Author: David Wyndham

1. **Introduction**

We recognise that Data Security and Protection is essential for modern optical practices delivering private and NHS services. We take the security and protection of our patients' data extremely seriously. All data will be processed in full accordance with the Data Protection Act 2018 incorporating GDPR. This Policy includes the requirements of the national Data Security Standards applicable to an optical practice.

The Practice's Senior Information Risk Officer (SIRO) is responsible for implementing this policy in conjunction with Practice management. The SIRO will also work alongside the Practice's Data Protection Officer (DPO) and the Practice's Caldicott Guardian.

- The Practice's SIRO is **David Mack** (Data Security Standard 1.1.1).
- The Practice's DPO is **David Mack** (Data Security Standard 1.1.6).
- The Practice's Caldicott Guardian is **David Wyndham** (Data Security Standard 1.1.3).

The Practice is registered with the Information Commissioner. Our registration number is **Z6894129**

Expires 29/07/2021

The Practice has an up to date Freedom of Information Act statement which is available to patients. The Practice has a separate Privacy Policy which explains individuals' rights under GDPR (see Appendix 1) (Data Security Standard 1.3.3).

This Data Security and Protection policy, including the list of all systems/information holding personal information, is reviewed annually or more frequently as required (Data Security Standard 2.1.1.).

2. Purpose

The purpose of this policy is to demonstrate the measures we take to ensure data security and protection. It describes the data that we hold about patients, how we hold it, how we protect it, how we use and process it (including what patients need to be provided with) and how we transfer it (Data Security Standard 1.2).

3. Audience

The audience of this policy is:

- Our staff
- NHS England and other commissioners
- Patients
- Other stakeholders.

3.1. Distribution plan

The policy is provided to all staff. It is used to demonstrate contract compliance to NHS England. It is available to view on request to any other interested party.

3.2. Training plan and support

The Practice's SIRO will conduct a data security and protection Learning Needs Analysis (LNA) (Data Security Standard 3.1.1) for current and new staff. This will identify overall data security and protection skills and knowledge gaps for both the

whole team and specific individuals to help the practice meet its future needs and developments. LNAs will use a combination of questionnaires, staff discussion groups, job analysis and evaluation and desktop reviews.

Findings from the LNA will be used by the SIRO to develop group and individual training programs suitable to role, with learning priorities (Data Security Standard 3.1.3 and 3.1.4). A data protection and security induction is in place for new members of staff (Data Security Standard 2.3.1).

All staff will pass the data security level 1 test (Data Security Standard 3.3): https://www.dsptoolkit.nhs.uk/Help/30. [1]

Training will be held at regular intervals to ensure all staff are familiar with this policy's contents and practical applications. Staff with specialist roles will receive suitable training to those roles (Data Security Standard 3.4). The SIRO will also be responsible for ensuring management is suitably trained (Data Security Standard 3.5).

Training outcomes will ensure that users know what constitutes a breach incident, how to spot these and where to report them to (Data Security Standard 6.2).

4. Roles and responsibilities

The Practice maintains a current record of staff and their roles (Data Security Standard 4.1.1). We understand which members of staff have access to particular systems (Data Security Standard 4.1.2). We also audit account users regularly. (Data Security Standard 4.2.1). In the event of a mismatch between user role and system access granted we will make a list of incidents and rectify each situation (Data Security Standard 4.2.2).

[1] As commercial third parties the Practice accesses the training by submitting its ODS code and filling out the form through this link: https://millennium.kayako.com/nhsdigital/Tickets/Submit

All staff understand their responsibilities to handle information responsibility and their personal accountability for deliberate or avoidable data breaches. Staff are aware that IT systems are logged and their duty to use IT responsibly. Staff recognise that if they have acted inappropriately they may have action taken against them. We will display an acceptable usage banner on our systems including a personal accountability reminder for staff (Data Security Standard 4.3.5), liaising with our service providers as necessary.

All systems administrators have signed an agreement which holds them accountable to the highest standards of use (Data Security Standard 4.3.1). Systems administrator activities are logged, and these logs are only accessible to appropriate personnel (Data Security Standard 4.3.2).

Where our systems do not support individual login making it difficult to carry out user audits we hold a list of these systems (Data Security Standard 1.4.5).

We practice role-based access to ensure that information is used only by those with a need to use it (Data Security Standard 1.6.3). We will implement physical controls to areas of our systems where full access is not appropriate (Data Security Standard 1.6.4).

5. Process/ Procedure

The Practice has a number of processes in place to ensure patient data security and protection.

<u>The Practice holds a patient records in a variety of formats:</u>

- Paper records for sight test and contact lens clinical records (historical).
- Paper records for spectacle prescription and dispensing information (historical).
- Clinical records are held electronically on computer with up to date virus protection. We will record incidents picked up by virus protection (Data Security Standard 6.3.2), number of spam emails blocked per month (Data Security Standard 6.3.3) and number of emails being filtered per month (Data Security Standard 6.3.6).
- Spectacle prescription and dispensing information in the practice management software.
- Recall dates held in the practice management software.
- Photographic information (retinal and anterior segment) held in the imaging software.
- Visual Field records held either as paper (historical), as data in the VF software or as images within the imaging software.
- Appendices to this policy sets out minimum retention periods for types of records and the action to be taken when records are securely destroyed or archived (Data Security Standard 1.8.1). We hold a separate records retention schedule (Data Security Standard 1.8.2).

<u>This information is protected in the following ways:</u>

- All practice staff have a confidentiality clause within their contracts.
- There is a clear understanding of what personal confidential/sensitive personal data is held (Data Security Standard 2.1).
- All personal information contained on practice records, whether paper or electronic, is considered confidential.

- We will not discuss personal information with anyone other than the patient or, if under 16 and not Gillick competent, patients' parent or guardian without their permission.
- Care is taken that records are not seen by other people in the practice.
- All staff are aware of the importance of ensuring and maintaining the confidentiality of patients' personal data and that such data must be processed and stored in a secure manner. There is approved staff guidance on confidentiality and data protection issues (Data Security Standard 1.5.1).
- All electronic data is protected by suitable back-up procedures and any on-line backup uses a service, which encrypts the data securely before transmitting it from the practice PC. (See also our separate "guide to preparing a backup policy" below.)
- When computers are replaced, old hard drives are securely erased or physically destroyed.
- Records are retained for periods as agreed by the optical bodies.
- Confidential paper information requiring destruction is shredded.
- Records due for destruction are shredded.
- If the need arises to transfer information we have procedures that include consent and secure transfer. (See section on how we transfer personal data below).
- Any suspected breaches of security or loss of information are reported immediately and are dealt with appropriately by the SIRO.
- Paper records are kept secure and away from access by the public.
- Patient identifiable information must not be removed from the optical practice.

To discharge our legal and contractual duties:

- When patients have a sight test they will be given a copy of their spectacle prescription as soon as their sight test is completed.
- We will give patients a written statement that they are being referred, with the reason for the referral *(e.g. "cataract"*) written on the GOS2 or similar private form.
- If patients are fitted with contact lenses they will be given a copy of their contact lens specification when the fitting process has been completed.
- We make sure that staff who help in the provision of GOS are appropriately trained and supervised for the tasks that they undertake.
- We may also use the information we hold about patients to remind them when they are due for check-ups and we may send them eye care and eyewear information. Patients can opt out from this.
- In addition to the Data Protection Act 2018/GDPR we will comply with the Accessible Information Standard (AIS). Staff are required to implement the Optical Confederation's AIS guidance: http://www.opticalconfederation.org.uk/downloads/accessibleinfoguidanceopticalconfedjuly16.pdf

Patient data (information flows) is always securely transferred:

- We will normally ask patients' permission if we want to transfer personal information about them to someone else.
- We may not ask permission if we transfer the information to another healthcare professional who is responsible for patients care and who needs that information to help to care for patients.
- We may also not ask patients permission if we are ordered by law to transfer the information. This may be if a court asks us for the information.

- We hold a record that details each use of sharing of personal information including the legal basis for the processing (Data Security Standard 1.4.1). These information flows have been approved by the SIRO (Data Security Standard 1.4.2) and the Practice's management (Data Security Standard 1.4.3). We also hold a list of all systems/information assets holding or sharing personal information (Data Security Standard 1.4.4).

Breach reporting

In the event of a data breach occurring an internal data security and protection breach reporting system is in place (Data Security Standard 6.1). Staff will report data breaches to the SIRO who will in turn report it to management. Breaches will be logged, and root cause analysis undertaken to investigate the incident. Training will be conducted as necessary to mitigate against future occurrences.

Incident reporting

We hold a Business Continuity Plan which includes provision for data security incidents and staff understand how to implement this (Data Security Standard 7.1). This has been approved by the SRIO (Data Security Standard 7.1.2). We test and review this plan annually (Data Security Standard 7.2) and record attendees signatures and roles (Data Security Standard 7.2.1). We have planned for all risks potentially impacting on the Practice's business continuity (Data Security Standard 7.2.2). We will document issues and record which staff members are responsible for which actions (Data Security Standard 7.2.3).

All emergency contacts are kept securely, in hardcopy and are up to date. Staff are aware of where to locate these. The contact lists are updated as required (Data Security Standards 7.2.4 to 7.2.7). In the event of cyber-attack, we will document lessons learned and integrate these into our Business Continuity Plan (Data Security Standard 7.2.10).

Software

All our software used is surveyed to ensure it is supported and up to date, working with our software providers as necessary (Data Security Standard 8.1). Connected systems are kept up-to-date with the latest security patches (Data Security Standard 8.3). While we do not use unsupported software, in the unexpected event that we do in the future, we will categorise and document this to identify and manage security risks (Data Security Standard 8.2). If patches are not applied for a greater period than two months the SIRO will be notified with explanation why (Data Security Standard 8.3.4).

IT Networking

All networked systems have had their default passwords changed (Data Security Standard 9.1). We risk assess our networking protocols to ensure that penetration tests are not required given the size of our organisation (Data Security Standard 9.3). Feedback from this is presented to the SIRO to devise a data improvement plan (Data Security 9.4). Our management evidences discussion of the top three data security and protection risks that arise from network testing (Data Security Standard 9.4.3).

Reviews

As part of our review of our Data Security and Protection policy annually we will review all processes above (Data Security Standard 5.1). As an optical practice we will include clinicians (optometrists and dispensing opticians) in this comprehensive review (Data Security Standard 5.2). We will take action to address problem processes (Data Security Standard 5.3).

6. **Monitoring of compliance and effectiveness of implementation** The SIRO has operational responsibility for monitoring compliance and effectiveness of

implementation. However, ultimate responsibility sits with the Practice's management. Staff have provided explicit understanding that their activity of systems can be monitored (Data Security Standard 4.3.5).

The SIRO will conduct regular compliance monitoring/staff spot checks to ensure that this policy and associated guidance is being followed (Data Security Standard 1.5.2). Results will be followed upon by the SIRO and management as necessary (Data Security Standard 1.5.3).

Monitoring of access to systems to which users and administrators have access to is carried out by the SIRO and listed (Data Security Standard 4.3.5).

<u>The Practice is aware of its responsibilities under GDPR.</u>

Individuals' rights are respected and supported as per GDPR 12-22 (Data Security Standard 1.3). All data will be processed in full accordance with the Data Protection Act 2018 incorporating GDPR. We ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.

- 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- 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.

All transparency information required by GDPR (Articles 13 and 14) relating to the public being properly informed of the use of their personal information and rights is published by the Practice within its privacy policy and is therefore available to patients and the public (Data Security Standard 1.3.2).

We hold a staff procedure on providing information about processing and individuals' rights under GDPR (Data Security Standard 1.3.4). This includes information about meeting subject access requests to meet shorter GDPR timescales (Data Security Standard 1.3.5). We hold details of how any information requests have been complied with in the last twelve months (Data Security Standard 1.3.6) in the format below:

For period dd/mm/yy to dd/mm/yy	
No of SARs	
No of SARs late	

No of FOI	
No of FOI late	

Practice staff are required to be familiar with Optical Confederation guidance on GDPR: http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance-version-15-december-final.pdf

The Practice can name its suppliers, the products and services they deliver and contract durations (Data Security Standard 10.1). Any contracts we hold with third parties that handle personal information are compliant with GDPR (Data Security Standard 10.1.2). We have secured statements from suppliers confirming their compliance with GDPR (Data Security Standard 10.2.3). We have also conducted basic due diligence against suppliers as per ICO and NHS Digital guidance (Data Security Standard 10.2).

In the event of any disputes between us and our suppliers we will record these, noting any risks to data security (Data Security Standard 10.3). In the event of instances where we cannot comply with data security standards because of supplier-related issues we will record these and discuss them at management level (Data Security Standard 10.4). Suppliers required to do so have completed the Data Security and Protection Toolkit at a level appropriate for their profile (Data Security Standard 10.5).

Data Protection Impact Assessments

We conduct Data Protection Impact Assessments (DPIA) that follow relevant ICO guidance. (Data Security Standard 1.6.7). DPIA guidance has been agreed by management in consultation with the DPO (Data Security Standard 1.6.8 and 1.6.9).

Our DPIA is published in the interests of transparency (Data Security Standard 1.6.13).

7. Appendices

Appendix 1

The Practice holds its own Privacy Policy.

Appendix 2

Guide to preparing a Backup Policy

You should describe your own practice backup procedures. These might include some or all of the following:

- Mirrored hard drives for business continuity
- Regular backups to:
    - DVD *(Low quality dyes used on cheap CD/DVD-R can cause optical disks to degrade and lose data within a couple of years)*
    - USB memory sticks
    - External hard drives
    - NAS devices (Network Attached Storage)
    - Online backup services
    - Remote company servers
    - Tape devices.

Points to bear in mind when devising a policy:

- It is useful to be able to restore quickly – this may mean an onsite copy of the backup.
- Store onsite backups and software discs in a fireproof safe.
- It is important for safety to keep a backup off site.
- Any data taken offsite should be secure (password protected or not left unattended and/or locked away).
- If online backup services are used (and some are very simple and convenient these days), ensure that it encrypts the data securely before transmitting it from the practice PC (most do so).
- Full backups take longer than incremental backups.
- Restores from full backups are quicker than those from incremental backups

    - i.e. don't do too many incremental backups between full backups.
- If your backup is not a mirror or snapshot of the hard drive, but a copy of the data, then you will need to restore the operating system and programmes as well as the data. Ensure that you have copies of the original software discs safely stored.

Backups are only any use if (a) they are carried out regularly and (b) they work. Don't leave any longer between backups than you feel you can afford in terms of the time it will take to re-input lost data. Daily is generally appropriate. Do ensure that your backup works. Even if you don't wish to try an actual restore, do check that the backup is running when you think it is, that it completed rather than stopped with an error message and that the data is present in the backup.

Appendix 3

RECORD RETENTION

- This policy applies to the following:
    - Spectacle records
    - Contact lens records
    - Appointment diaries
    - Telephone and/or tele-health consultations.
- All records are retained for 10 years* from the date of last seeing the patient.
- Records of children are retained until they are 25 AND it is 10 years since they were last seen.
- Records of the deceased are kept for 10 years.
- Records are destroyed by shredding.

  Examples:

Age at last test	**Time to retain record**
Age 5	Until age 25
Age 10	Until age 25
Age 17	Until age 27

* Although 7 years is the minimum requirement in GOS contacts, 10 years is the minimum recommended by the optical representative bodies. The rights to be forgotten/erasure under GDPR does not extend to health records.

Over 18	For 10 years

Appendix 4

Recording of telephone calls and/or consultations

Telephone calls between patients and providers will not be recorded or monitored due to the complexity of obtaining consent for this process and the subsequent storing of patient sensitive data.

If telephone calls are to be monitored and/or recorded a specific policy will be required taking into account:

- Regulation of Investigatory Powers Act 2000 ("RIPA")
- The Telecommunications (Lawful Business Practice) (Interception pf Communications) Regulations 2000.
- The Data Protection Act 2018
- The Employment Practices, Data Protection Code.
- Human Rights Act 1998
- Code of Practice – FSA Handbook – Code of Business Handbook and Direct Marketing Association's Code of Practice, PCI DSS.
- Telecoms Licence obligations – The Service Provision Licence

Communications strategy and Implementation plan

The provider should have readily available information relating to paragraph 2(3) of Part II of Schedule 1 of the Data protection act.

(2)A data controller is not obliged to supply any information under subsection (1) unless he has received—

(a)a request in writing, and (b)except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

[F2(3)Where a data controller—

(a)reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks, and

(b)has informed him of that requirement, the data controller is not obliged to comply with the request unless he is supplied with that further information.]

Appendix 5

Disclosure of data to commissioners

The practice (provider) agrees to provide anonymised, pseudonymised or aggregated data as may be requested by the co-ordinating commissioner or LOC Company/Primary Eyecare Company

Personal data will not be disclosed without written consent or lawful reason for disclosure.

Exceptions to this are covered by:

Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001), allows the common law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

Data Protection Principles

Personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

Appendix 6

NHS Care Record Guarantee

All data processed on behalf of the commissioner with regard to community services must be processed and handled in line with the NHS Care Record Guarantee.

All staff handling data should be aware of the obligations placed upon them by the NHS Care Record Guarantee and the commitments laid out in it.

In summary this covers:

Why people may access patient records:

- As the basis for health decisions
- Ensure safe effective care
- Work effectively with other
- Clinical audit
- Protect health of the general public
- Monitor NHS spending
- Manage the health service
- To investigate complaints
- Teaching and research.

Law relating to records:

- Confidentiality under common-law duty of confidentiality
- Protection about how information is processed (Data Protection Act 2018)
- Privacy (Human Rights Act 1998)

These rights are not absolute, and they need to be balanced against those of others.

Other patient rights regarding records

- To ask for a copy of all records held in paper or electronic form (a fee may be payable for complex or repeated requests)
- To choose someone to make decisions about the patient's healthcare if the patient becomes unable to do so (lasting power of attorney).

Duties placed upon the practice (provider)

- Maintain accurate records of the care provided
- Keep records confidential, secure, and accurate (even after the patient dies)
- Provide information in accessible formats (e.g. large print).

The complete NHS Care Record Guarantee will be available for staff members to consult.

Appendix 7

Caldicott Principles

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law.

Quality Statements

1. Patients are treated with dignity, kindness, compassion, courtesy, respect, understanding and honesty.
2. Patients experience effective interactions with staff who have demonstrated competency in relevant communication skills.
3. Patients are introduced to all healthcare professionals involved in their care and are made aware of the roles and responsibilities of the members of the healthcare team.
4. Patients have opportunities to discuss their health beliefs, concerns and preferences to inform their individualised care.
5. Patients are supported by healthcare professionals to understand relevant treatment options, including benefits, risks and potential consequences.
6. Patients are actively involved in shared decision making and supported by healthcare professionals to make fully informed choices about investigations, treatment and care that reflect what is important to them.
7. Patients are made aware that they have the right to choose, accept or decline treatment and these decisions are respected and supported.

8. Patients are made aware that they can ask for a second opinion. (This would not be funded by GOS as there is no mechanism for this).
9. Patients experience care that is tailored to their needs and personal preferences, taking into account their circumstances, their ability to access services and their coexisting conditions.
10. Patients have their physical and psychological needs regularly assessed and addressed, including nutrition, hydration, pain relief, personal hygiene and anxiety. (This statement will to all intents and purposes not apply to optical services).
11. Patients experience continuity of care delivered, whenever possible, by the same healthcare professional or team throughout a single episode of care.
12. Patients experience coordinated care with clear and accurate information exchange between relevant health and social care professionals.
13. Patients' preferences for sharing information with their partner, family members and/or carers are established, respected and reviewed throughout their care.
14. Patients are made aware of who to contact, how to contact them and when to make contact about their ongoing healthcare needs.

Appendix 8

Handling requests for prescription and clinical information

Spectacle prescription (Spec Rx) or contact lens specification

Where a patient requests a copy of their own, or their child's spectacle prescription or contact lens specification this will be provided. It will be double checked for accuracy and signed by an optometrist. Such information may be collected or posted or faxed to the patient. It may also be emailed to their personal email address if they so request.

Contact lens specification

Where a 3rd party supplier requests the verification of a contact lens specification they should provide the following details:

- Patient's full name and address
- Full specification including parameters and power of the lenses
- An expiry date of the specification
- The name or registration number of the person signing the specification.

The answer can only be yes or no; the details are correct or not. If the details are not correct, further information must not be supplied without the explicit consent of the patient. In that event the supplier should be told that a copy of the specification, with all the correct details, will be posted to the patient. The request, and the result, should be noted on the patient's record.

Requests from another optometrist for spec Rx information

In all cases you should be satisfied that the patient has consented to the transfer of the information. That may be obvious and implicit "the patient is on holiday elsewhere and has broken their glasses", but if not, ask to speak to the patient or for

a signed consent to be faxed to us. The request should be noted on the patient's record.

Requests from another optometrist for clinical information

The optometrist should satisfy themselves that the request is for the clinical and health benefit of the patient and should conduct the phone conversation and provide the information themselves. They should also be satisfied that the patient has consented to the transfer of information.

Requests by us for clinical or spec Rx information.

These requests will be made by the optometrist personally. A signed consent should be held in case this is requested by the other party. If the information is not urgent the request may be made in writing.

Appendix 8

Communicating Patient Identifiable Data

Patient data may be communicated in the following ways:

By ordinary 1st or 2nd class post

- This will be in a sealed envelope

By fax

- This will be to a safe haven fax where possible. The cover sheet will state:

This fax contains proprietary confidential information some or all of which may be legally privileged and or subject to the provisions of privacy legislation. It is intended solely for the addressee. If you are not the intended recipient, you must not read, use, disclose, copy, print or disseminate the information contained within this fax. Please notify the author immediately by replying to this fax and then destroy the fax.

By email:

Patient consent is required for sending data that can identify a patient except where both sender and recipient have NHS emails ending in @nhs.net, or the "SECURE" function of NHS mail is used.

Emails will carry a message stating:

This e-mail contains proprietary confidential information some or all of which may be legally privileged and or subject to the provisions of privacy legislation. It is intended solely for the addressee. If you are not the intended recipient, you must not read, use, disclose, copy, print or disseminate the information contained within this e-mail. Please notify the author immediately by replying to this e-mail and then delete the e-mail.

Verbally

- With care that confidentiality is maintained
- The recipient of the information is identified
- A note is made on the record.
- Information that could result in errors will be communicated in writing where possible