Dunhill Medical Trust (DMT)

Title: Outsourcing and third party compliance
Version: 1.0
Date: March 2018
To be reviewed: March 2019
Classification: Public

Introduction

This Policy is a sub-policy of the Information Security Policy (ISP-01) and outlines the conditions that are required to maintain the security of the DMT's information and systems when third parties, other than the DMT's own staff, are involved in their operation.

Scope

This policy applies to any member of DMT staff who is considering engaging a third party to supply a service where that service may involve third party access to the DMT's information assets. It also applies to any third parties who may have access to the DMT's non-public information or systems for a specified purpose. This third party access could occur in a number of scenarios, common examples being:

- The use of cloud computing services;
- When third parties are involved in the design, development or operation of information systems for the DMT;
- When third party access to the DMT's information systems is granted from remote locations where computer and network facilities may not be under the control of the DMT;
- When users who are not staff of the DMT are given access to information or information systems.

Managing outsourcing risk

Prior to outsourcing or allowing a third party access to the DMT's non-public information or systems, a decision must be taken by staff of appropriate seniority that the risks involved are clearly identified and acceptable to the DMT. The level of staff seniority will depend on the nature and scale of the outsourcing.

Formal outsourcing

Where a service is formally outsourced by the DMT, the process must be managed by the relevant DMT staff and a contract must be in place that covers standards and expectations relating to information security (see 'Contractual issues').

Due diligence

The process of selecting a third party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the DMT is not exposed to undue risk. This process may involve advice from those with expertise in contract law, IT, information security, data protection and human resources, as appropriate.

This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the DMT.

Contractual issues

All third parties who are given access to the DMT's non-public information or systems must agree to follow the information security policies of the DMT.

Confidentiality clauses must be used in all contractual arrangements where a third party is given access to the DMT's non-public information.

Use of third party services must not commence until the DMT is satisfied with the information security measures in place and a contract has been signed.

All contracts with external suppliers for the supply of services to the DMT must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

Data Protection Legislation

An impact assessment must be completed at the outset of any project that will potentially involve personal data being accessed by a third party. Any outsourcing arrangement involving the transfer of personal data to a third party must include the acceptance of the DMT's standard personal data processing terms.

If the outsourcing involves the transfer of personal data outside the European Economic Area (EEA), it must only be to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Information Commissioner's Office (ICO) provides a list of countries it has deemed to provide an adequate level of protection. If the transfer is to the USA, the company or organisation must be signed up to the US-EU Safe Harbor scheme (or equivalent successor schemes) for the duration of the contract. The appropriate actions must have been taken under the prevailing legislation to ensure individuals are aware that their personal data may have been transferred outside the EEA.

Informal outsourcing

There are extensive IT services that are available to DMT staff via the internet which the DMT will have no formal agreement or contract in place with - examples include email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions and the DMT has no ability to negotiate as it would via the formal outsourcing procedure.

The use of such services for storing DMT information present a real risk to the DMT as there is no way the DMT can ensure the confidentiality, integrity and availability of the information without a formal agreement in place. In light of these risks, wherever possible, DMT staff should only use services provided or endorsed by the DMT for conducting DMT business. The DMT recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

DMT data which is subject to the Data Protection Act (and its successor legislation, for example, the General Data Protection Regulation) or which has a classification of confidential or above should be stored using DMT facilities or with third parties subject to a formal, written, legal contract with the DMT. In cases where it is necessary to otherwise remove data from the DMT, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

DMT staff must not configure their DMT email account to automatically forward incoming mail to third

party services with which the DMT has no formal agreement.