

Private & Confidential

Viamed Ltd  
15 Station Road  
Cross Hills  
Keighley  
West Yorkshire  
BD20 7DT

22 May 2018

RECEIVED 29 MAY 2018

Dear Sir/Madam,

### New Contractual Commitments for the General Data Protection Regulation 2016

We are writing to you as a supplier to this Trust, about the General Data Protection Regulation 2016 (GDPR), which will take effect from 25 May 2018. This applies to any organisation directly or indirectly processing personal data. GDPR requires a higher level of data protection and security for the personal data of Barking, Havering and Redbridge Hospitals NHS Trust (the "Trust") employees, patients, service users and third parties ("Data Subjects").

The new law will require data controllers (the Trust) and data processors (your organisation) to demonstrate compliance with the principles of lawful data processing set out in the regulation. The Trust is working locally to implement the changes and requirements needed to ensure compliance. We are fully committed to GDPR compliance because of (i) our duty of care to our data subjects, and (ii) the value we place on personal data in health and social care which may be confidential or sensitive in nature. This means complying with the law and standardising best practice are high priorities across the Trust.

This letter provides some guidance to your organisation regarding relevant GDPR provisions applicable to the processing of personal data by data processors. We refer to any contract(s) that the Trust may hold with your organisation that may involve access to personal data of staff or patients of the Trust.

Whilst established key principles of data protection will remain relevant, there are a number of changes that will affect contractual arrangements, both new and existing, with suppliers and service providers that process data. GDPR specifies that any processing of personal data, by a data processor, should be





## APPENDIX A

### CHANGE CONTROL NOTE (GDPR COMPLIANCE SCHEDULE)

#### **PART A – DEFINITIONS AND INTERPRETATION**

In this Schedule, the following terms shall have the following meanings:

**Contractor:** means SUPPLIER, SERVICE PROVIDER OR DATA PROCESSOR

**Contractor Personnel:** means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this agreement;

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer:** have the meaning given in the GDPR;

**Customer:** means Barking, Havering and Redbridge University NHS Trust (BHRUT, the Trust);

**Data Loss Event:** any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this agreement, including any Personal Data Breach;

**Data Protection Impact Assessment:** an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

**Data Protection Legislation:** (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 (subject to Royal Assent) to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

**Data Subject Access Request:** a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

**DPA 2018:** Data Protection Act 2018;

**GDPR:** the General Data Protection Regulation (Regulation (EU) 2016/679);

**ICO:** means the Information Commissioner's Office;

**Law:** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Contractor is bound to comply;

**LED:** Law Enforcement Directive (Directive (EU) 2016/680);

**Party:** a Party to this agreement;

**Protective Measures:** appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of any such measures adopted by it.

**Services:** means the services provided by the Contractor to the Customer under this agreement.

**Sub-processor:** any third Party appointed to process Personal Data on behalf of the Contractor related to this agreement.



adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of this agreement unless the Contractor is required by Law to retain the Personal Data.

*Subject to paragraph 1.6, the Contractor shall notify the Customer immediately if it:*

(f) receives a Data Subject Access Request (or purported Data Subject Access Request);

(g) receives a request to rectify, block or erase any Personal Data;

(h) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(i) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(j) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(k) becomes aware of a Data Loss Event.

*The Contractor's obligation to notify under paragraph 1.5 shall include the provision of further information to the Customer in phases, as details become available.*

*Taking into account the nature of the processing, the Contractor shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:*

(l) the Customer with full details and copies of the complaint, communication or request;

(m) such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(n) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;

(o) assistance as requested by the Customer following any Data Loss Event;

(p) assistance as requested by the Customer with respect to any request from the ICO, or any consultation by the Customer with the ICO.

The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this Part B. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(q) the Customer determines that the processing is not occasional;

(r) the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(s) the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

The Contractor shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.

The Contractor shall designate a Data Protection Officer if required by the Data Protection Legislation.

Before allowing any Sub-processor to process any Personal Data related to this agreement, the Contractor must:

(t) notify the Customer in writing of the intended Sub-processor and processing;

(u) obtain the written consent of the Customer;



governed by a contract with certain provisions included.

To make sure our contractual arrangements comply with GDPR, we have enclosed new contractual commitments, see Appendix A. These supplementary provisions are an addition to any existing contract(s) with your organisation. These commitments include those required from data processors under Article 28 of the GDPR.

The update of your organisation's contract(s) may involve either using the new NHS Contract For Services when your contract is due to be renewed or the updating of existing contract terms by way of a contract variation based on the generic standard clauses published by the Department of Health and Social Care. The new contract terms and conditions will also ensure that specifications and service delivery schedules reflect the roles and responsibilities between the Controller and the Processor, as required by the new regulations.

Through the continued supply of products, provision of services and/or processing of person data as a data processor, you confirm your agreement to these commitments being added to your organisation's contract(s). Please complete and return Appendices B1 and B2 to:

[procurementsupplychain@bhrhospitals.nhs.uk](mailto:procurementsupplychain@bhrhospitals.nhs.uk)

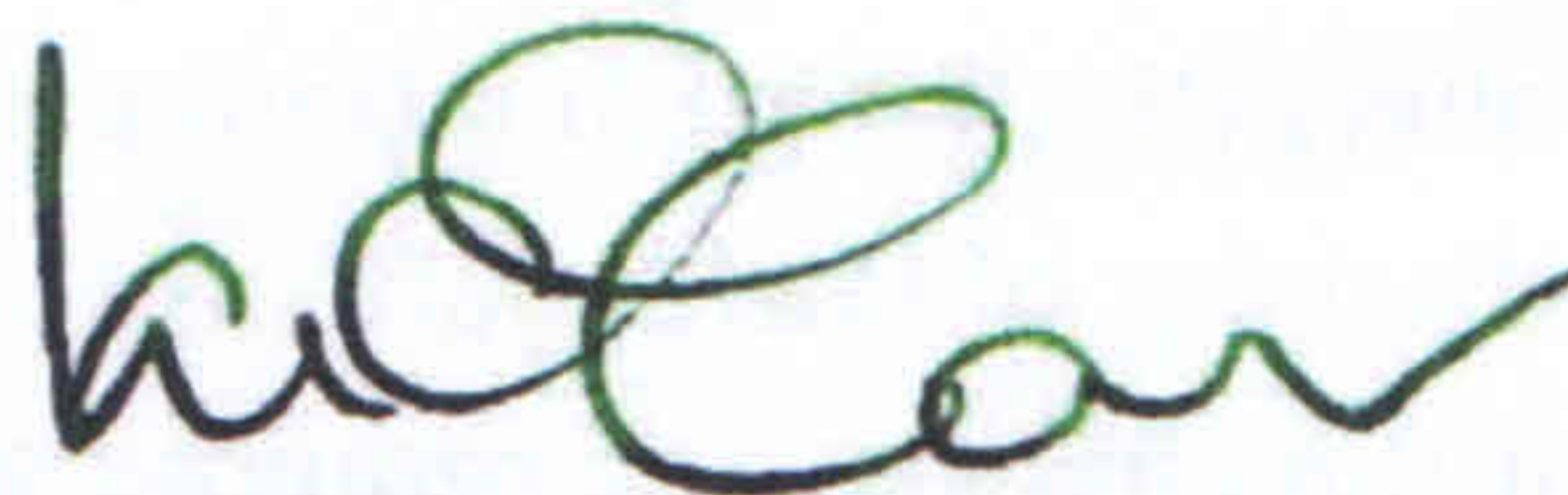
In any event, these commitments apply from 25 May 2018 regardless of updates to contractual arrangements.

Please retain a copy of this letter for your records and kindly acknowledge receipt by 25<sup>th</sup> May 2018. If you have any questions, please email us at the above address.

Yours faithfully



ADRIAN STOBIE  
DIRECTOR OF PROCUREMENT



IAN O'CONNOR  
DIRECTOR OF FINANCE



SARLA DRAYAN  
CHIEF PHARMACIST



## PART B - DATA PROTECTION

The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is as listed in Part C of this Schedule by the Customer and may not be determined by the Contractor.

The Contractor shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

The Contractor shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

- (a) a systematic description of the envisaged processing operations and their purpose;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
- (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this agreement:

(a) process that Personal Data only in accordance with Part C of this Schedule, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:

- (i) nature of the data to be protected;
- (ii) harm that might result from a Data Loss Event;
- (iii) state of technological development; and
- (iv) cost of implementing any measures;

(c) ensure that:

- (i) the Contractor Personnel do not process Personal Data except in accordance with this Schedule;
- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Contractor's duties under this Part B;

(B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

- (i) the Customer or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;
- (ii) the Data Subject has enforceable rights and effective legal remedies;
- (iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an



(v) enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Schedule such that they apply to the Sub-processor; and

(w) provide such information regarding the Sub-processor as the Customer may reasonably require.

The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

The Contractor may, at any time on not less than 30 Working Days' notice, revise this Part B by replacing it with any applicable controller to processor standard provisions or similar terms forming part of an applicable certification scheme.

The Parties agree to take account of any guidance issued by the ICO. The Customer may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any relevant guidance.

## **PART C – PROCESSING, PERSONAL DATA AND DATA SUBJECTS**

The Contractor shall comply with any further written instructions with respect to processing by the Customer. Any such further instructions shall be incorporated into this Part C.

<b>Description</b>	<b>Details</b>
Subject Matter of the Processing	[ State a brief high level description of the agreement ]
Duration of the Processing	The term of this agreement
Nature and Purposes of the Processing	<p>Nature: [ Examples: Collection / Recording / Structuring / Modification / Conservation / Extraction / Consultation / Disclosure by transmission / Dissemination / Interconnection / Alignment / Combination / Restriction / Erasure / Destruction – include as required ]</p> <p>Purpose: [state which aspect of the Services the processing is required for]</p>
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc. – include as required]
Categories of Data Subject	[ Patients and/or Staff of the Client – include as required]
Plan for return and destruction of the data once the processing is complete	[Describe how long the data will be retained for, how it be returned or destroyed]