EIDO Healthcare

GCloud-15 Service Definition Document

1. Introduction

This is a service definition document for our G-Cloud Inform Digital Consent Suite service. Below you will find information about how to use this document and what the document contains. It is important you read this introduction section to get the best experience from this document and ensure you find the information you need quickly and easily.

1.1 Document Sections

This document has the following sections:

Section 1 - Service Information contains essential information about our service, its functionality, security, and brief aspects of pricing.

Section 2 - G-Cloud Alignment Information details how our service and company aligns with the

G-Cloud buying process and provides typical information to help you understand how to buy, configure and consume our services, and how to leave our services should the need arise.

Section 3 - About Our Company and Our Services provides information specific to our company and how we can solve the problems faced by customers in the public sector.

Section 4 - Appendices provide supplementary service information that explain the functionality and benefits in greater detail.

1.2 How to Use This Document

This service definition document is an active document which means you can click on the links we provide to move around the document viewing only those specific sections you are interested in during the different phases of your G-Cloud buying process. There are also links to enable you to return to this section to speed up the reviewing process.

2. Service Information

2.1 Section Introduction

EIDO provide surgeons and other healthcare professionals with the tools required to support patients in making an informed decision.

In this section we describe our Inform Digital Consent Suite service, and you will find information about our service functionality. We describe the functionality in a way that should be understood by people familiar with this kind of service.

2.2 Inform Digital Consent Suite Overview and Assurance

EIDO's Inform Digital Consent Suite (DCS) empowers organisations to **educate** staff, **inform** patients and obtain **consent** to treatment. It combines EIDO's medico-legal eLearning course (Educate module), library of patient information (Inform module), and multi-language procedure-specific guided consent forms (Consent module) to support shared decision making and to obtain medical procedure consent. Inform is widely endorsed and certified by Royal Colleges and Associations, patient support groups and the Plain English Campaign. EIDO's DCS is modular, easy to implement and install, and supports many workflows, from supplying patient information to creating digital consent forms.

These can be signed at home or in hospital using our cloud-based App. All data is stored by AWS, who have many data security accreditations including ISO27001, ISO27018, NIST & SOC2.

- **Patients** need time to consider the implications of having a medical procedure. They may need to share information with family or friends to help them decide whether to consent to a procedure.

- **Clinicians** need to find more efficient ways to obtain consent from patients, making them instantly available to both patients and staff while not compromising the clinical integrity of the shared decision-making process.
- **Organisations** need reassurance that patients' informed consent is legally robust. If patients need to be treated at multiple sites, there is a risk of paper records being lost or not being available in a timely manner.

EIDO's DCS is a digital platform designed to address these issues and provides a digital informed consent solution for healthcare organisations. EIDO has 20 years of expertise in providing informed consent solutions through Trust, regional and nation-wide contracts.

2.2.1 Legal Benefits

Montgomery v Lanarkshire (2015) highlighted how vital the provision of procedure-specific information was to patients, alongside specific advice from clinicians, allowing patients to make informed decisions. EIDO's digital consent solution supports this legal obligation by ensuring that consistent, nationally recognised information is provided to all patients, documenting any patient-specific questions and clinician notes, providing a clear audit trail to ensure this standard is upheld for every patient. Freedom of Information data shows that Trusts who use EIDO's solution pay out over 25% less in consent litigation fees.

2.2.2 Patient Benefits

GMC consent guidance highlights the need to give patients sufficient time to consider information that they have been provided. In a pilot of the EIDO system at a large NHS University Hospital, patients spent, on average, 19 minutes reading through the procedure specific information. They were able to read this at home and share the decision-making process, improving the patient journey towards a more informed decision.

2.2.3 Clinician/Organisation Benefits

Organisations and clinicians know the importance of the digitisation of the consent process. Lost consent forms, lacking procedure-specific information to support patient-clinician conversations, too much paper use, and poor audit trails of patient engagement are some of the many challenges that our solution addresses.

Benefits to using EIDO's DCS include a reduction in theatre visit delays, facilitation of Day-of-Surgery admissions, increased ease of cross-site staff movement, and visibility of patient consent information from any Trust device, even if taken from

another clinician. This enables instant visibility for patients of their own copy from home, furthering the Trust's own IT and clinical strategies to create a more robust and reliable single Digital Consent Solution.

2.2.4 Service Functional Capabilities

The Inform Digital Consent Suite (DCS) is a modular system, split into three categories: Clinician Education, Patient Education and Patient Consent.

The Patient Education modules deliver procedure-specific information directly to patients. There are three modules:

Patient Education

PDF Module

Email PDF patient education documents directly to the patient.

Download PDF documents to print and hand out to support patients that are not yet digitally enabled.

Article Module

Email or SMS a digital patient education article to the patient.

The digital articles include digital content and the ability to link out to additional content. Patient experience is improved through the use of animation and video footage, easier access on mobile devices and support for accessibility requirements.

Dynamic Module

A patient-specific digital education article.

Engagement with the article is measured to evidence whether the patient has read the article and how long they spend. This timing data can be added to the consent form, to build a body of evidence to support consent. The Patient Consent modules creates procedure and patient specific digital consent forms:

Patient Consent

Remote patient

Send your patient a draft consent form to complete at home.

This can be printed out and completed in pen and ink by the clinician or viewed digitally in hospital as part of a fully paperless consent process.

Hospital patient

Take consent digitally for medical procedures in hospital.

This module works from the web browser on any device – tablet, laptop, desktop. All consent forms are catered for – Consent Form 1-4 and any bespoke forms the hospital requires. The consent forms are completely customisable.

Clinician Education

eLearning for clinicians

EIDO's Educate Consent eLearning Course (Educate) is an online training course developed and maintained by leading law experts, which further enhances EIDO's role as the partner of choice for consent risk management.

The course uses problem-based learning scenarios and self-test questions to steer learners towards a full appreciation of informed consent. Participants will be guided to identify important issues in difficult situations and how they should be resolved. It is in use in hundreds of hospitals in the UK.

Using final assessment tests, participants are able to confirm their knowledge and understanding of the medico-legal issues. The course can be self-administered by end users, or your hospital can take a more active role in monitoring usage and issuing a 'certificate of completion'.

It has been accredited for CPD points by

- Association of Surgeons of Great Britain and Ireland (ASGBI)
- The CPD Certification Service

You can claim one CPD point for each module studied, up to a maximum of eight.

Core modules

EIDO Educate covers the foundations of patient informed consent in four key modules:

- Consent and the law
- Consent in practice
- Capacity and consent
- Adult end-of-life issues

Specialist modules

Specialist modules help you and your team understand the medico-legal issues of clinical consent where the law can be more complex including:

- Obstetrics
- Paediatrics
- Accident and emergency
- Research and innovative treatment

Service Delivery Options

EIDO Educate can be delivered as a fully cloud-hosted and managed service. In this case, Trusts will pay an annual license fee covering implementation, support, updates and a defined number of learner 'seats' depending on the size of the organisation. Additional learner seats required are chargeable.

EIDO Educate can also be delivered as SCORM compatible files to be imported into Trust Learning Management Systems. In this case Trusts will pay an annual license fee covering the production of the SCORM file set, customised to Trusts system requirements, course content updates and license for unlimited learning 'seats'.

2.2.5 Clinician/Organisation Benefits

API integration is a key component of the service to ensure interoperability with other hospital systems. This allows the service to add patient data automatically from a 3rd party EPR or PAS system and trigger the sending of patient education articles without the need for additional staff input and to safely store patient consent records on the hospital system alongside the patient's other records. Data can be sent via HL7, FHIR or Restful JSON.

Other integrations can allow:

- Audit logs to the stored by the Trust
- SMS or EMAIL messaging to patients via existing platforms or patient portals
- Patient readiness to proceed data sent to POA system

2.2.6 Information Assurance

The system is hosted in a secure, modern Amazon AWS cloud infrastructure, within the London Region. The system is dynamically scaled, highly available and distributed across availability zones.

AWS data centres are ISO 27001 accredited, and all data is encrypted both in transit and at rest. EIDO is NHS Digital accredited and GDPR compliant.

EIDO infrastructure is separated into testing and production environments. All patient data is securely contained within the production environment.

EIDO have no access to patient data contained within the live production environment. Only admin and standard users created by the organisation have access to their individual dashboard to administrate patients.

A duplicate sandbox environment is available to EIDO, with dummy data, for testing purposes.

The review patient activity screen has a reading time summary graph, to help the clinician ascertain if the time spent reading the information article was sufficient.

Any specific pages of the article not read are highlighted, to allow the clinician to discuss these aspects of the procedure with the patient.

This offers much more insight into the patient's engagement with the information provided and will lead to a better, more informed discussion between patient and clinician.

If the clinician believes the patient has a thorough understanding, then a quicker workflow can be used, to provide greater time savings for the clinician and organisation.

The system has been penetration tested by Predatech, a third-party Crest and PCI approved supplier. Qualys TLS implementation checks have been performed. EIDO are Cyber Essentials Plus compliant and meet the standards of DSP Toolkit (ODS Number: 8JM91)

2.3 Security

The EIDO Consent Suite is a SAAS cloud-based software application hosted with Amazon (AWS). A modern approach has been taken to development such as Infrastructure as Code (IaC),

Continuous Integration / Continuous Deployment (CI/CD) and Kubernetes to run the applications scalable and highly available. It is important to understand how these systems are put together to understand the security considerations.

When prioritising security, it's crucial to also address data protection and high availability, rather than solely focusing on usability. Striking a balance between

robust security and user-friendly experiences is essential. No compromises have been made; both security and usability remain paramount.

Key features of the System architecture:

- Firewall and Ingress: This uses AWS security groups as well as AWS Application Load Balancers for access to the API.
- Aurora: This is a multi-region, highly available database cluster that is serverless and has a MySQL compliant interface.
- Redis: Handles caching and job queues.
- SSO/SAML: Single sign-on is implemented on a per customer requirement basis. 5 Gitlab code repositories and pipelines used for CI/CD.
- MicroServices includes utility applications such as a PDF generator and an XML procedure interpreter.

2.3.1 Secure Encrypted Connection from the Client to the Application

There are only two points of external access to the system. There is access for the applications to the API through the Firewall and there is access for GitLab to deploy new applications. Developers have no direct access to the internal running systems.

2.3.2 Firewall and Ingress

Only HTTPS (TCP Port 443) is allowed through the firewall. This is then accepted by the Application Load Balancer (ALB). The ALB does SSL offload and forwards the incoming request to the correct Kubernetes service based on the incoming host header. The Kubernetes services in turn are only accessible through another NAT gateway that allows entry to the private subnet where the Kubernetes nodes are run. There is no public access available to them.

2.3.3 GitLab Deployment

GitLab builds code into releases which get deployed to AWS EKS. To be able to access the cluster GitLab uses the AWS CLI tool and sets up access for kubectl using a secret key which is stored securely within GitLab. All communication using kubectl and aws-cli is encrypted using TLS.

Developers never update infrastructure directly and never deploy new code directly. This always happens through the automated system.

New software builds go through 4 stages:

- Build: This builds the Docker image with all needed dependencies.
- Test: This tests the built image making sure that there is no software regressions and that no bugs or security issues have crept in.
- Release: This creates a new release of the image, tagging it with a unique number. This makes it easy to revert to any release at any time.
- Deploy: The system deploys the new release to Kubernetes, and it goes live in a rolling update fashion.

2.3.4 Application Authentication

It is necessary for application users to authenticate to the API to ensure that they are only allowed to access features and data that they are supposed to.

Authentication is based on username and password credentials which generates a JWT token from the API and is then used in subsequent requests to identify the user. All of this is encrypted using TLS.

The API implements a role-based system that checks allowed access on each method.

2.3.5 Secrets Managements

Secrets that are used by the API (e.g. database access details), are automatically created using AWS KMS and stored as a Kubernetes secret. This gets read into the system environment as a variable when a Kubernetes pod starts up. These secrets are never on any developer machine and only available in the environment where the API is running.

2.3.6 Aurora Database

The system uses AWS Aurora as a data store. This is a serverless and managed service provided by AWS. Security updates and complicated configurations are handled by AWS. Database user and password credentials are created on creation and stored as a

Kubernetes secret. These details are not contained in any application code nor is it available on any developer machine.

The Aurora cluster has Encryption at Rest enabled and uses the industry standard AES-256 encryption algorithm. This means that all data on the underlying storage is encrypted, and this includes all backups, read replicas and snapshots.

2.3.7 Regions, Availability Zones and Security

The system uses the AWS eu-west-2 region which is in London. The region has 3 availability zones and Kubernetes nodes are distributed across them. If two zones fail, the system will keep on running.

2.4 Backup/Restore and Disaster Recovery Provision

The database used for the system is serverless and provides continuous backup, which allows for point-in-time backup to any point in the previous 7 days. Redundant standby databases are stored in each of 3 availability zones in the UK region, each with a backup. Therefore, there are 6 copies of data available immediately. In addition, full snapshot backups are taken every night and stored separately. On failure, the database will automatically failover to a replica, which is stored in the same geographical region. The failover is typically complete within 30 seconds. More information can be found here: https://aws.amazon.com/rds/aurora/mysql-features/#High_Availability_and_Durability

In the event of catastrophic failure, the entire system can be restored easily, as the infrastructure is stored as code and data can be restored via continuous backups. All application code is stored in Gitlab repositories and is highly available.

The system is cloud hosted and requires a network connection to work. If the trust network is not available, this solution will not work. For dashboard and step by step processes, the data is stored periodically to the database. The user will lose whatever actions they performed since connection was lost. Data is stored locally in the browser for as long as possible but may be lost if the user closes the browser down.

No data is stored on the servers. In the unlikely event a server fails, another will be created automatically and brought into the load balancer rotation.

The system is a web application rather than a desktop application. Data is sent to the database through the private API on each call it makes. Therefore, should the application fail, the minimum number of actions taken by the user will be lost.

Should the PC or tablet being used fail - power failure or suchlike, the user will lose any data since the last API call. This depends what action they are completing with the application.

Data is sent to the database through the private API on each call it makes. Therefore, should the application fail, the minimum number of actions taken by the user will be lost.

2.5 Technical Requirements

The content within the Inform library is reviewed and certified by the Plain English Campaign to ensure patients can easily read and understand the procedure-specific information. The patient interface

is designed to work on any web-enabled device and browser and is rated AA against the WCAG 2.1 standards. Information in printable large print, giant print and screen-reader enabled formats are available to support patients unable to use the digital platform.

2.6 Browsers

The patient and clinical dashboards are warranted to work on the latest 2 stable releases of:

- Microsoft Edge
- Firefox
- Chrome
- Safari

Legacy browsers are supported on a 'best efforts' basis.

2.7 Service Pricing

In this section you will find a list of the types of charges that you may incur in consuming our service. This will identify any setting up costs, operating costs, service closure costs and any optional charges from services that may accompany our services such as consultancy and training.

- Implementation – project management, documentation packs and project meetings
- Integration – standard integration using EIDO's API, or enhanced integration with hospital or 3rd party systems.
- Hardware/infrastructure requirements – if VPN, onsite or private cloud installation is required.
- Software – core system license, procedure-specific content, accessible and foreign language modules.

- Training – train-the-trainer to support Trust helpdesk staff, implementation clinDCS and new- feature webinars.
- Support and Maintenance – ticketing system via web and email, enhanced support via telephone.

2.7.1 Service Provision Pricing

- There are three elements in the service provision pricing:
    - System licensing (implementation, integration, core software license, training and support)
    - Content licensing
    - Per patient episode (consent license, support, messaging)
- To allow maximum flexibility for Trusts to access the service on a procedure, departmental or hospital-wide basis the three elements can be tailored to match usage requirements. Existing customers may already license these elements in part or in full.
- In most cases the System licensing fee is from £4,500 to £50,000 ex VAT per year, depending on the scope of installation. This includes standard implementation and integration using the EIDO API, software licensing and core system support.
- The content licensing fee is based on the per-procedure requirements of the Trust.
- The per patient episode fee is from £1 ex VAT per patient and can be pre-paid in blocks to match anticipated usage.
- The three elements combine to give the overall pricing for a Trust, though not all Trusts will need all elements.

2.7.2 On-Boarding Charges

For most Trusts the quoted system fee, content fee and patient episode fee is an 'all-in' cost. Standard implementation, integration via API, SSO integration, support and training (of the Trust's implementation team) and project management are included in the system license fee.

Customisation of consent form templates, hospital branding of email communications, webpages and PDF documents is included in the per patient episode fee.

Additional on-boarding costs could be chargeable for enhanced end-user training, deep integration with Trust or third-party platforms. Additional

authentication needs such as VPN, Certificate Authority and SSO could incur additional cost depending on the local Trust's requirements.

2.7.3 Off-Boarding Charges

There are no specific off-boarding charges. Trust data is sent to hospital systems as part of 'business as usual' usage for long term data warehousing. Manual data extraction of audit logs and patient SARs can be done by Trust administrators at point of need (CSV and PDF format).

Any unpurged data can be provided to the Trust using Industry standard database formats. This work would be charged at our technical day rate of £750 ex VAT

2.7.4 Termination Charges

In the case of early termination, the System license fee, Content fee and patient episode fees for the current license period will be due as they will include pre-planned system service licensing, customisation and support.

Any bespoke integration or implementation costs that have been quoted will be due.

2.7.5 Training Charges

EIDO uses a train the trainer approach. For most Trusts the quoted annual fee and patient episode fee is an 'all-in' fee. This includes training for Trust admin staff and key stakeholders during the implementation phase, and at the regular group training events agreed with the Trust.

Additional one to one training can be delivered at our day rate of £500 ex VAT.

2.7.6 Other Charges

The system interface can be provided in multiple languages. This is outside the scope of a standard license. The additional cost varies by language, so will be quoted on a case-by-case basis.

As a SaaS product, the primary delivery route is via EIDO's hosted Cloud, or on a Trust's private cloud. On premises installation with bespoke requirements is out of scope of the standard fees so will be quoted on a case-by-case basis.

3. G-Cloud Alignment Information

3.1 On-Boarding and Off-Boarding Processes

3.1.1 On-Boarding

After an initial consultation, we will collaborate with the Trust to devise comprehensive project plans. These plans will include steering group meeting agendas, communication templates, and support materials.

The Project Team that the Trust will be assigned by EIDO will include a Project Sponsor, Project Manager, Key Account Manager, Data Protection Officer, Clinical Safety Officer, Digital Project Director and Chief Marketing Officer.

The Trust helpdesk staff will receive support through instructional videos and resource materials, along with on-site training. For end-user staff, we will provide access to a video-supported knowledge base, online demos, and group training. Additionally, a dedicated account manager will deliver targeted training sessions to facilitate the service launch.

3.1.2 Off-Boarding

At end of contract the Key Account Manager will provide communication templates for circulation to Trust staff to explain the end of license requirements.

Access to the service will be revoked on a date mutually agreed with the Trust. Prior to this, the Key Account Manager with work with the Trust to ensure data extraction to Trust systems is complete. After this date, all personally identifiable data held by EIDO as a data processor of the Trust will be purged.

3.2 Service Level Details

3.2.1 General Support details

Standard Support is provided Monday to Friday, 9am to 5pm, and this is allocated in the core fee. Tickets can be submitted by email or website.

- Email – support@eidohealthcare.com
- Online support portal - support.eidohealthcare.com

An Enhanced Support option is available which provides 24/7 cover. Tickets can be submitted by email, website or phone.

For all levels of support, a knowledgebase is available for training and solutions to common issues. This is available on the system, and on a directed support link from the system.

The Support Policy is detailed in Appendix 1 which explains our service levels in further detail.

3.2.2 Award and Payment of Service Credits

EIDO does not offer service credits as standard practice. For customers that request/require them, we negotiate service credits on a per customer basis.

Customers can apply for service credits in line with the contractual agreement by submitting a credit request to the relevant EIDO representative for checking and processing.

The scope and limit of the credit request will be defined in the service level agreement during the original contract negotiation.

3.2.3 Financial Recompense

EIDO does not usually offer financial compensation for failing to meet its service targets. Customers have access to senior management if they wish to escalate any dissatisfaction with our service levels.

3.2.4 Technical Boundary

Services that are out of our scope:

- Management of third-party integrations and IT solutions.
- Management of NHS IT solutions.
- EIDO incorporating third party information in the article library. This can be managed as a self-serve procedure.
- Version control, archiving and back up of third-party information that has been added to the article library.
- Long term storage of identifiable data on the EIDO platform. Standard is 180 days.

Enhanced support with telephone, email and web access on a 24/7 basis is available as an additional service.

3.3 Service Constraints

The system is designed to be available 24/7. System updates are deployed to a test environment before being made live. This does not usually require downtime.

3.3.1 Support Boundary

Patient support – EIDO do not have direct contact with patients.

End user support – EIDO will provide technical support and helpdesk services to designated users through an agreed triage process.

3.3.2 Planned Maintenance

New versions of the system are scheduled and pushed live once testing has been completed. The update occurs outside of usual business hours.

Urgent updates may be pushed live sooner than the scheduled pushes, but also outside of business hours.

We provide a system status web page, which provides updates on changes in system status. Relevant users can subscribe to notification from this service to be proactively informed of outages, whether planned or not, and resolutions.

3.3.3 Emergency Maintenance

In the rare event of a bug or issue with the software preventing customers from using the system, a fix will be pushed to the production server as soon as it is available and has been tested. This may occur during business hours.

Any such incident will be communicated to customers in advance, with regular incident updates.

3.4 Training

The Key Account Manager will coordinate with the Trust to devise comprehensive project plans which will include steering group meeting agendas, communication templates, and support materials.

The Trust helpdesk staff will receive support through instructional videos and resource materials, along with on-site training. For end-user staff, we will provide access to a video-supported knowledge base, online demos, and group training. Additionally, a dedicated account manager will deliver targeted training sessions to facilitate the service launch.

A regular update webinar will be provided to reinforce best practice and showcase any system updates.

3.5 Invoicing Process

On receipt of an official purchase order EIDO will issue an invoice by email. Standard payment terms are 28 days.

3.6 Termination Terms

The customer acknowledges that it has purchased the Services for the Minimum Period and any Renewal Term(s), as defined in the Certificate or Order Summary.

We expect a 60-day notice period if there is termination at the end of licence period. If a licence is paid upfront, then there is no refund for that period if terminated early.

3.7 Data Extraction/Removal Criteria

The EIDO Consent Suite built in functionality for specific data extraction, for instance responding to a Data Subject Request.

Extraction of data for the purposes of analysis or migration to an alternative solution will be facilitated by EIDO on a case-by-case basis, using industry standard data formats.

3.7.1 Data Standards in Use

The EIDO Consent Suite supports HL7 and FHIR for transferring of information to and from other systems.

Any data stored is done so in a SQL database.

3.7.2 Consumer Generated Data

If the consumer is the patient, all information related to patient interaction is provided as PDF reports. This data can be provided in an electronic format if required, but this will incur an additional cost at technical day rate of £750 ex VAT.

3.7.3 Data Extraction

Data can be extracted in CSV or PDF format by Admin users on a self-service basis. Data can also be extracted in industry standard database formats by EIDO.

3.7.4 Purge & Destroy

Customers are able to define a purge period, all data that is older than that period will be purged. Purged records have all identifiable fields overwritten, non-identifiable fields are retained for statistical reporting.

3.8 Data Processing and Storage Locations

Data is stored in AWS in the London region and not transferred outside of the territory of operation.

3.9 Data Restoration/Storage Migration

Patient reports are sent to the customer EPR system and should be accessible from there if the EIDO Consent Suite dashboard is non-functional.

EIDO provides customers with access to the EIDO Download Centre which makes available PDF versions of the patient education content available for download in order to consent patients manually.

3.10 Customer Responsibilities

As the customer will be the data controller and EIDO will process data on their behalf, the customer is responsible for ensuring patient data is being acquired and used according to data privacy regulations.

The EIDO Consent Suite does not store the engagement reports and consent forms of patients beyond the purge period. It is the responsibility of the customer to ensure these electronic documents are stored and archived appropriately.

3.11 Details of any Trial Service Available

A free trial of the service is available which includes license for the core system with the full EIDO Inform library, custom procedure module, core UK consent form templates, integration using EIDO's industry standard API (FHIR, JSON), SSO option and support helpdesk account for Trust's pilot team. Recommended trial period is 3-6 months depending on size and scope of Trust pilot.

4. About Our Company and Our Services

4.1 About Us

EIDO Healthcare provides a complete and comprehensive range of content, processes, systems and solutions to successfully manage and deliver informed consent. For over 20 years, EIDO Healthcare has been providing resources and support to help health professionals reduce the risk of litigation, specifically in the area of informed consent to surgery and medical treatment.

Developed by clinicians for clinicians, we deliver content and cloud-based solutions designed to support health professionals in achieving excellence in obtaining and recording informed consent from patients.

EIDO consent solutions can be bought directly by your hospital or seamlessly integrated into third- party healthcare technology systems.

4.2 Why Choose Us?

Our 20 years of knowledge and experience in medico-legal informed consent means that we can help mitigate and reduce the risk of litigation and legal claims, lower operational costs and increase patient satisfaction. In use in over 1000 hospitals worldwide, EIDO's Inform Consent Library has supported millions of patient consent decisions.

We follow a rigorous 10-step document production process to ensure that EIDO's information is produced to a gold standard. This is detailed in full in Appendix 2. Clinicians can feel safe in the knowledge the information they are giving patients is evidence based, accessible and up to date.

By continuously updating our content, and never outsourcing to other sites, we can confidently say that our information is safe to use.

In that time, we have not had a single indemnity claim made against us. In fact, our documents have been requested for use as evidence in 100s of cases.

With over 65% of acute NHS Hospitals and 85% of private hospitals as customers, EIDO Healthcare has become the UK standard in quality, evidence-based patient information.

Some of our customers include:

4.3 Why Choose Our Services?

Today, the EIDO suite of risk-management consent tools are used in over 1000 hospitals in the UK and internationally. Over 8 million patients each year benefit from our informed consent resources. This is only set to increase with the EIDO Inform Digital Consent Suite; a range of digital consent products that can help even more patients as well as reducing the risk of litigation. EIDO Healthcare is committed to helping our customers achieve excellence in the vital areas of informed consent and clinical governance.

ONLY EIDO Informed Consent

- Is endorsed by the Royal College of Surgeons of England, Royal College of Surgeons Edinburgh and NHS England Information Standard
- Is reviewed and approved by the Patient Information Forum
- Supports over 8 million surgical consent decisions annually
- Serves 65% of NHS hospitals and 85% of acute private hospitals in the UK
- Delivers 400+ treatment-specific patient consent information, peer-reviewed by over 100 speciality contributors
- Is in use over 1000 hospitals in the UK and internationally

5. Appendices

5.1 Appendix 1: Support Policy

1. Interpretation

The following definitions and rules of interpretation apply in this schedule.

1.1 Definitions:

Authorised Person a person authorised by the Customer to make a Support Request being only those persons listed in Schedule 1 of SaaS Agreement Contract. (Documentation to be agreed upon at start of implementation)

Customer Cause any of the following causes:

a. any cause arising from or connected with any breach by the Customer of its obligations under clause 6 of EIDO's Saas Agreement Contract of this agreement;

b. any improper use, misuse or unauthorised alteration of the Software by the Customer; any use of the Software by the Customer in a manner inconsistent with the then-current

Documents; or any failure by the Customer to maintain the correct operating environment for the Software as specified in the Functional Specification.

Fault failure of the Software to operate in accordance with the Functional Specification.

Out-of-scope Services any services provided by the Supplier in connection with any apparent problem regarding the Software reasonably determined by the Supplier not to have been caused by a Fault, but rather by a Customer Cause or a cause outside the Supplier's control (including any investigational work resulting in such a determination).

Solution either of the following outcomes:

a. correction of a Fault or;

a workaround in relation to a Fault.

Support Request a request made by an Authorised Person in accordance with this Schedule for support in relation to the Software, including correction of a Fault.

Support Services maintenance of the then-current version or release of the Software but excluding any Out-of-scope Services.

2. Support Services

2.1 The Supplier shall perform the Support Services during Normal Business Hours.

2.2 The Support Services shall comprise:

2.2.1 the provision of the services specified in paragraph 2.12 in respect of all Faults notified under paragraph 2.6; and

2.2.2 provision by the Supplier of technical support for the Software.

2.3 The Customer acknowledges that the Supplier is not obliged to provide Out-of-scope Services.

2.4 The provision of Out-of-scope Services shall be charged for at the Supplier's standard applicable time rates from time to time in force which at the date of this agreement is £100 per hour plus VAT plus any related expenses, which in the case of travelling by car shall be charged at HM Revenue & Customs mileage rate then in force and otherwise at the cost to the Supplier.

2.5 A Support Request may only be made by an Authorised Person.

2.6 An Authorised Person may request Support Services by way of a Support Request using any of:

2.6.1 Email – support@eidohealthcare.com

2.6.2 Online support portal - support.eidohealthcare.com

2.7 Each Support Request shall include a description of the Fault, and the Customer shall on request by the Supplier provide such other information as may be requested by the Supplier to allow it to assess the Fault and provide the Support Services.

2.8 Following submission of a Support Request the Authorised Person will receive by email an automatically generated Support Ticket Number. The Customer will be able to use such Support Ticket Number to monitor the status and history of a Support Request using the

Support Request tracking function on the online support portal at support.eidohealthcare.com

2.9 The Customer shall provide the Supplier with:

2.9.1 prompt notice of any Faults which it becomes aware of; and

2.9.2 such output and other data, documents, information, assistance and (subject to compliance with all Customer's security and encryption requirements notified to the Supplier in writing) remote access to the Customer System, as are reasonably necessary to assist the Supplier to reproduce operating conditions similar to those present when the Customer detected the relevant Fault and to respond to the relevant Support Request.

2.10 Unless otherwise agreed in writing by the parties, all Support Services shall be provided on an off-site remote basis

2.11 The Supplier shall within two Normal Business Hours of receipt of a Support Request and based on its reasonable assessment of the severity level of the Fault reported notify the Authorised Person of its categorisation of the Fault as either a:

2.11.1 Severe Fault - a failure of the Software to operate in accordance with the Functional

Specification that has a significant impact on the Customer's ability to use the Software for its intended purpose;

2.11.2 Moderate Fault - a failure of the Software to operate in accordance with the Functional Specification that has a moderate impact on the Customer's ability to use the Software for its intended purpose;

2.11.3 Minor Fault - a failure of the Software to operate in accordance with the Functional Specification that has a minor impact on the Customer's ability to use the Software for its intended purpose.

2.12 Following the categorisation of a Fault under paragraph 2.11 the Supplier shall:

2.12.1 in respect of a Severe Fault, use reasonable endeavours to achieve a Solution as soon as possible.

2.12.2 in respect of a Moderate Fault, use reasonable endeavours during Normal Business Hours to achieve a Solution as soon as possible.

2.12.3 in respect of a Minor Fault, use reasonable endeavours during Normal Business Hours to achieve a Solution within a reasonable period of time.

5.2 Appendix 2: The EIDO 10-step document production process