Exhibit C - Merge Healthcare Data Security and Privacy Principles

for Technology Support Services

The data importers provide information technology services and/or technical support and/or other support services to the Customer. This document provides an overview of the security measures implemented by the data importers. The Customer, in its capacity as the data controller, has reviewed and accepted the below measures and determined them to be appropriate to its data.

These Data Security and Privacy Principles apply to all activities where employees of the data importer or any third parties commissioned by it may have access to the Customer's personal data.

(1) Physical Access Control:

The servers on which the Customer's personal data will be processed are located within access-protected areas. Those areas are subject to data importers' internal security requirements (such as badge security, logbook, etc.). These requirements are subject to continuous checks (e.g. annual revalidation of continued business need and access authorizations).

(2) Logical Access Control:

Access to servers containing Customer's personal data is regulated by means of user IDs and passwords. An authorization approval process is required. User IDs are subject to regular validation.

(3) Data Access Control:

Designated support employees may access the Customer's personal data located on the servers and download data within the data importers' network, including on individual workstations, for the sole purpose of management and resolution of problems and implementations of solutions (see paragraph 4 below regarding Transfer Control).

(4) Transfer Control:

The data importers' internal IT infrastructure is required to have access controls, user IDs, password rules, internal network access reviews and firewalls to prevent access from external networks.

Systems and components are checked regularly to confirm that these protective measures are in place. Transfer of data within the data importers' network shall take place behind the data importers' firewall.

(5) Entry Control:

The data importers will use such data for the sole purpose of management and resolution of problems and implementations of solutions. Data will not be used for further data processing or for any additional business processes. No personal data will be modified or deleted on Customer's systems without Customer's consent.

(6) Order Control:

Data analysis will be performed by order of the Customer only based on a service request to data importers' call management tool to identify and/or solve a problem within the Customer's hardware and software installations, or by other authorized services resulting in a work order assigned to data

importers' designated personnel. The data importer's call management tool is subject to the protective measures in Section 4 above.

(7) Separation Control:

The protective measures described in Sections (1)-(6) above are designed and sufficiently appropriate to prevent access by individuals other than those authorized by the data importers.

(8) Compliance:

To verify adherence by data importer employees to data importers' security policy:

- Security assurance health checks and security technical testing are conducted by the data importers at periodic intervals.
- Security process reviews are conducted at periodic intervals by the data importers' internal audit and business controls functions on a representative sample of data importers' computing system platforms.

Employees of the data importers are reminded at least on an annual basis of their job-related obligations, including ethical business conduct, confidentiality obligations and security responsibilities.