NOVA HEALTHCARE SERVICES

GDPR Policy

Nova Healthcare Services Ltd is required to take a proportionate and appropriate approach to UK GDPR compliance. Nova Healthcare Services Ltd understands that not all organizations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organization, as well as the processes already in place to protect personal data.

Nova Healthcare Services Ltd understands that if significant volumes of personal data are processed, including **special categories of personal data,** or it has unusual or complicated processes in place in terms of the way personal data is handled, Nova Healthcare Services Ltd will consider obtaining legal advice specific to the processing conducted and the steps that may need to be taken.

UK GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

- **Process for Promoting Compliance at Nova Healthcare Services Ltd**

  Nova Healthcare Services Ltd recognizes that, in addition to complying with the key principles, it must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. Nova Healthcare Services Ltd understands that a 'privacy by design' approach must be adopted. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an afterthought. These ideas are also covered in more detail in the Key Principles Guidance.

- **Processing Personal Data**

  The provision of health or social care or treatment or the management of health or social care systems and services is expressly referred to in UK GDPR as a lawful basis upon which an organization is entitled to process special categories of data.

  In terms of other types of personal data, Nova Healthcare Services Ltd must only process personal data if it is able to rely on one of several grounds set out in the UK GDPR. The grounds which are most commonly relied on are: Processing Personal Data.

- The data subject has given their consent to the organization using and processing their personal data.
- The organization is required to process the personal data to perform a contract with the data subject, and.
- The processing is carried out in the legitimate interests of the organization processing the data – note that this ground does not apply to public authorities.

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation.
- The processing is necessary to protect the vital interests of the data subject or another person.
- The processing is necessary to perform a task carried out in the public interest.

Data Protection Officers

Nova Healthcare Services Ltd understands that some organizations will need to appoint a formal Data Protection Officer under UK GDPR (a "**DPO**"). The DPO benefits from enhanced employment rights and must meet certain criteria, so it is recognized that it is important to know whether

Nova Healthcare Services Ltd requires a DPO. This requirement is outlined in the Appointing a Data Protection Officer Policy and Procedure. Nova Healthcare Services has appointed a singular person, Nikki Virk, as our formal Data Protection Officer to have overall responsibility for the management of personal data and compliance with UK GDPR.

Data Security and Retention

Two of the key principles of UK GDPR are data retention and data security.

- Data retention refers to the period for which Nova Healthcare Services Ltd keeps the personal data that has been provided by a data subject. At a high level, Nova Healthcare Services Ltd must only keep personal data for as long as it needs the personal data.

- Data security requires Nova Healthcare Services Ltd to put in place appropriate measures to keep data secure.

- **Subject Access Requests**

  One of the key rights of a data subject is to request access to and copies of, the personal data held about them by an organization. Where Nova Healthcare Services Ltd receives a subject access request, it understands that it will need to respond to the Subject Access Request following the requirements of UK GDPR. To help staff at Nova Healthcare Services Ltd understand what subject access requests are and how they should deal with a subject access request, a Subject Access Request Policy, and Procedure is available to staff.

- **The Rights of a Data Subject**

  In addition to the right to place a subject access request, data subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing, and the right to request that their personal data be corrected by Nova Healthcare Services Ltd. Not all rights apply in all circumstances. The rights of the data subject are covered in detail in the corresponding guidance.

- **Breach Notification Under UK GDPR**

  In certain circumstances, if there is a personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data), the ICO must be notified and potentially any affected data subjects. There are strict timescales in place for making such The processing is necessary to comply with a legal obligation The processing is necessary to protect the vital interests of the data subject or another person The processing is necessary to perform a task carried out the public interest Data retention refers to the period for which Nova Healthcare Services Ltd keeps the personal data that has been provided by a data subject. At a high level, Nova Healthcare Services Ltd must only keep personal data for as long as it needs the personal data Data security requires Nova Healthcare Services Ltd to put in place appropriate measures to keep data secure notifications. Nova Healthcare Services Ltd understands that this requirement is likely to have less impact on NHS organizations that are already used to reporting using the NHS reporting tool.

- **Data Privacy and Consent Form**

  Organizations are required to provide data subjects with certain information about how their personal data is being processed. The easiest way to provide that information is in a data privacy policy. A privacy policy template is available for Nova Healthcare Services Ltd to use and adapt on a case-by-case basis.

  The privacy policy sits alongside a consent form which can be used to ensure that Nova Healthcare Services Ltd obtains appropriate consent, particularly from the Service User, to the various ways in which Nova Healthcare Services Ltd uses the personal data (where Nova Healthcare Services Ltd needs to rely on consent as a basis for the processing). The Consent Form contains advice and additional steps to take if the Service User is a child or lacks capacity.

- **Transfer of Data**

  If Nova Healthcare Services Ltd wishes to transfer personal data to a third party, an agreement must be set out on how the third party will use the personal data. If the third party is processing data on the instruction of Nova Healthcare Services Ltd, the contract must cover specific points set out in UK GDPR. Nova Healthcare Services Ltd must consider carrying out due diligence investigations on third-party recipients of personal data of which Nova Healthcare Services Ltd is the controller.

  Transfers of personal data outside of the UK and EEA (and other countries with an adequacy decision in place for such data transfers) may only be made under specific circumstances. This includes where a data processor processes personal data in such jurisdiction. For such transfers, Nova Healthcare Services Ltd recognizes that further protection will need to be put in place and other aspects considered before the transfer takes place.

- **Data Protection Impact Assessments**

  Nova Healthcare Services Ltd carries out Data Protection Impact Assessments each time it processes personal data in a way that presents a “high risk” for the data subject. Examples of when a Data Protection Impact Assessment should be conducted are provided in the relevant policy and procedure. Given the volume of special categories of data that are frequently processed by organizations in the health and care sector, there are likely to be several scenarios that require a Data Protection Impact Assessment to be completed.

- **Compliance with UK GDPR**

  Nova Healthcare Services Ltd understands that there are two primary reasons to ensure that compliance with UK GDPR is achieved:

  It promotes high standards of practice and Care and provides significant benefits for staff and, in particular, Service Users.
  Nova Healthcare Services Ltd appreciates that it is important to remember, however, that the ICO intends to educate and advise, not to punish. The ICO wants organizations to achieve compliance and offers guidance to organizations about how to comply. A one-off, minor breach may not attract the attention of the ICO but Nova Healthcare Services Ltd persistently breaches UK GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special category personal data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Nova Healthcare Services Ltd and its data protection policies and processes and to issue instructions for Nova Healthcare Services Ltd to comply or outright data processing practices including requiring Nova Healthcare Services Ltd to stop providing services or to notify data subjects of the breach, delete certain personal data held or prohibit certain types of processing.

For any questions or concerns related to this policy, please contact admin@novahc.co.uk

Policy Approval Date: **01/01/2025**
Policy Review Date: **31/12/2025**

Nikki Virk.
Director and Founder.
Nova Healthcare Services Ltd.