St Helens & Knowsley NHS
Health Informatics

CONFIDENTIALITY AGREEMENT FOR THIRD PARTY SUPPLIERS

Stockton Heath Medical Centre

Do the rIGht thing

Version No: 2.0
Issue Date: August 2018

Confidentiality agreement for third party suppliers

1 Who are the third parties covered by this agreement?

Third parties are located on-site for a period of time as defined within their contract. They could include the following:

- Hardware and software maintenance and support staff (for all of the document)
- Cleaning, catering, security guards and other outsourced support services

2 General contractor clause (based on clause from Introduction to Data Protection in the NHS (E5127) and ISO 27002)

The Contractor undertakes:

- To treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee, servant or agent or sub-contractor of the contractor as a result or in connection with the contract; and

- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and

- To ensure that he, his employees, servants, agents and sub-contractors are aware of the provisions of the General Data Protection Regulations 2016 (GDPR) Data Protection Act 2018 and ISO 27002 and that any personal information obtained from the Practice shall not be disclosed or used in any unlawful manner; and

- To indemnify the Practice against any loss arising under the GDPR/ Data Protection Act 2018 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

All employees, servants, agents and/or sub-contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of the Practice sites where they may see or have access to confidential personal and/or business information (see last page).

3 Supplier Code of Practice (based on example from Introduction to Data Protection in the NHS (E127) and ISO 27002)

1 The following Code of Practice applies where access is obtained to personal data/information, (as defined within the GDPR/Data Protection Act 2018), held by the Practice for the purpose of preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade, replacement or any other related activity.

2 The access referred to in paragraph 1 above may include:-

a. Access to data/information on the Practice's premises
b. Access to data/information from a remote site
c. Examination, testing and repair of media (e.g. fixed disc assemblies)
d. Examination of software dumps
e. Processing using Practice data/information

3 The Supplier must certify that his organisation has notified the Information Commissioner that they are processing personal data (GDPR/Data Protection Act 2018) and that they are legally entitled to undertake the work proposed.

4 The Supplier must undertake not to transfer the personal data/information out of the EEA unless such a transfer has been registered, approved by the Practice and the country to which information is to be transferred has been deemed to have an adequate level of protection for personal information; or is a USA company which has signed up to a Safe Harbor agreement.

5 The work shall be done only by authorised employees, servants, or agents of the Supplier (except as provided in paragraph 12 below) who are aware of their personal responsibilities under the GDPR/Data Protection Act 2018 to maintain the security of the personal data/information held by the Practice.

6 While the data/information is in the custody of the Supplier it shall be kept in appropriately secure means.

7 Any data/information sent from one place to another by or for the Supplier shall be carried out be secure means. These places should be within the Supplier's own organisation or an approved sub-contractor.

8 Data/Information which can identify any patient/employee of the Practice must only be transferred electronically if previously agreed by the Practice. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the GDPR/Data Protection Act 2018 and ISO 27002. This will also apply to any direct-dial access to a computer held database by the Supplier or their agent.

9 The data/information must not be copied for any other purpose than that agreed by the Supplier and the Practice.

10 Where personal data/information is recorded in any intelligible form, it shall either be returned to the Practice on completion of the work or disposed of by agreed secure means and a certificate of secure disposal shall be issued to the Practice.

11 Where the Supplier sub-contracts any work for the purposes in paragraph 1 above, the Supplier shall require the sub-contractor to observe the standards set out in 3-11 above.

12 The Practice shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal data/information.

13 The Practice reserves the right to audit the Supplier's contractual responsibilities or to have those audits carried out by a third party.

14 The Practice will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the Supplier's employees and/or any agents and/or sub-contractors.

15 Any security breaches made by the Supplier's employees, agents or sub-contractors will immediately be reported to Karen Chriscoli, Practice Manager or Bev Hackwell, Executive Lead in KC's absence then depending upon the severity of the breach; report to the Data Protection Officer DPO

Third Party Agreement

Third Party Contracts requiring access to Clinical Systems

By completing and signing this formal request for access, the Supplier certifies that it understands that:

- Information concerning patients or staff is strictly confidential and must not be disclosed to unauthorised persons. This obligation shall continue in perpetuity.
- Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the GDPR/Data Protection Act 2018 or an action for civil damages under the same Act in addition to any disciplinary action taken by the Practice.

Further, the Supplier certifies that:

- It will not give access to any of the Practice's networks to any external organisation (NHS or not) unless that body has been formally authorised by the Practice to have such access.
- The Information Commissioner has been appropriately notified that it will be processing personal data.
- It is legally entitled to undertake the work agreed in the contract agreed with the Practice.
- It will abide by the requirements set out in para 1 - 15 above for handling any of the Practice personal data/information disclosed to their organisation during the performance of such contracts

A formal request for access is requested by:

Please complete in clear BLOCK **CAPITALS**

Company Name:	
Company Representatives Name:	
Job Number:	

Proposed purpose for access:	
Approximate Duration:	
Signed by:	
Dated:	
Approved by:	
Title:	
On Behalf of (Practice)	
Dated:	

Third Party Agreement outlining personal responsibility concerning security and confidentiality of information (relating to patients, staff and the business of the Practice)

In the course of your employment or associated work with the Practice, you may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised officer within the practice, on no account should such information be divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of registered computer data, will result in disciplinary action, which may lead to your dismissal.

You should also be aware that regardless of any action taken by the Practice, a breach of confidence could result in a civil action against you for damages.

You must ensure that all records, including VDU screens and computer printouts of registered data, are never left in such a manner that unauthorised persons can obtain access to them. VDU screens must always be cleared when left unattended and you must ensure you log out of computer systems, removing your password. All computer passwords must be kept confidential.

No unauthorised use of the internet or email is allowed.

I understand that I am bound by a duty of confidentiality and agree to adhere to the conditions within the Contract between the Practice and my personal responsibilities to comply with the requirements of the GDPR/Data Protection Act 2018.

NAME OF ORGNAISATION:	
CONTRACT DETAILS:	
PRINT NAME:	
SIGNATURE:	
DATE:	