University Hospitals Plymouth NHS Trust

DATA PROTECTION IMPACT ASSESSMENT TOOL

The Data Protection Impact Assessment Tool is a risk assessment tool that should be used at the start of all projects/changes to identify and manage Data Protection concerns. For help with completion of this tool, please see the Data Protection Impact Assessment Procedure.

Project Title:	**Telecare in Audiology**	**Project Ref:**	**N/A**
Senior Responsible Owner (SRO)	**Name: xxxxx**	**Information Asset Owner (IAO)**	**Name: xxxxx**
	Email: xxxxx		**Email:xxxxx**
	Telephone: xxxxxx		**Telephone: xxxxx**
Business Case Manager (BCM)	**Name: N/A**	**Information Asset Administrator (IAA)**	**Name: xxxxx**
	Email:		**Email: xxxxx**
	Telephone:		**Telephone: xxxxx**
Project Manager	**Name: N/A**	**Date:**	
	Email:		
	Telephone:		
External Organisations/Suppliers/ Companies involved in this project/change (Please list):	**GNReSound (hearing aid manufacturer)** **Auditdata (supplies existing audiology patient management system, but not directly involved in the project)**		

Project/Change Description: (what is the new project/change being implemented?)

(To improve access, outcomes and efficiency we have the option to use cloud-based support for our patients. We currently have a backlog of nearly xxxxx patients, and this project is part of the work to reduce this and reduce further build-up. It also provides care closer to home, utilising digital systems and services to reduce travel, patient time and staff time.)
Patients' hearing aids are linked to their smartphones. Via this link, they will be able to provide feedback from their smartphones, via a cloud-based system. We will then be able to reprogramme their hearing aids to meet their needs using our existing hearing aid software - this data will be sent back via the cloud-based system to their smartphones, and they can then upload this reprogramming into their hearing aids.

Version Control		
Version Number:	**Date:**	**Comment:**

University Hospitals Plymouth NHS Trust

DATA PROTECTION IMPACT ASSESSMENT TOOL

Section 1				
Number	**Assessment Questions**	**Yes**	**No**	**Response (please add a response for all questions answered 'Yes')**
1	Does this project/change involve information about people?	Yes		The information that will be held contains: individual patient information, patient reported communication difficulties, hearing aid programming data.
2	If this project/change does involve information about people - can the person be identified?	**Yes**		**Please see section 2**
3	Can the information be pseudonymised or anonymised in any way?	**Yes**		Both fields are pseudonymized information in GNOS as it must be combined witch HCP local data to get the actual customer information (we don't do this).
4	Will information about individuals be disclosed to organisations or people who have not previously received it?		**No**	

DATA PROTECTION IMPACT ASSESSMENT TOOL

5	Is this a new or existing system?		**No**	**If yes, specify if new or existing** **If no, then no response is required to questions 5 & 6**
6	If this is an existing system, is there an up to date System Level Security Policy (SLSP) for this system?	**Yes**		**SLSP for Auditbase in place**
7	If this is a new system, is an SLSP being drafted?			
8	Is this system currently recorded as an information asset on the Information Asset Register or will it be added in due course?	**Yes**		
9	Are there any contracts or information sharing agreements in place to support the implementation of this project/change?		**No**	

If you have answered 'yes' to any of the questions in Section 1, please continue to Section 2. If not, go straight to Section 3 – The Declaration				
Section 2				
Number	**Assessment Questions**	**Yes**	**No**	**Response**

DATA PROTECTION IMPACT ASSESSMENT TOOL

<table>
<tr><td>10</td><td>Who is the subject of the information?</td><td></td><td></td><td>Hearing aid users – NHS patients within Audiology</td></tr>
<tr><td>11</td><td>What type of data is being held?
(highlight in red all that apply)</td><td></td><td></td><td>
<table>
<tr><td>Name</td><td>Gender</td><td>Date of Birth</td></tr>
<tr><td>Ethnicity</td><td>NHS Number</td><td>Hospital Number</td></tr>
<tr><td>Address</td><td>Post Code</td><td>Email</td></tr>
<tr><td>GP</td><td>Religion</td><td>Sexual Orientation</td></tr>
<tr><td>Political Opinion</td><td>Trade Union</td><td>Job Title</td></tr>
<tr><td>Next of Kin</td><td>Medical History</td><td>Genetic/ Biometric</td></tr>
<tr><td>Audio Recording</td><td>Visual Recording</td><td>National Insurance Number</td></tr>
</table>
</td></tr>
<tr><td>12</td><td>What purpose does the collection of data serve?</td><td></td><td></td><td>Is included in consent:
“Where you provide Part A Consent, you consent to your Hearing Care Professional (HCP) and/or the Manufacturer (as specified) receiving and processing the following personal information about you in the manner, and for the purposes, detailed below which <u>IS NECESSARY</u> in order for the GN Online Services to be provided to you:
The following data categories are processed by the Manufacturer and HCP:
• Your name and email address: for the purpose of enabling fine-tuning and logging your consent.
• Hearing threshold, hearing threshold shift, and other details regarding your hearing loss (health information): for the purpose of enabling fine-tuning.
• The length of time you use your hearing instrument: for the purpose of enabling fine-tuning and optimizing your settings.</td></tr>
</table>

				• **The hearing instrument's serial number, hardware identification number and software version** for the purposes of enabling fine-tuning and enabling firmware updates. • **Fitting specifications and fitting type**: for the purpose of enabling fine-tuning and optimizing your settings. • **Hearing instrument settings**: for the purpose of enabling fine-tuning and optimizing your settings. • **Information about the sound environment when sending a request via the app**: for the purpose of enabling fine-tuning and optimizing your settings. The following data categories are processed by the Manufacturer: • **Device type information**: Generic device-specific information such as the type of mobile device and mobile operating system: for the purpose of optimizing your settings and providing customer services (questions, complaints, repair, etc). • **Technical log information**, Technical information in server logs, e.g., details of how the apps are used, Internet protocol, device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL: for the purpose providing customer services (questions, complaints, repair, etc). • **Location information**, when the location and GPS-enabled services are in use, the Manufacturer may collect information that show

DATA PROTECTION IMPACT ASSESSMENT TOOL

				the countries and locations where the app is being used; for the purpose of optimizing your settings. (You are free to switch off the location and GPS function on your mobile device at any time and prevent the collection and processing of this information). The data above is hosted by Microsoft Ireland on the Manufacturer's behalf (see the **"Third Party"** section below for further information).
13	What is the legal basis for processing this data?			A process of consent is included within the software\app
14	Does the project apply new or additional information technologies that have potential for privacy intrusion? If yes, provide further information.	**Yes**		All permanently stored health data is stored on external data storage media hosted by the sole external infrastructure provider – namely Microsoft Azure. No health data is stored without a specific consent from the user (be it the HCP Admin, HCP or the end-user). Data is stored in an encrypted fashion utilizing standard data base encryption provided by Microsoft SQL Server as provided via Azure core services. Microsoft Azure data centers are compliant to very strict security and is governed via the service level agreement (SLA) between Microsoft and GN Hearing.
15	Does the implementation of this project/change improve any existing data protection risks? Provide details in the response section.		**No**	

DATA PROTECTION IMPACT ASSESSMENT TOOL

16	Are there any existing data protection risks that will not be mitigated by this project/change? If yes, provide further information.		**No**	
17	Have any of the organisations involved in this project/change completed a Data Security & Protection Toolkit submission or are accredited to ISO 27001? If so, provide details.	**Yes**		Microsoft's Azure is compliant with and certified per the following standards relevant for network security aspects: • ISO 27001 • SOC2 reports GN Hearing use ISO 27001 as a framework for GNOS with IT Security Policies and Procedures included Risk handling and SOA/Statement of Applicability
18	If there are any external organisations involved in the project/change, are they registered as a fee payer with the Information Commissioner's Office and what is the registration number?		**No**	
19	Does the project/change involve new or changed data collection practices? If yes, provide details.	**Yes**		**See 14**
20	Does the project/change involve new or changed consolidation, inter-linking, cross referencing or matching of personal data from multiple sources?		**No**	
21	How will the information be kept up-to-date and checked for accuracy and completeness?			Through review processes (e.g. User review). HCP's have the responsibility to asses/review own users to GN Online services to ensure accuracy and completeness.

DATA PROTECTION IMPACT ASSESSMENT TOOL

				Demographic data is kept up-to-date via existing PAS link to Auditbase
22	Does the project/change involve new or changed data security arrangements? If yes, give details.		**No**	
23	Does the project/change involve new or changed data disclosure arrangements? If yes, give details.	**Yes**		The HCP will be presented for a Privacy information notice to hearing care professional as part of the activation process for each user to allow finetuning of a hearing instrument
24	If the data subject makes a request to see the data held about them can this be easily obtained from the system?	**Yes**		GN DPO (Data Protection Officer) is responsible for all requests regarding GDPR (General Data Protection Regulation) and rights. Request about this is included in GN Data Privacy Policy: https://www.resounds.com/en-gb/privacy
25	What is the data retention period? Is data deleted/destroyed after the minimum retention period?	**Yes**		GN Online Services retains data for minimum 10 years from creation date. MDD/ISO 13485/RED directive requirements.
26	If the project/change involves the implementation of a new system to collect information about patients, is the system compliant with the NHS number?	**N/A**	**N/A**	**We don't collect NHS number in GN Online Services.**
27	Does the project/change provide a facility for separate testing and a dedicated training environment which does not utilise live patient data? Provide details.	**Yes**		**There are different environments (Test and Verification) in which the tests take place before releasing to production.**

DATA PROTECTION IMPACT ASSESSMENT TOOL

28	Who will have access to this information? What are their access controls?			GN IT (IT operational purposes & builds with 2 Factor login), R&D (Read access with 2 factor login for special purposes if needed for troubleshooting), DPO for access/support of GDPR requirements.
29	Detail how audit records of staff recording, accessing and sharing information will be created and held.			GNOS have an audit trail of user activities. The system will not connect to an integrated audit solution. The customer has the responsibility for always ensure the correct internal users (HCP/employees) have the correct access/role to GNOS trough the GNOS user portal. The user activity/audit log is for internal GN purposes, and not accessible for customers. Auditbase logs all activity via username, and has a comprehensive security log.

Section 3

DATA PROTECTION IMPACT ASSESSMENT TOOL

Following the completion of the questions above, the responses will indicate what level of risk (if any) the proposed change/project will have on Data Protection. Use the table below to assess the severity of the risk, include a reason for the risk level and complete the DPIA declaration. The SRO must sign off the DPIA once completed.

Please refer to the table provided on the next page to complete the below.

Severity of Risk	**6**	**Reason**	**There is personal data held, which if intercepted includes identifiable information, use of hearing aids and (if the user opts to use this) GPS data. This would therefore potentially cause moderate harm. However, the data transmission is encrypted, and the data centre meets relevant ISO standards, so the likelihood of this taking place is low.**

DATA PROTECTION IMPACT ASSESSMENT TOOL

Likelihood		Impact				
		Insignificant Patients Minimal impact on patients. Staff Minimal impact on staff. Trust Day-to-day operational challenges.	**Minor** Patients Minor injury or harm to patient(s) requiring minimal to clinical intervention. Staff Temporary staffing issues resulting in increased pressure on staff and challenges in maintaining service quality. Trust Temporary restriction to service delivery with limited impact on stakeholder confidence.	**Moderate** Patients Moderate injury or harm to patient(s) requiring clinical intervention. Staff Short-term staffing issues resulting in low staff morale or restrictions to service quality. Trust Short-term failure to deliver key objectives with temporary term adverse local publicity.	**Severe** Patients Serious or permanent harm to patient(s). Staff Medium-term staffing issues resulting in very low morale or significant reduction in service quality Trust Medium-term failure to deliver key objectives with ongoing adverse publicity or negative impact on stakeholder confidence.	**Catastrophic** Patients Avoidable death of patient(s). Staff Long-term staffing issues resulting in poor morale, staff welfare issues or fundamental reduction in service quality. Trust Continued failure to deliver key objectives with long-term adverse publicity or fundamental loss of stakeholder confidence.
Likelihood	**Almost Never** This probably will never happen/recur.	1	2	3	4	5
	Unlikely Do not expect it to happen/recur, but it may do so.	2	4	6	8	10
	Likely Might happen or recur occasionally.	3	6	9	12	15
	Highly Likely Will probably happen/recur, but is not a persisting issue or circumstance.	4	8	12	16	20
	Almost Certain Very likely to happen/recur; possibly frequently.	5	10	15	20	25

University Hospitals Plymouth NHS Trust

DATA PROTECTION IMPACT ASSESSMENT TOOL

DATA PROTECTION IMPACT ASSESSMENT DECLARATION Identify the relevant statement of the three listed below and complete boxes			
STATEMENT	**YES**	**NAME**	**DATE**
This project/change does not involve information about people or people cannot be identified from the data			
This project/change has had a Data Protection Impact Assessment completed and the severity of the risk is Yellow/Green	**Yes**	**xxxx**	**xxxx**
This project/change has had a Data Protection Impact Assessment completed and the severity of the risk is Amber or Red. This has been placed on the Trust's Risk Register.			

DATA PROTECTION IMPACT ASSESSMENT SIGN OFF		
SIGN OFF	**DATE**	**PRINT NAME**
Senior Responsible Owner (SRO)		

DATA PROTECTION IMPACT ASSESSMENT TOOL

Section 4 (to be completed by the Information Governance Team)		
1. Any projects that do not involve information about people will be signed off by a member of the Information Governance Team. **2. The Information Governance Team and Information Security will be notified of all Data Protection Impact Assessments on projects/changes that involve information about people. Both will need to approve the privacy risk.** **3. Any project/change that represents a significant risk to privacy will be escalated to the Senior Information Risk Owner via the Caldicott and Information Governance Assurance Committee.**		
DATA PROTECTION IMPACT ASSESSMENT REVIEW		
REVIEW	**DATE**	**DECISION**
Information Governance Team (no information about people)		
REVIEW	**DATE**	**DECISION**
Information Governance Team		

DATA PROTECTION IMPACT ASSESSMENT TOOL

Information Security		
FOR INFORMATION	**DATE**	**DECISION**
Caldicott and Information Governance Assurance Committee		