GDPR QUESTIONS AND RESPONSE: HEALTH ASSURED

No.	Data Protection Compliance	Y/N	Responses
1	Will you be in a position to meet your obligations as a data controller or processor (as applicable) under the GDPR by 25 May 2018?	Yes	Health Assured currently processes all personal data in accordance with the Principles of the Data Protection Act 1998. Health Assured are aware of GDPR and its obligations and are currently considering our position in relation to it and the compliance manager is driving the project forward. We are aiming that any required changes will be implemented before May 2018 to ensure we are as compliant as can be by 25th May 2018.
2	Do you have a DPO? Please provide details. If you do not have a DPO who is responsible?	Yes	Gail Tuck: Group Compliance Manager
3	Do you have GDPR-compliant data protection and information security policies?	No	All policies and procedures are compliant with ISO27001. We are in the process of reviewing and finalising our policies and procedures to ensure that they will be GDPR compliant by 25th May.
4	Can you confirm that you have appropriate measures in place to ensure that you, your staff and any subcontractors/sub-processors do not process personal data except on documented instructions from the client?	Yes	Policies, Procedures and controls have been implemented to ensure that personal data is not processed except on documented instructions from the client.
5	Do you have systems and procedures to notify recipients to whom personal data has been disclosed regarding data subject requests to rectify, erase or restrict the processing of their personal data? Please provide details.	Yes	Procedures are currently under review to contact processors in the event of a person making a request for rectification, erasure or restriction. This will also be captured in data processing agreements.
6	Will you be providing training to your staff on compliance with the GDPR? If so, please provide details.	Yes	Training is already in progress. The whole business will receive GDPR training and more in-depth training will be provided for managers as required.

	IT Security Policy		
7	Who is responsible for IT Security in the organisation? Please provide details.	Yes	**Mark Winstanley.** Information Security Manager mark.winstanley@peninsula-uk.com **Gail Tuck**. Group Compliance Manager gail.tuck@peninsula-uk.com
8	Does an IT security policy exist and, if so, how is it communicated to employees?	Yes	During induction training and reinforced periodically during training sessions throughout the year.
9	What policies and procedures do you have in place for immediate reporting and investigation of suspected data security breaches, and remedial action in respect of actual breaches? Do you have a data security breach policy?	Yes	Data Protection Policy and a Data Breach policy
10	Is your organisation compliant and certified for any recognised IT Security and Data Protection standards.	Yes	Health Assured is ISO27001 certified and holds Government accredited Cyber Essentials certification (Certificate Number: 1089522795658013). Health Assured use Salesforce.com's cloud for data storage, which is certified to ISO27001 standards (Accreditation Number:IS559052). Their services can deliver solutions compliant with HIPAA, PCI DSS and FISMA.
	Physical Security		
11	How is the physical security of buildings providing Information Services to the company ensured.	Yes	The reception is staffed 24/7. A door access control system is in place throughout the building and all entrances are monitored by CCTV including the Data Centre.
12	What specific precautions are used to ensure only authorised access to areas containing data processing, communications and storage equipment used for company data.	Yes	Secure areas are protected by appropriate entry controls to ensure that only authorised staff are allowed access. Staff requiring access to secure areas are limited to the minimum required and their access removed when their employment ends or move roles. They are issued with an access control card that allows them entry. CCTV monitoring is deployed at all access points.

13	Do you have a Disaster Recovery/Business Continuity plan? If so, When was the last test and what were the results? Has all necessary remediation been carried out and retested?	Yes	A full annual DR test is conducted within Salesforce and Individual components are tested individually on a regular basis. All necessary remediation has been carried out.
	Staff Security		
14	Do you have a dedicated team to support Information and Cyber Security?	Yes	As part of the Peninsula Group, Health Assured has a dedicated InfoSec team with network security SIEM platform and incident monitoring. Similarly, Salesforce has a 24/7 SOC.
15	How are staff Screened prior to employment?	Yes	CV and phone screening. Face to face interview. Induction in data protection. Clinical staff qualifications checked for validity and membership to professional bodies.
16	Do Employment Terms & Conditions cover information security responsibilities including data protection?	Yes	These are included in the Employee handbook, which is issued to all new employees.
17	Do these contain confidentiality clauses?	No	However, a Restrictive Covenant is signed prior to employment. All staff are then required to sign a confidentiality agreement on the first day of their employment. Also contained within the employee handbook.
18	Please explain the approach to ensuring that staff are adequately trained in IT Security and Data Protection principles.	Yes	All staff receive security training as part of induction. This is reinforced periodically during training sessions and presentations.
19	What is the internal process for reporting and managing security incidents	Yes	All security incidents are managed by the InfoSec team, logged, and investigated accordingly.
20	How quickly is staff access revoked on them leaving employment?	Yes	Immediately. Health Assured have a leaver's policy in place, in which a leaver form is circulated to a group of system administrators with a termination date. The system administrators disable the accounts, blocking all access on the date specified.
21	What protection is in place to ensure that staff credentials are not compromised by malware, remote access tools, keyboard loggers etc.	Yes	Antivirus and malware protection is deployed on all endpoints to detect, alert and neutralise these threats.

	Data Security		
22	What Operating Systems are in use and what steps are taken to ensure they are protected.	Yes	Desktops and laptops use Windows 10 or Windows 7. A rollout is in progress to move all endpoints to Win10. Windows updates are pushed out and installed automatically
23	How is it ensured that software used to process company data is kept up to date.	Yes	All software is managed and patched centrally. Only approved software is permitted on user machines and updates are managed through Software Centre
24	Will vendor staff ever carry company data on portable devices (inc storage media)? If so how will the data be protected from loss/theft.	No	This is prohibited. However, all laptops are encrypted for added protection.
25	What measures are in place to prevent unauthorised access to Data from outside "hackers" (e.g. firewalls and other security measures) and to what extent is the adequacy of current precautions monitored?	Yes	External connections are protected with enterprise, resilient firewalls and dedicated security monitoring ex. SIEM, IDS, IDP
26	What restrictions are in place to ensure control of data entering or leaving via internet access (via web browser, email, ftp, online storage etc.)?	Yes	Internet access is controlled by a dedicated Web filtering appliance, which restricts the types of traffic and URLS. Firewalls and monitoring control and monitor traffic entering and leaving the organisation.
27	Which Applications will host company Information? Please identify any in use, which are not fully supported by the software provider.	Yes	Salesforce is the primary platform. No sensitive information would be stored on unsupported systems.
28	How are application patches evaluated, tested and deployed?	Yes	All patches are governed by the Change control process, which includes evaluation, testing and deployment.
29	What security mechanisms are in place to protect access to the company's data?	Yes	All access is controlled through ADS permissions and access is granted on the principle of least access. Security monitoring has been deployed including a dedicated SIEM platform.
30	What are the password complexity requirements?	Yes	All passwords must be unique and complex: 8 characters minimum with one small case, capital letter, symbol and number.

31	How often are passwords forced to change?	Yes	Password changes are enforced every 30 days.
32	Are idle time screensaver locks enforced for all staff? If so what is the timeout?	Yes	2 minutes
33	Can you confirm that all default admin and application backdoor accounts have been removed?	Yes	A standard build procedure ensures that all default admin and backdoor accounts are removed. Network monitoring identifies any non-compliance.
34	For systems, which are accessible to users from the Internet, what precautions are taken to prevent the existence and exploitation of web application vulnerabilities such as cross scripting or SQL Injection.	Yes	A dedicated web application firewall protects the application from malicious actors and vulnerabilities such as cross-site scripting and SQL injection. External facing websites are scanned regularly to identify any vulnerabilities, which are addressed immediately.
35	Where is information stored?	Yes	Within the secure CRM platform (Salesforce).
36	How is access secured?	Yes	Access control is managed through the database platform. This integrates with internal Active Directory security. Salesforce is accessed via https secure internet browser.
37	Is the data encrypted?	Yes	Full database encryption is in place and secure SSL web access for client portal access
38	If so how is the encryption key managed	Yes	Encryption keys are managed in accordance with strict policies and procedures. The key is stored in a secure location, which is accessible only to data base admins.
39	Is a Data Loss Prevention in place.	No	Data Loss Prevention is currently managed by policies, procedures and controls. However, a dedicated DLP appliance will be deployed in the near future.
	Backup System		
40	How is data backed up?	Yes	Data is backed up continuously through the high availability platform. In addition, all data is backed up to physical media daily.
41	How is access to backup data secured?	Yes	Physical backup media is encrypted using AES256 bit encryption
42	How often will data be backed up?	Yes	Data is backup to physical media on a daily basis.
43	How often is the data restore process tested?	Yes	The restore process is tested monthly or as required.

44	What other measures are in place to ensure data integrity and continuity.	Yes	Performance monitoring and File integrity monitoring are in place.
	Local Storage		
45	What controls are in place for making local copies of data on PC Hard Drives/USB keys/DVD-RW etc?	Yes	Local copies are not allowed. This policy is enforced through Microsoft Group Policy and Kaspersky device control.
46	Please explain any policies or circumstances that could lead to company data being held on employees personally owned devices and controls over this.	Yes	The written policy states clearly that this is forbidden and this policy is enforced through technological controls. InfoSec and Director approval is required for policy exceptions.
47	Will personal data be stored and/or processed on equipment outside of vendor premises? If so, please give details of how and where together with associated security controls.	Yes	Some employees work from home and use corporate laptops, but no data is stored on laptops by default. Laptops are encrypted and protected by antivirus plus security is enforced by Group Policy
	Retention/Disposal		
48	What is your retention/deletion policy that applies to personal data?	Yes	Data is retained in line with Health Assured's Retention Policy. Therefore, we are committed to taking a practical approach in line with legal, contractual and commercial requirements when dealing with the ownership, retention and disposal of information relating to our business activities within the UK and Ireland. Data is destroyed/deleted when we no longer have legal, contractual or commercial requirements to hold the data.
49	Are there any circumstances in which a copy of any personal data is stored after the end of the services?	Yes	Only as per the data retention policy
50	How is paper information containing company data destroyed?	Yes	Confidential waste bins are located on each floor and this is securely shredded by a vetted third party.
	Cloud Services & 3rd Party Access		
51	Does your organisation use Cloud Storage facilities for processing data?	Yes	Yes. Salesforce is built on secure cloud infrastructure.

52	How is security maintained and tested?	Yes	Salesforce has a dedicated security team, which regularly tests and verifies that all controls are operational. Salesforce is Crest approved.
53	Does all data reside in the EU?	Yes	All data resides in the Primary Data centre in the UK and secondary in Germany.
54	What contractual IT Security Requirements are in place with third parties?	Yes	Contractual requirements with Salesforce mandate that all data is stored in Tier 1 data centres within the EEC, with appropriate controls and monitoring for Tier 1. Further, all Health Assured data is not only segregated from other customers but from other Peninsula Group Business units.
55	Do you have in place with third parties written contracts including conditions requiring compliance with Data Privacy legislation?	Yes	Health Assured has a contract in place with Salesforce, which is compliant with Data Privacy legislation. The Information Security manager worked with the Salesforce director to ensure security and data protection.