Document name: KennetLahti optical Glazing ltd Ltd’s [Specialist Data Security and Protection Plan]

Date created: 27 September 2022

Author: Kennet Lahti

1. Introduction

The Practice recognises that a Data Security and Protection Plan is necessary to ensure that it is best placed to deal with the specialist nature of data incidents. Data Security is essential for protecting patients and ensuring that the Practice maintains its reputation, and that commissioners are confident that we are fulfilling our responsibilities. This Plan is designed to prepare our response to data incidents so that we may mitigate the effects of these as best as possible.

2. Purpose

The purpose of this plan is to ensure that the Practice’s staff implement the specialist data security and protection plan following a serious data incident and ensure that the business continues for the benefit of our patients.

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

Training will be as per the Practice’s Data Security and Protection Policy. In addition, Practice management and the information lead will conduct regular sessions ‘testing’ this plan to ensure that staff implement it correctly in the event of a real incident.

4. Roles and responsibilities

All staff are responsible for ensuring that patients’ information rights are understood and that requests are processed correctly and within correct time periods. Staff management and the information lead hold the ultimate responsibility for ensuring that the Practice is meeting its requirements.

5. Process/Procedure

Staff use the following matrix to determine the likelihood and impact of a data security incident:

Risk Assessment descriptors: Use the descriptors below to assess the Likelihood of a risk occurring					
Score	**5**	**4**	**3**	**2**	**1**
Descriptor	**Probable**	**Possible**	**Unlikely**	**Rare**	**Negligible**
Likelihood of occurrence	More likely to occur than not	Reasonable Chance of occurring	Unlikely to occur	Will only occur in rare circumstances	Will only occur in exceptional circumstances
	>50% chance	50% to 5%	5% to 0.5%	0.5% to 0.05%	0.05% to 0.005%
	>1 in 2 chance	1 in 20 chance	1 in 200 chance	1 in 2000	1 in 20,000
Risk Impact: **Use the descriptors below to assess the Impact severity if a risk occurs**					
Score	**5**	**4**	**3**	**2**	**1**
Descriptor	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Severity of Impact	Permanent loss of core service or facility	Sustained loss of service which has serious impact on delivery of patient care	Some disruption in service with unacceptable impact on patient care. Non-permanent loss of ability to provide a	Short term disruption to service with minor impact on patient care	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide a

The likelihood and impact of data incidents are recorded here:

Record the likelihood and impact of potential hazards and /or threats together with the recovery time frame options.

			Option 1	**Option 2**	**Option 3**
Hazard or threat	Likelihood Score	Impact Score	(2 hours)	(24 hours or more)	(5 days or more)
Loss of computer systems/ essential data					
Loss of the telephone system					
Loss of essential					
Loss of optical practice					
Loss of security systems					

In the event of a data incident occurring the following plan is to be used:

Incident Occurs

↓

Company reports to local reporting systems

↓

Inform patient of serious incident management in process – ideally within three days

↓

Grade incident (grading chart below)

↓

Notify commissioning body within two working days

↓

Incident reported on Serious Incident Reporting and Learning Framework within two working days

↓

Consult commissioner as necessary over grading

↓

The Company to establish appropriate investigation

↓

Undertake investigation communicating with relevant local health bodies, patients and carers if applicable

↓

Develop action plan

↓

Submit incident investigation report to commissioner

↓ ↓

Implement action plan → Commissioner closes incident

↓

Share lessons learned if appropriate

↓

Review actions taken

The grading chart below is used to determine post-incident action:

Incident Grade	**Example Incidents**	**Investigation Grade and action**	**Timeframe**

1	Data loss and information security.	**Investigation Level 1:** Concise root cause analysis (RCA) for both No Harm and Low Harm and/or where the circumstances are very similar to other previous incidents. A concise RCA will enable the Company to ascertain whether unique factors exist, thus focusing resources on implementing service improvement. **Investigation Level 2:** Comprehensive RCA for incidents causing moderate to severe harm or death. The Company's policy is this will be the default investigation level for grade 1 incidents. The Company may seek advice and services from specialist external sources as required.	The Company to submit initial report within two working days. The Company will submit completed investigation within 45 working days.
2	Data loss and information security (DH Criteria level 3-5).	Comprehensive RCA.	Initial report within 2 working days. The Company will submit a completed investigation within 60 working days.
	Selected grade 2 incidents These might include major systemic failure with multiple stakeholders.	**Investigation Level 3:** Independent RCA.	Initial report within 2 working days. Independent investigators should be commissioned to complete an investigation

6. Monitoring of compliance and effectiveness of implementation

Practice management and the information lead monitor staff to ensure familiarity with this process. Any gaps in knowledge are addressed through training.