Penguin GDPR Statement

Cievert Ltd.

18th October 2018

Category	Information Governance
Version	1.0
Classification	Public

Document Control

Organisation	Cievert Ltd
Title	Penguin GDPR Statement
Author	Chris Kennelly
Filename	Penguin_GDPR Statement_v1.0 (FINAL)_Oct 2018
Owner	Chris Kennelly – Managing Director
Subject	Information Governance
Protective Marking	Public
Review date	N/A

Revision History

Revision Date	Version Number	Revised By	Description of Revision

Table of Contents

1. Introduction

1.1 Purpose and Scope

This document sets out why the Penguin application when used in accordance with our recommendations complies with GDPR and is suitable for use in clinical practice across the NHS and private healthcare providers.

Cievert Limited is committed to protecting the personal privacy and choices of all data subjects whose personal data is processed using Cievert products and software. This document is not intended as a patient facing privacy policy for the Penguin application.

This document should be read in conjunction with the accompanying technical specification for the Penguin software application which can be found here http://cievert.net/document. This document provides our analysis of the compatibility of the Penguin application with the GDPR (when used in accordance with our recommendations).

The aim is to set out our analysis of how the application is compatible with the GDPR, and guidelines published to date by the Information Governance Alliance and the Information Commissioner's Office, in order to provide prospective stakeholders and purchasers/subscribers to the application with an overview of the key GDPR considerations arising under the application. It is not intended as a substitute for you (or your Trust's Information Governance Lead) carrying out your own risk analysis of GDPR compatibility and risks presented by your own practices, IT environment or use of the application.

The document encapsulates the design of the application at the time of writing and acknowledges that requirements, designs, minimum requirements and any other specifications as detailed in this document and the accompanying specifications are subject to change. We will update this document regularly to the extent that any such design changes for the application impact upon the GDPR analysis set out herein.

1.2 Definitions

The document uses the term 'application' to refer to the Penguin software described in the accompanying technical specification document, along with the hosting and storage environment associated with it.

'patient' includes the person and the user role reserved for patients on the system. 'consultant' refers to consultants, clinicians and anyone using the system in a clinical capacity. 'administrator' refers to a special system user that has privileges above the standard system user to redefine system behaviour.

1.3 Overview of Penguin

Please see the accompanying technical specification for a more complete description of the application and the various cybersecurity and verification measures in place for the application. Briefly, for the purposes of this document, the application allows for the creation of questionnaires and the recording of patient responses. The questionnaires will be created by the clinician from templates available in a specific clinician only interface. The questionnaire can then be accessed via a patient interface. The interface will list several questions, relevant to the treatment and reflecting the expected side-effects experienced by

the patient. The patient can then complete the questions, providing a representation of the state of their current wellbeing. The application will store the patient response for a given day. The same question set can then be presented to the patient at intervals and the data captured as before. Numerous repetitions of the above process allow for the monitoring of patterns and behaviours during the recovery period.

From this recorded data, markers can be created that will allow any remarkable patient response to be flagged to a consultant for their attention. The model used for patient recovery data capture is that of a mini-questionnaire related to their exact treatment and associated side-effects.

The application is a web-based software application. The first iteration is localised as a server-based web-app, accessible via browser for use onsite only by clinicians, and patients under supervision. Thus the current version remains within the four walls of the hospital Trust/purchasing organisation and all personal data is preserved within the N3 secure system/virtual private network. As such, all personal data entered into the application is preserved within the same IT approved and maintained network environment as is already in use for the storage and processing of patient's personal data in the NHS.

Subsequent versions of the application will be moving outside the N3 environment once approval has been gained for the move from the Trust's Information Governance Lead. The move outside the N3 environment will not occur without your admins and IG leads being fully aware and will be subject to their approval. Once the move outside N3 has been approved, future versions of the application should include additional software components and platforms, including a SmartPhone app to support remote use of the application, and separate sub-systems to support data analysis and predictive analytics. This addition is being postponed for the timebeing due to the unresolved issue of perceived potential security concerns for NHS stakeholders of data flow outside of the N3 virtual private network.] There are currently[, and when the extra-N3 system is established will be further,] numerous cybersecurity measures taken to ensure the databases storing patient personal data are kept secure, isolated and inaccessible by the patient interface (only upload of questionnaire responses will be allowed from the patient interface). You can see a visual illustration of these technical security and isolation measures in the enclosed diagram. Essentially, in establishing remote access outside the N3 network, a separate server would present the questionnaire to the patient and temporarily (pending transfer to the main database) store the patient's answers. The core application would then use an encrypted hash to pull the answers from the server onto the secured central database. Only once safely within the limits and secured environment of the core application would any link be created between patient identifiable data and answers provided. These measures are discussed in greater detail in the technical specification for the future iterations of the application. Thus the main threat to security – namely an insecure interface presented by the patient and its access – is isolated from and prevented from causing issues for the main database repository for Penguin.

In terms of server security, both in the current N3 environment and going forward, access to the server will be granted to Cievert Ltd. development staff only via SSH secure authentication. Deployment of code will be made manually and under full control of the development staff. This means no third-party deployment tools will be used to update live

instances of the code. In addition, all databases used for the application will require authentication with username and password.

Cievert uses password supported SSH encryption rather than a plain key since access to the server may give access to the database where the application's source code and database are housed on the same server.

As an additional note, the PHP code that drives the system is housed outside the web-root directory so incorrect configurations will not risk exposing the code content of the web application.

2. GDPR and Penguin

2.1 Key changes in the legislation

The law on personal data protection changed in May 2018, when the Data Protection Act 1998 was replaced by the EU General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018"). The new legislation increases rights for individuals and places additional obligations and compliance requirements on those involved in processing personal data. Some key changes in the context of clinical care include:

- consent to processing will only be valid where it can be freely given;
- processors (such as Cievert as a provider of applications and eventually cloud based software as a service, which stores patient personal data on behalf of clinicians) now have direct liability for breach of the data protection legislation;
- pseudonymised data must be treated in accordance with the data protection legislation. Only truly anonymised data will fall outside the GDPR and DPA 2018.

2.2 Personal data

Personal data is any information which identifies an individual living person. It is data from which a person can be identified directly; but also includes data where the person can only be identified indirectly from that information in combination with other information. Personal data may also be special category personal data, including information about a person's health, sexual health or sexual orientation. Special category data is considered to be more sensitive than other types of personal data and can only be processed and collected in more limited circumstances than ordinary personal data.

In using Penguin both the clinician and the patient will be inputting and generating a lot of personal data about that patient, including special category data. That information may include the patient's name, address, date of birth, height, weight and gender. Other types of special category data likely to be gathered or generated as part of using the Penguin application will include ongoing health conditions, information about lifestyle, the healthcare providers' opinions about the patient, the patient's condition and how they have responded to treatment. All of this information is personal data, and must be processed in accordance with the data protection legislation.

Another key change is that pseudonymised data must also be treated in accordance with the data protection legislation. Data only ceases to be personal when it is stripped of all personally

identifiable information and is truly anonymous. Thus patient data which is stripped of name, address and dob, and identified instead by e.g., a randomly generated unique identifier (i.e., pseudonymised) must still be treated in accordance with the GDPR, even by those who do not hold the encryption key or other means necessary for re-identifying the data. Pseudonymisation is a key method of protecting personal data and a security measure encouraged under the GDPR. But it does not take the data outside the remit of the GDPR. Thus Penguin uses pseudonymisation as a key measure in keeping patient data secure during its transmission and storage, but Cievert continues to treat all such pseudonymised data in accordance with the GDPR as if it was still in directly identifiable form.

Pseudonymised data must be treated the same way as personal data. As such, Cievert as a processor of pseudonymised patient data has key primary responsibility and liability when processing personal data on behalf of the Trust via the Penguin application.

2.3 How does Penguin process personal data

The accompanying technical specification sets out in detail how Penguin processes personal data, how patient data is captured (patient and consultant input), how it is transferred (secure means) and where it is stored (current N3 VPN). In future Penguin's secure cloud storage provided by third party host with whom Cievert hold GDPR compliant processing arrangements. That technical information is also summarised in section 1 of this document, and the diagrams at the end of this document.

In non-technical terms, the only ways in which we process patient data are in accordance with the consultant/Trust's instructions and criteria. Essentially the Penguin application is a system into which the clinician and patient input personal data, which is then subject to the software's predetermined processing and the outputs and other data stored as set out above. Cievert only accesses the Penguin application in order to deliver the contracted services which include support services, trouble shooting and system maintenance. Cievert does not harvest the personal details of patients for any purpose, it does not use the personal data for any purpose, it merely facilitates the client-patient use and interaction with the application to allow the functionality briefly described in the introduction.

Within the terms of the data protection legislation, Cievert only ever acts as a processor of patient data acting on the instructions and on behalf of the data controller – being the hospital/clinician/NHS Trust as the case may be.

2.4 What are the relevant GDPR lawful grounds and special conditions for processing in Penguin

The GDPR requires organisations (controllers) responsible for processing personal data to demonstrate compliance with the GDPR. To achieve compliance controllers must identify and publish (via appropriate, fair and transparent privacy notices targeted to the relevant data subjects) a lawful basis for the processing taking place, and (in addition) a special condition if processing special category data.

The legislation also requires that where controllers appoint third parties, such as software as a service and cloud storage providers, to carry out processing of personal data on behalf of the controller, that the controller and processor enter into appropriate written processing terms, which satisfy the requirements set out in Article 28 GDPR. Such processors, (which is

the category into which Cievert is placed in respect of patient data processed via the Penguin application), rely upon the instructions given by the controller, the fair privacy notices provided by the controller and the lawful grounds for processing established by the controller. We have entered into an appropriate processing contract with the Trust in which you operate. The processing contract between Cievert and the Trust contains all those elements required under Article 28 for processing contracts.

As briefly mentioned above, in the context of the personal data protection legislation, consent may no longer be considered the appropriate (or fair) lawful ground for processing patient data in the context of direct health care services. It is essential to understand that there is a difference between consent from patients required for other purposes, for example consent to treatment, consent to access other confidential records and so on. Such consents will continue to be required. However, it is likely to be appropriate (and in almost all cases preferable) to rely on grounds other than consent when looking at the lawful justification for personal data processing. As stated in the IGA guidelines on lawful grounds for processing in the context of healthcare:

> *"Health and social care organisations will need to apply another basis for their processing [other than consent], typically: 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'. Relying on this lawful basis requires that: 1) it is necessary for the controller to process the personal data for those purposes (i.e. it is reasonable, proportionate and you cannot achieve your objective by some other reasonable means); and 2) the controller can point to a clear and foreseeable legal basis for that purpose under UK law (whether in statute or common law). The legal basis does not need to refer specifically to the processing of personal data but must establish the 'official authority' to conduct the activity for which the processing is necessary."*

[The NHS is funded by the public purse in order to conduct tasks that are considered to be in the public interest, thus the public task ground will apply to all NHS clinics and activities. We anticipate that our Penguin purchasers/customers operating within the NHS will primarily rely on Article 6(1)(e) performance of a task carried out in the public interest as their lawful grounds for processing in providing direct care. The Penguin application is a tool utilised by the customer in providing direct care to patients. Cievert (as the company offering the Penguin application) is acting as a processor on behalf of its customer, in a similar way to other cloud and software as a service providers. As such the lawful grounds for processing the personal data which is identified and relied on by the controller is the ground on which the contracted processor relies.

A further possible ground is performance or preparation to perform a contract with the data subject (Article 6(1)(a) GDPR. But this will likely only apply in the context of private health care clinics. Typically, the key lawful ground for all private clinic direct care personal data collection and processing will be the performance or preparation to perform a contract (for private healthcare services) with the data subject (patient) (Article 6(a) GDPR).

In addition to a lawful ground for processing under Article 6, where special category data is being processed a special condition must also be identified. This special condition does not have to accord with or be linked to the Article 6 lawful ground, although it may be. Again,

consent is one possibility (for Article 9 it is termed "explicit" consent). However, the difficulty of how patients can be considered to "freely give" consent in the context of the imbalance of power between the parties applies again. Equally the difficulties of making the consent as easy to withdraw as to give in the direct care context put consent beyond the reach of many care givers as a special condition for health data processing.

From the IGA guidelines on lawful grounds, we can see that provision of direct care and the use of tools (including the Penguin application) as part of that direct care will be on the basis of the following special condition: Article 9(2)(h) processing necessary for:

> *"…'medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…' These conditions will also be the most appropriate basis for local administrative purposes such as: • waiting list management • performance against national targets • activity monitoring •local clinical audit • production of datasets to submit for commissioning purposes and national collections. These conditions will also apply where an organisation participates in activities with a statutory basis, such as responding to a public health emergency."*

Again, as a processor of personal data on your behalf as a controller, Cievert relies upon your special condition for processing. As set out above, this will in most cases be under Article 9(2)(h) GDPR and Part 1 Schedule 1 DPA 2018 provision and management of health care, including where carried out under a contract with a private healthcare provider.

2.5 Conclusion

The foregoing has been drafted taking into account guidance on lawful processing published by the Information Governance Alliance, which is available here: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

Please read that guidance if you require more information on the IGA's recommended approach to lawful grounds for the NHS.

There are obviously many aspects to complying with the data protection legislation, the above statement is to clarify for users and purchasers that the key elements of lawful grounds, special conditions and cybersecurity measures are in place to ensure compatibility between the Penguin application and the GDPR, when Penguin is used in accordance with our instructions. We invite you also to review our patient privacy policy regarding the Penguin application for more information on our responsibilities and how we process patient data entered onto the Penguin application. As a processor of patient data, we have taken the decision that the best way for us to ensure fair and transparent processing for the patients making use of the Penguin application is for us to include a full privacy notice on that application, setting out all those elements which would be required of a privacy notice provided by a data controller.

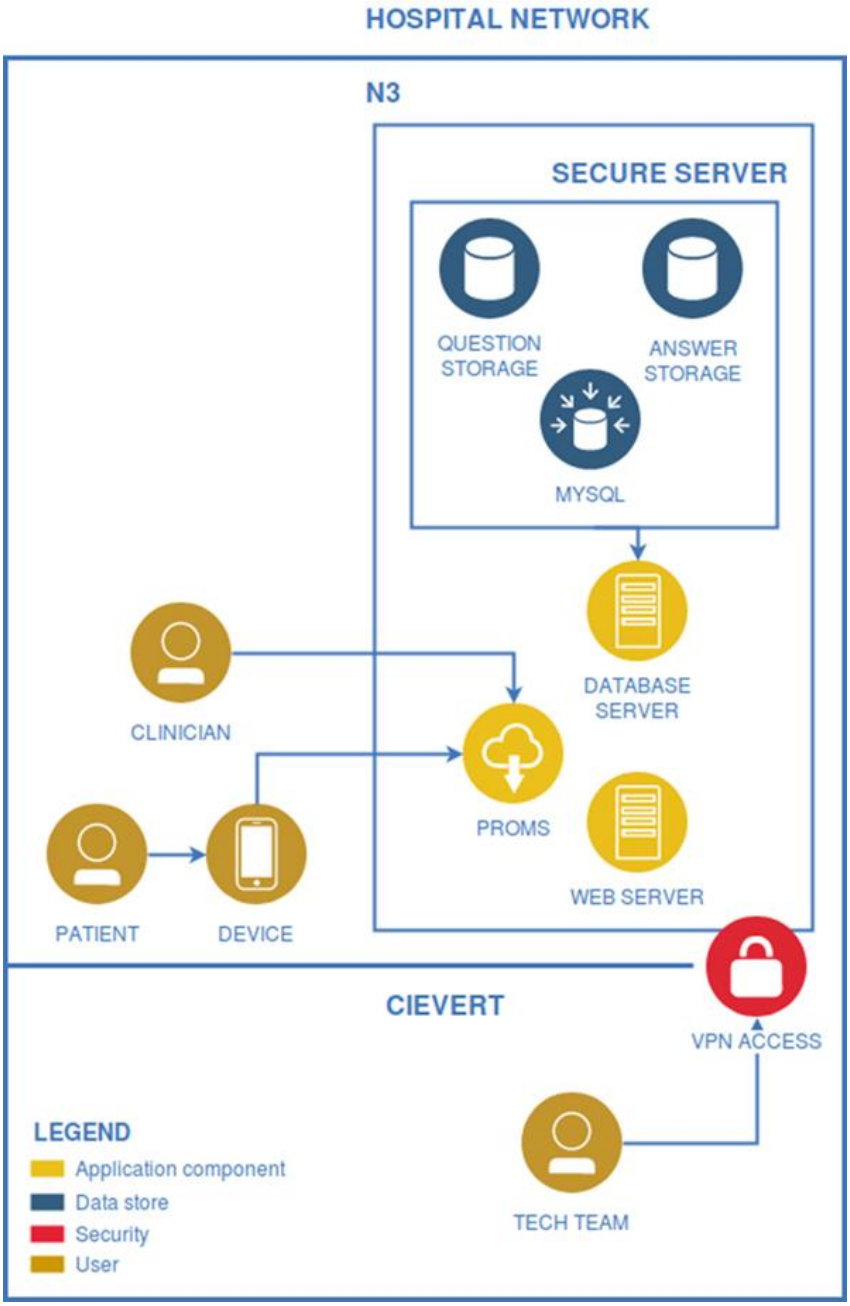
Clinics and Trusts will still provide patients with their own appropriate notices and information on how the clinic operates, what personal data it collects and generates and what

to expect from the data tools in use by the clinic and Trust and carry out their own GDPR compliance programmes. Please consult with your Information Governance Lead if you have any questions about GDPR, patient data, or use of Penguin.

Please also feel free to contact Cievert's Information Governance Lead or Data Protection Officer at info@cievert.co.uk if you have questions or concerns regarding this statement or the Penguin application processing of patient personal data.

3. Network Diagrams

3.1 Local Access N3 Model



4. Remote Access Model (future iteration and subject to IG Lead approval)

Questions are stored behind N3. Answers are stored externally, randomised but recoverable using lookup tables on N3. The application can then pull the answers into its network from within N3, only then making the link between patient and answer set.