**eOPS User Agreement (EUA)**

This eOPS User Agreement ("EUA") is a legal agreement between you (either an individual or a single entity) and the NHS Business Services Authority ("NHSBSA").

The NHSBSA grants you the right to access the NHSBSA’s online system known as ‘eOPS’, which includes computer software, the data supplied with it, and any associated media, printed materials, electronic documentation and internet-based services ("eOPS system"), provided that you comply with all terms and conditions of this EUA.

The right of access cannot be transferred to anyone else.

**Definitions**

**“Confidential Information”** means any information containing personal data, financial information and any other information clearly designated as being confidential (whether or not it is marked as “confidential”) or which ought reasonably to be considered to be confidential.

“**Data Breach**”means a breach of security or security incident which leads to the accidental, wrongful or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data or information contained within or obtained via the eOPS system.

“**Personal Data**” means information relating to natural persons who can be identified or who are identifiable directly from the information or who can be indirectly identified from the information in combination with other information.

**User Obligations**

The eOPS system is provided to facilitate effective monitoring, management and optimisation of the use of ophthalmic services within the NHS and wider Government commissioned services.

The eOPS system may not be used for personal purposes or to profit or otherwise benefit individuals or non-NHS organisations and you agree not to use or access any information via the eOPS system unless necessary for the performance of your duties for the NHS and/or and wider Government commissioned services.

You are responsible for ensuring the accurate production of any reports produced through the eOPS system. The NHSBSA shall not be liable for any losses or damage incurred by inappropriate or inaccurate use of any data provided through the eOPS system or reliance upon any inaccurate reports produced by users.

You agree not to publish or to use or include in any material which will be made public, any information obtained via eOPS without the prior written consent of the NHSBSA. Where consent of the NHSBSA is obtained, you must reference the data/information in accordance with the referencing instructions provided by the NHSBSA.

Access to the eOPS system through any allocated user ID is restricted to one named registered user. You must not share access, passwords, usernames or log on details to the eOPS system with any other person. Passwords must not be written down.

Where you no longer require use of the system, your personal details/ contact details change or where your role or circumstances change such that you no longer satisfy the terms of this agreement you are required to advise NHSBSA to this effect so that the account can be withdrawn or amended as necessary.

You must not access the eOPS system using an email address/account which you no longer use, or which has become inactive. Where your email address changes/becomes inactive you must notify NHSBSA as soon as possible so that NHSBSA records can be updated.

You are not permitted to access the eOPS system from outside the UK and the NHSBSA reserves the right to restrict access from any non-UK IP addresses.

You agree that NHSBSA has the right to audit yours and/or your employer’s use of eOPS and you and/or your employer will provide information and reasonable cooperation to the NHSBSA upon request.

You agree that the NHSBSA has the right to withdraw access to eOPS where you have breached or no longer satisfy the terms of this EUA, where any other abuse of eOPS is understood to have occurred (including unreasonably excessive use) or there has been a Data Breach.

The NHSBSA has the right to suspend an organisation’s access to eOPS pending an NHSBSA investigation into a user’s breach of the EUA, other abuse of the eOPS system or a Data Breach. You agree that where the NHSBSA considers it appropriate to do so following an investigation, the NHSBSA has the right to terminate an organisation’s access to eOPS.

You are responsible for informing the NHSBSA if you have access to information you do not consider to be appropriate to your NHS /Wider Government role. Where you become aware that you have access to Personal Data which is not appropriate to your NHS/Wider Government role, you should report this to the NHSBSA via email at DataServicesSupport@nhsbsa.nhs.uk as soon as possible and in any event within 24 hours of becoming aware.

You are responsible for informing the NHSBSA promptly if you become aware of a Data Breach which does not concern any Personal Data. Such a Data Breach must be reported to NHSBSA via email at DataServicesSupport@nhsbsa.nhs.uk as soon as possible.

You are responsible for notifying the NHSBSA if you consider your organisation’s data and security standards, policies and procedures and technical and organisational measures are not equivalent to the standard of security required by NHS security policies and the NHSBSA reserves the right to audit your organisation’s measures, standards, policies and procedures. Please contact NHSBSA via email at DataServicesSupport@nhsbsa.nhs.uk

if you require information on the data and security standards which are required by NHSBSA to be in place.

**Freedom of Information Requests**

For the purposes of Freedom of Information (FOI) legislation eOPS system information is held by the NHSBSA. You agree not to use the eOPS system to download information to answer an FOI request. You need to refer the FOI requester to nhsbsa.foirequests@nhs.net.

The only exception to this is where you have downloaded eOPS information to your local systems before the FOI request was received. Where this is the case, you agree to consult with NHSBSA at DataServicesSupport@nhsbsa.nhs.uk before responding to the FOI request.

**Subject Access Requests**

You can request a copy of the information we hold about you. Information on how to make a subject access request can be found here <https://www.nhsbsa.nhs.uk/privacy>.

**Personal Data**

You agree that you will comply with all data and security standards, policies and procedures applicable to you as an employee or contractor of the NHS or wider Government commissioned service and that you will only use, hold and distribute data accessed via the eOPS system within the NHS/wider Government and solely as required for the purposes of your employment.

Where data you have obtained via the eOPS system is no longer required, it must be destroyed in a secure manner in accordance with any applicable legislation and/or NHS data retention policies and/or the instructions of the NHSBSA.

You agree that you and your employer have in place appropriate technical and organisational measures to prevent unauthorised or unlawful processing of Personal Data and to prevent against accidental loss or destruction of, or damage to Personal Data which are at least equivalent to the standard of security required by the NHS security policies; and you and your employer shall take reasonable steps to ensure the reliability of any employees who will have access to Personal Data.

You will be liable for any “breach of confidence”, breach of Data Protection legislation and/or Data Breach which involves any Personal Data and upon becoming aware of such an incident you are required to report this to the Information Commissioner’s Office (ICO) as soon as possible.

NHSBSA must also be advised of any Data Breach or suspected data breach concerning Personal Data without undue delay, and in any event within 24 hours of you becoming aware of such a breach or suspected breach, via email at DataServicesSupport@nhsbsa.nhs.uk.

Any small number, rate or percentage derived from NHSBSA data must be suppressed if there is a risk of identification. Figures that may identify individuals when subtracted from totals, subtotals or other published figures must also be suppressed.

**Confidentiality**

You acknowledge that in using the eOPS system you may have access to Confidential Information with respect to ophthalmic activity.

You agree that you shall hold any Confidential Information in confidence and, unless required by law, shall not:

* Make any Confidential Information available to any third party (other than to a party to whom you are satisfied that you may legally disclose such Confidential Information); or
* Use the Confidential Information for any purpose otherwise than in the proper performance of your duties as an NHS employee or contractor (as applicable); or
* Permit or cause any unauthorised disclosure of Confidential Information through any failure to exercise due care and diligence; or
* Release any data in public that could allow information about an individual that is not already public to become identifiable, or able to be deduced from any other data.

**Cookies**

You agree that cookies are enabled on the eOPS Access Management system. The purpose of the cookie is to aid the login process by ensuring your user details do not have to be re-entered.

The information relating to cookies can be found on NHBSA website <http://www.nhsbsa.nhs.uk/PrivacyPolicy.aspx>.

**Log in details**

All the information you provide when you register will be used to manage access to eOPS.

The email address you provide may also be used by NHSBSA for service-related communications and sending you newsletters relevant to our Information Systems.

If required we may use the email address provided to:

* contact you to complete surveys relating to NHSBSA services and systems and
* invite you to take part in research to help improve our services to you.

If you need to update, receive a copy of or delete your registration information then please contact DataServicesSupport@nhsbsa.nhs.uk.

Audits will be carried out incrementally by the NHSBSA on eOPS system user accounts to identify and remove inactive accounts and any accounts that have not been used by a user for a period of 6 months will be removed.

We will keep your information for 12 months after your account is closed.  This is to ensure that all transactions can be fully audited.

We do not disclose this information to third party organisations.