Information Security Assurance Assessment For Data Processing or Data Sharing Activities

Name of contract/agreement:	**LATITUDE Data Processing Agreement**
Indicate reason for transfer: e.g. data processing or information sharing.	**Data Processing**
Purpose:	**Processing of personal data of patients and hospital staff for diagnostic purposes, patient care, patient/physician administration and any other purpose determined by the Trust**

It is a legal requirement that the Trust whenever engaging in activities that require personal identifiable data (PID) to be transferred for data processing or information sharing purposes not only are justified but also occur with respect to:

> *The Data Protection Act 'Seventh Principle'*
> *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".*

The assessment will take into account whether security measures are "appropriate". In respect to the level of security appropriate to the risks represented by the processing considering:-

(i) Taking into account the state of technological development at any time and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

(a) the harm that might result from a breach of security; and

(b) the nature of the data to be protected.

(ii) The data controller must take reasonable steps to ensure the reliability of staff having access to the personal data.

(a) Management and organisational measures.

Data Processing or Data Sharing Activity

What information items are being transferred?	Demographic data (name, date of birth, phone number, …) Implanted device data (model, serial number, device parameters) Patient health data (cardiac condition, body weight, …) Patient care data (device programming, alerts, …)
Have the data subjects been informed what information, is being processed by who and where?	Yes, patients sign a Data Authorization Form
What country is the information being transferred to?	Data is transferred to Guidant Europe NV, a Boston Scientific company located in Belgium. Data are physically stored on servers in the UK and the Netherlands
What are the purposes of the transfer?	Diagnostic purposes, patient care, patient/physician administration and any other purpose determined by the Trust
What data protection laws are in place in the overseas country?	Data are processed in compliance to Belgian data protection laws in accordance with European Data Protection Directive 95/46/EC and Swiss law.

Assessment Criteria

Security management:	Describe measures/controls	Insert Evidence
1. Is the company registered compliant with European Data Protection Legislation OR the US-European Union Safe Harbour process? Does the company have a security policy setting out management commitment to information security within the organisation?	Yes, the Boston Scientific company Guidant Europe NV has registered the data processing with the Belgian Data Protection Authority Yes, Boston Scientific has implemented Standard Operating Procedures that call out specific data protection obligations under European Data Protection requirements	Registration can be consulted in the public register on http://www.privacycommission.be/ Internal SOP 001171 available on request
2. Is responsibility for the organisation's security policy clearly placed on a particular person or department?	Yes, Boston Scientific has assigned a dedicated Data Privacy Officer	Elimu Kajunju, Esq., CIPP, CISSP Chief Privacy Officer Boston Scientific Corporation 4100 Hamline Avenue North, Mail Stop 3-302 St. Paul, MN 55112

		Tel: (651) 582-3620; Email: elimu.kajunju@bsci.com
3. Are sufficient resources and facilities made available to enable that responsibility to be fulfilled?	Yes	
Controlling access to information:		**Insert Evidence**
4. Is access to the building or room controlled or can anybody walk in?	The LATITUDE computer equipment is managed by an independently accredited hosting provider. It is hosted in a Tier 4 data centre (which is the most stringent level as defined in TIA-942) with segregated access control. Security is enabled by limiting access to the facility in general. Furthermore, LATITUDE equipment is segregated into a separately secured "cage" which is not shared with other systems. Boston Scientific follows the ISO 27001 standard and contractually requires its business partners (i.e., hosting provider) to provide the same level of security.	Boston Scientific has a SAS70 report from the hosting provider which confirms the adequacy of the provider's security controls.
5. Can casual passers-by read information off screens or documents?	No	Boston Scientific staff accessing LATITUDE data are located in a separate area within an access controlled building.
6. Are passwords known only to authorised people and are the passwords changed regularly?	Yes	Boston Scientific staff access the LATITUDE system using two-factor authentication, where the second factor is a token code changing every 60 seconds. Subsystem access is highly restricted to LATITUDE Engineering Operations staff.

7. Do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned?	Data access in controlled at user level – multiple access privileges are assigned according the user's specific data access needs.	At the time of user login, the LATITUDE system will verify a specific user's assigned access capabilities and only allow access to records and functions that are granted by their current account access rights. Boston Scientific support staff has access to the entire dataset – Read-Only and Read-Write access are assigned based on user's role. Clinician users are restricted to access only data from their clinic and according to physician delegation levels. The LATITUDE system actively monitors user access to the system.
8. Are user access rights/changes activated and deactivated in a timely manner?	Yes	At regular intervals the list of employees with (sub-)system access will be audited according to internal standard operating procedure *Performing LATITUDE User Access Security Audits.*
9. Is there a procedure for securely cleaning media (such as tapes and disks) before they are reused or are new data merely written over old? In the latter case is there a possibility of the old data reaching somebody who is not authorised to receive it? (e.g. as a result of the disposal of redundant equipment).	Appropriate cleaning instructions are employed to prevent unauthorized access	LATITUDE requires usage of validated secure data destruction as specified by the US DoD National Industrial Security Program Operating Manual (NISPOM - US DoD 5220.22-M) for all LATITUDE data including system and security information, customer data, system and audit logs, etc.

10. Is all removable media including but not exclusive to laptops, CDs, Floppy disks, Hard drives, USBS, medical devices encrypted to AES 256 encryption standard or equivalent. Please specify what encryption tool/solution(s) are employed by the organisation.	Yes	Encryption during storage (encryption method(s) used) LATITUDE uses hardware-based 256-bit AES full-disk encryption solution for its data storage.
11. Are transfers of personal identifiable data done so securely? Please state how the data is intended to be transferred securely between the data controller and the data processor.	Yes - The LATITUDE system ensures that the data transmitted from the patient location to the clinician browser is securely managed. Industry standard forms of security including data encryption in transit and at rest, multiple levels of firewalls, and intrusion detection have been implemented as part of the system design.	Encryption during transport (encryption method(s) used) Boston Scientific employs a Public Key Management System (PKMS) based on X.509 V3 format with a 2048-bit RSA Key Pair for digital signatures and identity certificates used for mutual authentication between the Patient monitoring devices and the LATITUDE Server.
12. Is printed material disposed of securely, for example, by shredding level considered appropriate for the destruction of confidential data?	Yes	Boston Scientific staff accessing LATITUDE data are instructed to promptly dispose of any printed materials no longer required. A shred box is installed for this purpose.
13. Is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?	Yes	Clinician users are authenticated using a security question Patients are verified using date of birth
14. Is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home? What security measures are individual members of staff required to take in such circumstances?	Personal Data is not removed off-site	

15. Are responsibilities for security clearly defined between a data processor and its customers? Version 1 [as print date] 42 Data Protection Act 1998	Yes	Data Processing agreements are in place with all parties involved in data processing
16. Is restriction on further use of the information appropriately covered in the contractual arrangements between the organisations?	Yes	Data processing agreements specify the processing purposes and restrictions.
Ensuring business continuity:	**Describe measures/controls**	**Insert Evidence**
17. Are the precautions against burglary, fire or natural disaster adequate?	Yes	The LATITUDE servers are sited at a third-party hosting facility with rigorous physical security and business continuity safeguards. Boston Scientific has a disaster recovery plan that provides for a geographically separate backup system and off-site storage of critical recovery data.
18. Is the system capable of checking that the data are valid and initiating the production of back-up copies? If so, is full use made of these facilities?	Yes	LATITUDE utilizes several methods to ensure data integrity including state-of-the-art encryption techniques, data hashing algorithms and other integrity checks throughout the system
19. Are back-up copies of all the data stored separately from the live files? If yes where are they stored?	Yes	The LATITUDE data retention process employs tape storage in a secured off-site facility
20. Is there protection against corruption by viruses or other forms of intrusion?	Yes	Malicious software detection and intrusion detection mechanisms are an integral part of LATITUDE system requirements
21. Have arrangements for future access or disposal	No, after the data processing agreement has	Boston Scientific does provide the

of the data in the event of the contract end or dissolve of the company been specified?	ended, LATITUDE data access is revoked.	possibility for integrating LATITUDE data with the clinics electronic medical records system. This allows for LATITUDE data to be automatically uploaded and appended to the patient record.
Staff selection and training:	**Describe measures/controls**	**Insert Evidence**
22. Is proper weight given to the discretion and integrity of staff when they are being considered for employment or promotion or for a move to an area where they will have access to personal data?	Yes	Staff is specifically trained on the importance of data protection and a specific addendum to their employment contract reinforces this
23. Are the staff aware of their responsibilities? Have they been given adequate training and is their knowledge kept up to date?	Yes	See above
24. Do disciplinary rules and procedures take account of the requirements of the Act? Are these rules enforced?	Yes	Data Protection principles and requirements have been included in a multitude of Corporate and LATITUDE specific standard operating procedures and employees are required to re-certify on these procedures on a regular basis. Compliance to these procedures are implemented in each employee's performance objectives and evaluated on a regular basis.
25. Does an employee found to be unreliable have his or her access to personal data withdrawn immediately?	Yes	Yes, prompt disciplinary action is taken as deemed necessary
26. Are staff made aware that data should only be accessed for business purposes and not for their own private purposes?	Yes	This is specified in the global Information Assets Protection policy (standard operating procedure) and emphasized in the specific

		addendum to the employment contract staff accessing LATITUDE need to sign.
Detecting and dealing with breaches of security:	**Describe measures/controls**	**Insert Evidence**
27. Do systems keep audit trails so that access to personal data is logged and can be attributed to a particular person?	Yes	Audit logs are implemented on all systems that store or process critical (PHI) information.
28. Are breaches of security properly investigated and remedied; particularly when damage or distress could be caused to an individual?	Yes	As part of compliance to ISO 27002 standard, in the unlikely event of a security incident reported by external hosting vendors, customers (physicians, allied professionals and patients), or Boston Scientific employees, designated teams are charged with proper assessment and investigation. This has been specified in internal standard operating procedures, notably the Latitude Security Incident Response Process.
29. Have procedures for Subject Access requests under the Data Protection Act 1998 been considered?	Yes	Data Subjects are informed of their rights and provided with contact information should they wish to exercise those rights.

The Data Protection Act introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller. In order to comply with the Seventh Principle the data controller must –	Describe measures/controls	Insert Evidence
30. Choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take.	Technical and organizational security measures are in place.	Technical security measures are taken to safeguard the physical integrity of the system and the data contained in it (this includes encryption in transit and at rest, multiple levels of firewalls and intrusion detection). Organizational security measures have been implemented, notably restricted access to the LATITUDE system, persons accessing the data are informed that they are subject to applicable data protection laws and are bound by appropriate use and confidentiality obligations and provided with data protection guidelines.
31. Take reasonable steps to ensure compliance with those measures, and ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the Version 1 [as print date] 43 Data Protection Act 1998 data controller by the Seventh Principle.		A Data Processing agreement is signed between the Trust and Guidant Europe NV/SA, a Boston Scientific Company

32. The organisations data protection notification is in date: Please supply the organisations data controller's notification registration number. This is available by searching on the public register of data protection notifications at www.ico.gov.uk. Obviously some forms of processing do not require notification to the Information Commissioners Office. Only provide if your processing activities require notification.	The Boston Scientific company Guidant Europe NV has registered the data processing with the Belgian Data Protection Authority	Registration can be consulted in the public register on http://www.privacycommission.be/

The assessment will not just take into account whether assurances are deemed appropriate in respect to the processing in line with Principle Seven but will also assess as a whole the measures to be taken by data controllers/processors to provide security against any breaches of the Data Protection Act rather than just breaches of security.

Agreement:

I Stéphane Hübner, am authorised to complete this Information Security Assurance Assessment document on behalf of Guidant Europe NV/SA, a Boston Scientific Company.

That I believe the 'Information Security Assurance Assessment' to be true and accurate assessment of the technical and physical measures employed by the organisation to protect personal identifiable data and other confidential information (e.g. commercially sensitive data) supplied to the organisation under the terms an conditions of the LATITUDE Data Processor Agreement.

I understand that this information will be used by the Trust Information Governance function to assess the level of risk to information or personal data supplied under the terms of the said LATITUDE Data Processor Agreement.

I understand that the assessment may lead to further recommendations requirements to be fulfilled by Guidant Europe NV/SA, a Boston Scientific Company in order to ensure the level of risk is acceptable to allow the transfer of data to occur.

Role: LATITUDE Customer Support Manager

Print name: Stephane Hübner

Signed:

Date: 20 May 2011

Stéphane Hübner

Boston Scientific
LATITUDE® Customer Support