



Data Protection Impact Assessment for GP Practice Use

| | |
|-------------------------------------------|-------------------------------------------------------------------------------------|
| DPIA Title: | Heidi Health – Scribe Artificial Intelligence tool DPIA for Highfield Surgery |
| Data Protection Officer consulted (date): | 21/02/2024 |
| Data Protection Officer comments: | None |
| Data Protection Officer signature: | C. Mountford |
| Caldicott Guardian consulted (date): | 14 th April 2025 |
| Caldicott Guardian comments: | None |
| Caldicott Guardian signature: |  |
| SIRO approval (date): | 14 th April 2025 |
| SIRO comments: | None |
| SIRO signature: |  |

Commented [OB1]: GP Practice to ensure Caldicott Guardian and SIRO are consulted on this DPIA before signing off

| What is the process under consideration? | Guidance |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <p>Heidi is a healthcare IT system, specifically a cloud-based artificial intelligence medical scribe platform. It is a standalone software that is used to generate comprehensive clinical documentation using a combination of speech-to-text software, note taking and artificial intelligence models. Heidi is accessible via desktop and mobile browser to registered users, with servers and data hosted locally in the UK for all UK users.</p> <p>Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impression and/or management plans before, during and after the healthcare encounter. The clinician can also:</p> <ul style="list-style-type: none"> • Add additional contextual notes about the healthcare encounter which they may not wish to verbalise during the healthcare encounter. • Able to set and modify various settings within the Heidi platform in order to customise their Heidi experience as well as how their clinical documentation is structured and written. • Generate clinical documents, such as referral letters and patient explainer documents. These documents will follow templates already defined by Heidi, or the clinician can create their own template. <p>To generate the requested clinical documentation, the transcribed text and contextual notes along with the various user controlled settings are then through an artificial intelligence model which then generates the requested clinical documentation based on the data that has been given to the AI model.</p> <p>The comprehensive clinical documentation generated by Heidi can then be copied or integrated into an electronic medical record system or used with other word processing or communication tools to provide other clinicians and/or the patient with relevant information related to the healthcare encounter and the patient's care.</p> <p>The intended use and recommendations for Heidi are as follows:</p> <ul style="list-style-type: none"> • Heidi should be used by qualified and registered clinicians to assist them in writing their clinical documentation. • Heidi should not be used as a clinical decision making tool and is not a substitute for medical assessment. • Heidi's generated clinical documentation is intended to reduce the amount of time it takes clinicians to complete their medical records; however the clinician is ultimately responsible for their clinical documentation, and must ensure that the content of the notes and documents accurately reflects the healthcare encounter for which the documentation has been generated. | <p>Present a brief outline of the processing/scheme/project – i.e. the name of the project, reason for sharing data, etc</p> |

| | |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | |
| Will the process necessitate the use/processing/collection/sharing of any personal or pseudonymised data? | |
| Yes - Heidi operates within the context of medical consultations, capturing and processing information in the healthcare setting. | <p>Personal data - Any information relating to an identified living person ('data subject') by way of an identifier such as a name, address, date of birth, NHS Number.</p> <p>Pseudonymised data - Personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, i.e. local identifier which would then be reidentified if needed.</p> |

| What are the responsibilities linked to the processing? (i.e. who is the data controller, any possible data processors and joint data controllers) | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-------------------|---------------------------|------------|--------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-----|----------------|------------------------|---------------------------------------------------------------|-------|--------------|---------------------|-----------------------------------------------------|--------|----------------|--------------------|-------------------------------------------------------|----------|--------------|------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><GP Practice name> – Data Controller</div> <div>Heidi Health – Data Processor</div> <div>Sub Processors of Heidi:</div> <table><thead><tr><th>SUB-PROCESSOR</th><th>LOCATION</th><th>PURPOSE/ SERVICES</th><th>WEBSITE & CONTACT DETAILS</th></tr></thead><tbody><tr><td>Google LLC</td><td>EU (Ireland)</td><td>Google Workspace:<ul style="list-style-type: none">Employee emailGoogle DriveGoogle Meets</td><td>https://workspace.google.com/</td></tr><tr><td>AWS</td><td>United Kingdom</td><td>Cloud hosting provider</td><td>https://aws.amazon.com/</td></tr><tr><td>Kinde</td><td>EU (Ireland)</td><td>User authentication</td><td>https://kinde.com/</td></tr><tr><td>Stripe</td><td>United Kingdom</td><td>Payment Processing</td><td>https://stripe.com/</td></tr><tr><td>Intercom</td><td>EU (Ireland)</td><td>Customer Support</td><td>https://intercom.com</td></tr></tbody></table> <div>*Although Servers are in EU, there is an adequacy decision between UK and EU allowing data to be protected.</div> <div>**Stripe manages Heidi payment infrastructure for users i.e. clinics/PCN/specialists etc. They at no time have access to any patient information.</div> | | SUB-PROCESSOR | LOCATION | PURPOSE/ SERVICES | WEBSITE & CONTACT DETAILS | Google LLC | EU (Ireland) | Google Workspace: <ul style="list-style-type: none">Employee emailGoogle DriveGoogle Meets | https://workspace.google.com/ | AWS | United Kingdom | Cloud hosting provider | https://aws.amazon.com/ | Kinde | EU (Ireland) | User authentication | https://kinde.com/ | Stripe | United Kingdom | Payment Processing | https://stripe.com/ | Intercom | EU (Ireland) | Customer Support | https://intercom.com | <div>Definition: Data Controller - Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.</div> <div>Definition: Data Processor - Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.</div> |
| SUB-PROCESSOR | LOCATION | PURPOSE/ SERVICES | WEBSITE & CONTACT DETAILS | | | | | | | | | | | | | | | | | | | | | | | |
| Google LLC | EU (Ireland) | Google Workspace: <ul style="list-style-type: none">Employee emailGoogle DriveGoogle Meets | https://workspace.google.com/ | | | | | | | | | | | | | | | | | | | | | | | |
| AWS | United Kingdom | Cloud hosting provider | https://aws.amazon.com/ | | | | | | | | | | | | | | | | | | | | | | | |
| Kinde | EU (Ireland) | User authentication | https://kinde.com/ | | | | | | | | | | | | | | | | | | | | | | | |
| Stripe | United Kingdom | Payment Processing | https://stripe.com/ | | | | | | | | | | | | | | | | | | | | | | | |
| Intercom | EU (Ireland) | Customer Support | https://intercom.com | | | | | | | | | | | | | | | | | | | | | | | |
| What governance measures are in place to oversee the confidentiality, security and appropriate use of the data? | | Governance measures may include compliance with the Data Security and Protection Toolkit, having IG, data security and data breach policies and procedures in place, 95% minimum staff compliance with IG training. | | | | | | | | | | | | | | | | | | | | | | | | |
| <div><GP Practice name></div> <div><ul style="list-style-type: none"><GP Practice ICO registration><GP Practice DSPT status></div> | | | | | | | | | | | | | | | | | | | | | | | | | | |

Commented [OB2]: GP practice to update name

- The GP Practice has a set of IG policies and procedures approved which detail and stipulate IG responsibilities for all staff to adhere to, including a data breach policy and procedure. Staff are required as part of DSPT, to undertake Information Governance Training on an annual basis.

Heidi Health

- ICO registered ZB671518 - <https://ico.org.uk/ESDWebPages/Entry/ZB671518>
- DSPT compliant 23/24 Standards Met - <https://www.dsptoolkit.nhs.uk/OrganisationSearch/HHA001>
- Cyber Essentials Certificate *Due to expire April 2025 however is due for renewal.
<https://registry.blockmarktech.com/certificates/0fd4036c-35bd-4493-b704-95adc158e165/>



6. Heidi Health
Trading Ltd.pdf

- Information Security Management System – ISO/IEC 27001:2022 * Assurance received whilst registered with Heidi parent company, Heidi ISO27001 certification covers the entire information management system and processes including UK operations.
- Undertake penetration testing
- custom code developed for Heidi undergoes a thorough security review process as part of our commitment to maintaining high standards of cybersecurity and data protection. This internal review process is aligned with the principles outlined by the National Cyber Security Centre (NCSC), focusing on producing clean, maintainable code that minimizes security risks. Our development team adheres to best practices in secure coding, and each update or addition to our system's codebase is scrutinized for vulnerabilities and compliance with established security guidelines before being deployed.



Heidi DTAC Version
1.2 (14.12).pdf

- DTAC completed
- Privileged accounts have Multi-Factor Authentication (MFA) enabled
- Heidi has undergone comprehensive load testing to ensure it can handle the expected volume of users and data processing demands without compromising performance or reliability. This testing simulates real-world usage scenarios at peak load and beyond, to guarantee stability and responsiveness of our product under various conditions.

Note that “All organisations that have access to NHS patient information must provide assurances that they are practising good information governance and use the Data Security and Protection Toolkit to evidence this by the publication of annual assessments”
(<https://www.dsptoolkit.nhs.uk/Help/Attachment/5>)

- DCB0129 docs including the compliance assessment, clinical safety case report & hazard log



DCB0129 compliance
assessment.pdf



Heidi Health NHS
Hazard Log v1.3 19_0



Heidi Clinical Safety
Case Report 1.3 (7).pc

- Example DCB0160 clinical safety case report & hazard log



AI Scribe Hazard Log
Template - Draft v1.0:safety case report.pdf



DCB0160 clinical
Case Report 1.3 (7).pc



DPIA National
Template (Example).d



Installation of Heidi -
NHS DPIA Proforma.d

- Heidi undertaken their own DPIA documentation

No live recording is obtained, as the patient is talking the transcript is written. Heidi only holds the transcript which is de-identified. No identifiable recordings are stored or will be accessible to Heidi. Clinicians retain ownership of all transcripts, clinical notes, and clinical documents and can decide how long this data is stored. Additionally, the patient information contained in these transcripts and clinical notes/documents will only be accessed externally for the purpose of troubleshooting with the express permission of clinicians.

Heidi privacy policy details they safeguard personal information and ensure data security -

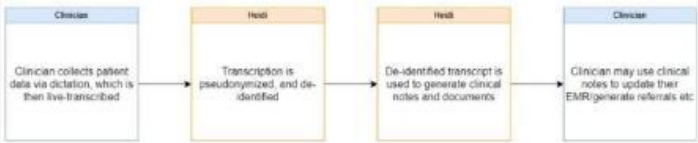
<https://www.heidihealth.com/uk/legal/ukgdp-compliance-policy>



17. ICO AI Toolkit_
Heidi Health 12 Sep.xl

Heidi have completed an ICO AI risk toolkit -

DATA, PROCESSES AND SUPPORTING ASSETS

| What is the data processed? | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The following patient data items may be recorded and transcribed by Heidi:</p> <ul style="list-style-type: none"> • Full name – forename, surname • Full address including postcode • Gender • Age • Contact details including telephone number, email address • GP details • Physical description • Sexual orientation • Date of birth • Relationship status • Family and social history • Medical history including physical and mental health • Progress notes • Medications & prescriptions • Allergies • Diagnosis status • Lab orders & results • Disability | <p>List the data collected and processed, i.e. name, address, date of birth etc.</p> |
| How does the life cycle of data and processes work? | |
| <p>Personal Information Flow Diagram</p>  <pre> graph LR A[Clinician] --> B[Heidi] B --> C[Heidi] C --> D[Clinician] A["Clinician collects patient data via dictation, which is then live-transcribed"] --> B["Transcription is pseudonymized, and de-identified"] B --> C["De-identified transcript is used to generate clinical notes and documents"] C --> D["Clinician may use clinical notes to update their EMR/generate referrals etc"] </pre> | <p>Present and describe how the product generally works (from the data collection to the data destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.</p> |

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | |
| What are the data supporting assets? | |
| <p>GP Clinical staff – utilising Heidi software to dictate and transcribe consultation</p> <p>Heidi software – creates a transcript of the consultation (No patient identifiable data stored)</p> <p>Amazon Web Server – cloud hosting provider. Hosted in the UK for UK users. (No patient identifiable data stored)</p> | <p>List the data supporting assets (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.)</p> |

Fundamental principles

PROPORTIONALITY AND NECESSITY

| | |
|-----------------------------------------------------------------|--|
| Are the processing purposes specified, explicit and legitimate? | |
|-----------------------------------------------------------------|--|

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Personal data will be processed by Heidi for the purpose of transcribing clinical appointments. Heidi will only be in use when the dictation session is started by the GP Practice clinician following agreement from the patient. | Explain why the processing purposes are specified, explicit and legitimate. How is the legal basis being specified? |
| What is the lawful basis for processing the data? | |
| <p>To support data processing for NHS services, using legal powers provided by:</p> <ul style="list-style-type: none"> • The National Health Service and Community Care Act 1990 • The NHS Act 2006 • The Health and Social Care Act 2012 <p>To process personal and special category data in accordance with UK GDPR:</p> <ul style="list-style-type: none"> • Art. 6(1)(e) – Public task • Art. 9(2)(h) – healthcare purposes <p>To process personal data in line with the Data Protection Act 2018:</p> <ul style="list-style-type: none"> • Condition 2 of Schedule 1 – Health and Social Care Purposes. <p>***Explicit consent is obtained from the data subject prior to consultation meaning that the individual knows or would reasonably expect the proposed use of disclosure and has not objected. The GP will confirm with the patient prior to starting the dictation process.</p> | <p>What is the legal basis for processing the data? – direct care, legislation or consent, (don't forget, consent should be a last resort and only used if there is no direct care or legislation in place). Remember to identify which Article 6 or 9 conditions will be used and if there is supporting legislation, what that legislation is, including the specific section of the legislation which supports the use of data for this purpose.</p> |
| Is the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')? | |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>No personal data will be processed that isn't necessary. The data will only be used by qualified and registered clinicians to assist them in writing their clinical documentation.</p> | <p>Need confirmation in here that there is no personal data being processed that isn't absolutely necessary for the purpose of the project. Is any information being collected that isn't required to complete the project?</p> |
| <p>Is the data accurate and kept up to date?</p> | |
| <p>Heidi has employed a stringent validation process involving rigorous quality assurance processes on all outputs, including clinical validation by internal healthcare professionals with clinical backgrounds and experience, technical accuracy assessments, and real-world testing to ensure Heidi meets the high standards. Heidi also implement continuous monitoring and updates post-deployment to guarantee our model remains as accurate and bias free as possible.</p> <p>Additionally, to ensure the clinician is always kept in the loop, Heidi use in-product reminders for clinicians to check all outputs for completeness, relevance, and accuracy.</p> <p>It is the responsibility of the GP practice to ensure the data recorded by Heidi is accurate and reflects the discussion with the patient.</p> <p>Heidi is noted to have the following limitations that users must be aware of:</p> <ul style="list-style-type: none"> • Heidi's generated clinical documentation is based on the clarity and quality of the speech & text data that is provided in the healthcare encounter. Users must review all clinical documentation generated to confirm their accuracy before capturing it in their electronic medical records or distributing documentation to other clinicians and/or patients. • Hardware issues such as poor microphone quality may cause sub-par audio being captured, resulting in an inaccurate text transcript which does not adequately reflect the healthcare encounter information. Users are recommended to test the quality of their microphones prior to and while using Heidi. • An unstable or slow internet connection may result in delays in information processing and potentially not capturing some or all of the healthcare encounter information. Therefore it is vital that users ensure they have a stable and fast internet connection when using Heidi. • Heidi's AI models occasionally make mistakes which may not accurately reflect the information discussed in the healthcare encounter. Users must ensure they have reviewed all clinical documentation generated by Heidi to confirm their accuracy before importing it in their electronic medical records or distributing documentation to other clinicians and/or patients. | <p>Describe what steps are taken to ensure the quality of the data. Need confirmation here of who will check the data is accurate and what process is in place to ensure the data is kept up to date.</p> |

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | |
| What is the storage duration of the data? | |
| <p>Identifiable data will be held in the patients clinical record within GP Practice systems. Data is held in line with Records Management Code of Practice for Health and Social Care.</p> <ul style="list-style-type: none"> • Adult Health and Social Care records - 8 years • Children's records - up to 25th birthday <p>No identifiable recordings are stored or will be accessible. Clinicians retain ownership of all transcripts, clinical notes, and clinical documents and can decide how long this data is stored.</p> <p>The information contained in transcripts and clinical notes/documents will only be accessed externally for the purpose of troubleshooting with the express permission of the GP practice. Information will be held by Heidi for the duration of the agreement and deleted within 10 business days of termination of the agreement.</p> | <p>Ideally there will be a list here of all the data assets being processed, how long they will be held for, where the timescales have come from (i.e., Information Governance Alliance code of practice for records management). This should be stated for each organisation that holds the data.</p> <p>Records Management Code of Practice for Health and Social Care 2021:</p> <p>https://www.nhs.uk/healthcare-professionals/information-governance/guidance/records-management-code/</p> |

CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How are the data subjects informed of the processing? | |
| <p>Explicit consent is obtained from the data subject prior to consultation meaning that the individual knows or would reasonably expect the proposed use of disclosure and has not objected. The GP will confirm with the patient prior to starting the dictation process and explain how Heidi works.</p> | <p>In here you would expect that privacy notices are made available to the data subjects and information and advice, perhaps even leaflets, about how data subjects can access privacy notices.</p> |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | |
| If consent is your lawful basis how is the consent of data subjects obtained? | |
| N/A – Consent is not the lawful basis. | If consent is not your legal basis, then this should say not applicable. If consent is the legal basis, then this should advise how the consent is obtained, what information is given to the data subject when obtaining consent about what data will be used and for what purpose, how the consent is recorded and what information is given to the data subject about how they can withdraw their consent. |
| How can data subjects exercise their rights of access and to data portability? | |
| The right of access and data portability will be managed by the patient's own GP Practice as they hold all the records. Therefore, existing practice mechanisms are in place. | Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests |
| How can data subjects exercise their rights to rectification and erasure? | |
| The right of rectification and erasure will be managed by the patient's own GP Practice as they hold all the records. Therefore, existing practice mechanisms are in place. | Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests |
| How can data subjects exercise their rights to restriction and to object? | |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The right to restriction and object will be managed by the patient's own GP Practice as they hold all the records. Therefore, existing practice mechanisms are in place.</p> <p>Prior to consultation the individual knows or would reasonably expect the proposed use of disclosure and has not objected. The GP will explain the use of Heidi and its purpose and will obtain explicit consent from the patient prior to starting the dictation process.</p> | <p>Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests</p> |
| <p>How can data subjects exercise their rights to auto-mated decision making and profiling?</p> | |
| <p>This right does not apply. There is no automated decision making, the dictation-scribe requires checking by the clinician before it can be uploaded to the patient record.</p> | <p>Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests</p> |
| <p>If there is a Data Processor involved, are the obligations of the processors clearly identified and governed by a contract?</p> | |
| <div data-bbox="147 865 192 906"></div> <p>Heidi Data Processing Agreement</p> <p>Draft Processing agreement between GP Practices and Heidi. <input type="text"/></p> | <p>If a data processor is involved, this should fully explain who the processor is and what their role is in relation to the processing. Need confirmation that there is a data processing agreement and/or contract in place between the data controller and the data processor which stipulates what the data processor will be doing with the data.</p> <p>If there is no data processor, then consideration should be made to a data sharing agreement being put in place.</p> |
| <p>In the case of data transfer outside the United Kingdom, are the data adequately protected?</p> | |

Commented [OB3]: GP Practice to sign agreement.

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No data is shared outside of the UK. Storage is on servers located within the EU. There is an adequacy decision between UK and EU allowing data to be protected. | This should confirm if any data is being transferred outside of the UK, this includes where servers, for systems being used, are based. If data is being transferred outside of the UK, then strict assurances need to be in place that where the data is being transferred to will meet GDPR compliance and a contract in place. |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Risks

This section allows you to assess the privacy risks, taking into account existing or planned controls.

Risk Factors to consider:

- Illegitimate access to data;
- Unwanted modification of data
- Data disappearance

PLANNED OR EXISTING MEASURES

See appendix A for information on working out Risk Likelihood and Severity

| # | Risk Ref | Risk Description | Mitigating Control(s)/Actions | Likely | Severity | Score |
|---|----------|------------------|-------------------------------|--------|----------|-------|
|---|----------|------------------|-------------------------------|--------|----------|-------|

| | | | (See details below) | (See details below) | | |
|---|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---|----------------|
| 1 | Process | If GPs are on a shared network, they need to consult with the other Practices to ensure they are happy for this to be rolled out onto their shared area. | Heidi is not connected to GP systems and doesn't need to be integrated to clinical systems therefore shouldn't affect other GP within the same network. | 0 | 0 | 0 - Eliminated |
| 2 | GDPR | EU AI Act prohibiting AI within practices. | <p>Heidi are:</p> <p>Keeping Heidi firmly in the low-risk category and avoiding any functionalities that could fall under prohibited AI practices. In addition Heide will continue having in-house medical knowledge team perform ongoing data and model validation tests and any conformance testing that might be required depending on classification (currently looks like it will be a limited or minimal risk system).</p> <p>Heidi have started pursuing ISO 42001 certification which is the newly created assurance framework for AI systems which are hoping to obtain by mid 2025.</p> <p>Heidi will remain aware of any legislative or regulatory developments in the EU and the UK.</p> | 1 | 1 | 2 - Low |
| 3 | Process | GP systems and data are breached by unauthorised persons or becomes unavailable | <p>GP practice to refer to data breach procedures in the event of data breach.</p> <p>Access controls are in place to prevent data breaches.</p> <p>Regular policy and Information Governance training is required by all staff, on an annual basis.</p> | 1 | 1 | 2 - Low |

| | | | | | | |
|---|------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---------|
| 4 | Process | Loss of Heidi AI software / System is unavailable during critical times | GP Practice to revert to previous procedures in manually taking notes of clinical appointment. | 1 | 1 | 2 - Low |
| 5 | GDPR | GP data are breached in transit due to improper encryption | <p>Patient data is de-identified prior to reaching Heidi systems. No patient identifiable data is within Heidi systems.</p> <p>Heidi employs stringent privacy and security measures, including end-to-end and at rest encryption. All privacy data is encrypted in transit using TLS 1.2 or higher and at rest with AES-256.</p> | 1 | 1 | 2 - Low |
| 6 | Process | Data Quality issues | <p>Heidi has employed a stringent validation process involving rigorous quality assurance processes on all outputs, including clinical validation by internal healthcare professionals with clinical backgrounds and experience, technical accuracy assessments, and real-world testing to ensure Heidi meets the high standards. Heidi also implement continuous monitoring and updates post-deployment to guarantee our model remains as accurate and bias free as possible.</p> <p>Heidi use in-product reminders for clinicians to check all outputs for completeness, relevance, and accuracy.</p> <p>It is the responsibility of the GP practice to ensure the data recorded by Heidi is accurate and reflects the discussion with the patient.</p> | 1 | 1 | 2 – Low |
| 7 | Governance | Records management risk as the vendor does not keep a copy of the patient consultation and | GP Practice/Clinician responsibility to ensure a copy of the transcription is uploaded into the EPR. | 1 | 1 | 2 – Low |

| | | | | | | |
|----|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|----------------|
| | | Heidi deletes it once the practice manager approves the translation prior to upload to EPR. Challenges if details recorded in the EPR system are questioned by the patient as the original file would not be available – i.e. personal injury claims, coroner court enquiries etc. | GP Practice to consider emailing a copy of the transcribed consultation or requesting the patient to verify before being uploaded to the EPR. | | | |
| 8 | GDPR | Function creep over how personal data is processed is caused by not defining what purpose you will use your AI system. As a consequence, individuals lose control over how their data is being used. | Heidi data flow diagrams are used to demonstrate our track of data usage across the system, including the AI system usage. We have clearly identified the purpose specification in AI system design documentation. In our publicly available UKGDPR Privacy Policy (https://www.heidihealth.com/legal/ukgdpr-compliance-policy) we outline the purposes of processing personal data. | 1 | 1 | 2 – Low |
| 9 | Supplier | AI systems producing unfair outcomes for individuals are caused by insufficiently diverse training data, training data inappropriate for the purpose of the AI system, training data that reflects past discrimination, design architecture choices or another reason. As a consequence, individuals suffer from unjustified adverse impacts such as discrimination, financial loss or other significant economic or social disadvantages. | Decision making is not automated. Heidi doesn't provide clinical decision making support, but rather provides a recreation of the consult. Users of Heidi have full visibility of all outputs, and have the ability to interrogate all outputs, and make changes as you see fit. Because of this a risk assessment for this statement is not required. | 0 | 0 | 0 – Eliminated |
| 10 | GDPR | The lack of transparency, interpretability and/or explainability is caused by choices about how an AI system is designed and developed. As a consequence, individuals lack the understanding about how their data is being used, how the AI system affects them, and how to exercise their individual rights. | Heidi have a publicly available UKGDPR Privacy policy that outlines individuals rights in regards to their personal data. This policy also outlines how data access, change, and deletion request are made (https://www.heidihealth.com/legal/ukgdpr-compliance-policy), as well as transparent, plain- | 1 | 1 | 2 – Low |

| | | | | | | |
|----|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---------|
| | | | language information on our safety page (https://www.heidihealth.com/safety), our trust center (https://trust.heidihealth.com/), and our UK compliance page (https://www.heidihealth.com/compliance/uk). | | | |
| 11 | Malware | Attack on Heidi system / undetected security vulnerabilities | <p>Heidi has implemented robust authentication and access control mechanisms for the entire system infrastructure. All data at rest or in transit are encrypted.</p> <p>To help identify or detect system vulnerabilities, Heidi provided staff with training including cybersecurity training, educated users on recognising and reporting potential security threats, established regular security audits and penetration testing, and implemented incident response and data breach notification procedures.</p> <p>In addition, Heidi has developed a secure enclave for processing highly sensitive data via de-identification model. We also conduct regular simulated attack exercises, and have implemented a formal process for continuous security assessment and improvement.</p> <p>Security testing frameworks in place within Heidi.</p> | 1 | 1 | 2 – Low |
| 12 | GDPR | The excessive and irrelevant collection of personal data is caused by a default approach to collect as much data as possible to design and build AI systems. As a consequence, individuals suffer from unlawful and unfair processing. | <p>To address this risk, Heidi has implemented data minimisation techniques. In addition, have developed AI models that can perform effectively with minimal data, implemented automated data relevance assessment tools.</p> <p>Heidi conduct regular internal discussion on the collection of personal data, and ways in which to minimise both the processing, and collection of personal data</p> | 1 | 1 | 2 – Low |

| | | | | | | |
|----|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|------------|
| | | | <p>Heidi employ a compliance and security monitoring software called Vanta. This allows for real-time monitoring of employee devices, security awareness training, and policy acceptance. Additionally, Heidi facilitate regular engineering knowledge sharing, to stay on top of best security and software development practices.</p> <p>Both Heidi Medical Knowledge and Engineering teams are comprised of industry experts who are well versed in best practices for data collection.</p> | | | |
| 13 | Supplier | Inappropriate access to training data, training code, and deployment code is caused by lax security policies. As a consequence, individuals may have their personal data subjected to data poisoning attacks leading to unfair advantages or disadvantages. | <p>Heidi apply stringent data security and privacy controls throughout the development, delivery, and support of Heidi. These controls include data encryption, secure coding practices, access control based on the principle of least privilege, and the implementation of privacy by design principles. Regular security audits and compliance checks ensure adherence to industry standards and regulatory requirements.</p> <p>Employee access rights are reviewed quarterly, and logs are maintained for all access and changes.</p> | 1 | 1 | 2 – Low |
| 14 | Supplier | The collection of too much personal data is caused by not applying de-identification techniques. As a consequence, individuals suffer from unlawful and unfair processing. | <p>Heidi employs a de-identification process to all transcripts. It is important to note that Heidi do not use these transcripts for the purpose of model training.</p> <p>Heidi perform regular vendor security reviews and engage in strict data processing agreements with our third-party vendors which enforce zero-retention and no secondary usage policies to protect our users' data.</p> | 2 | 2 | 4 - Medium |

| EXAMPLES of risks - FOR INFORMATION ONLY | |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Education | Breach of IG policies and guidance due to lack of visibility, communication and training |
| GDPR | Non-compliant with GDPR implementation |
| Malware | Threat from malicious links/ attachments |
| Process | Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls |
| Purchasing | Limited governance over low spends allows DPIA process bypass |
| Sharing | Sharing information inappropriately or illegally due to immature technology or understanding of legislation |
| Supplier | Suppliers breach Privacy Law due to poor information handling practices/ IT security |

Appendix A

| | |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption | Means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing. |
| Anonymisation | Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose. Remember to clearly distinguish between anonymous and pseudonymous data. |
| Partitioning | Implementation of data partitioning helps to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur. |
| Logical Access Control | Methods to define and attribute users' profiles. Specify the authentication means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.). |
| Traceability (logging) | Policies that define traceability and log management. |
| Archiving | Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives. |
| Paper document security | Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged. |

| | |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimising the amount of personal data | The following methods could be used: Filtering and removal, reducing sensitivity via conversion, Reducing the identifying nature of data, Reducing data accumulation, Restricting data access |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Physical Security Control

| | |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating security | Policies implemented to reduce the possibility and the impact of risks on assets supporting personal data. |
| Clamping down on malicious software | Controls implemented on workstations and servers to protect them from malicious software while accessing less secure networks. |
| Managing workstations | Controls implemented on workstations (automatic locking, regular updates, configuration, physical security, etc.) to reduce the possibility to exploit software properties (operating systems, business applications etc.) to adversely affect personal data. |
| Website security | Implementation of ANSSI's Recommendations for securing websites. |
| Backups | Policies and means implemented to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality. |
| Maintenance | Policies describing how physical maintenance of hardware is managed, stating whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner. |

| | |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processing Contracts | <p>Regulate the procurement relations via a contract signed intuitu personæ.</p> <ul style="list-style-type: none"> - Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the ICO's recommendations in this respect. - Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data: <ol style="list-style-type: none"> 1) The data to which it will have access or which will be transmitted to it. 2) The operations it must carry out on the data. 3) The duration for which it may store the data. 4) Any recipients to which the data controller requires it to transmit the data. 5) The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's). 6) The security objectives set by the data controller. - Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights. - Explicitly prohibit or regulate use of tier-2 processors. - Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract. |
| Network security | <p>Depending on the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.</p> |
| Physical access control | <p>Policies to ensure physical security (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.</p> |

| | |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitoring network activity | Monitor intrusion detection systems and intrusion prevention systems in order to analyse network (wired networks, Wi-Fi, radio waves, fibre optics, etc.) traffic in real time and detect any suspicious activity suggestive of a cyber-attack scenario. |
| Hardware security | Indicate here the controls bearing on the physical security of servers and workstations (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.). |
| Avoiding sources of risk | Documentation on implantation area, which should not be subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.). Specify if dangerous products are stored in the same area. |
| Protecting against non-human sources of risks | Policies describing the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief. |

Organisational Control

| | |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organisation | Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy. |
| Policy | Set out important aspects relating to data protection within a documentary base making up the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be |

| | |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | applied, etc.) and each communication target (users, IT department, policymakers, etc.). |
| Managing Privacy risks | Policy describing processes to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects (building a map of the risks, etc.) |
| Integrating privacy protection in projects | Existence of a policy designed integrate the protection of personal data in all new processing operations. |
| Managing personal data violations | Existence of an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy. |
| Personnel management | Existence of a policy describing awareness-raising controls are carried out with regard to a new recruit and what controls are carried out when persons who have been accessing data leave their job. |
| Relations with third parties | Existence of a policy and processes reducing the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy. |
| Supervision | Existence of a policy and processes to obtain an organization able to manage and control the protection of personal data held within it. |

Severity Definitions

| Severity | Description |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Negligible severity | Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem. |

| | |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Examples:</p> <ul style="list-style-type: none"> - physical : transient headaches - material : loss of time in repeating formalities or waiting for them to be fulfilled, receipt of unsolicited mail (e.g.: spams), reuse of data published on websites for the purpose of targeted advertising , etc., - moral : mere annoyance, feeling of invasion of privacy without real or objective harm (commercial intrusion), etc. |
| Limited severity | <p>Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties</p> <p>Examples :</p> <ul style="list-style-type: none"> - physical : minor physical ailments (minor illness due to disregard of contraindications), defamation resulting in physical or psychological retaliation, etc. - material : Unanticipated payments (fines imposed erroneously), denial of access to administrative or commercial services , Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects, etc. - moral : minor but objective psychological ailments, feeling of invasion of privacy without irreversible damage, intimidation on social networks, etc. |
| Significant severity | <p>Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties</p> <p>Examples:</p> <ul style="list-style-type: none"> - physical : serious physical ailments causing long-term harm (worsening of health due to improper care, or disregard of contraindications), Iteration of physical integrity for example following an assault, an accident at home, work, etc. - material : misappropriation of money not compensated, targeted, unique and non-recurring, lost opportunities (home loan, refusal of studies, internships or employment, examination ban), loss of housing, loss of employment, etc. - moral : serious psychological ailments (depression, development of a phobia), feeling of invasion of privacy with irreversible damage, victim of blackmailing, cyberbullying and harassment, etc. |

| | |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum severity | <p>Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome</p> <p>Examples :</p> <ul style="list-style-type: none"> - physical : long-term or permanent physical ailments, permanent impairment of physical integrity, death - material : financial risk, substantial debts, inability to work, inability to relocate, loss of evidence in the context of litigation, loss of access to vital infrastructure (water, electricity), etc. - moral : long-term or permanent psychological ailments, criminal penalty, abduction, loss of family ties, inability to sue, change of administrative status and/or loss of legal autonomy (guardianship), etc. |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Severity | Description |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Negligible likelihood | It does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader and access code). |
| Limited likelihood | It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader). |
| Significant likelihood | It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in offices that cannot be accessed without first checking in at the reception). |

| | |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum likelihood | It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in the public lobby). |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Risk Mapping

| In accordance with the Risk Treatment Process | |
|------------------------------------------------------|-------------|
| Score | Risk Class |
| 1 | Negligible |
| 2 | Limited |
| 3 | Significant |
| 4 | Maximum |

| | | Severity | | | |
|------------|-----------------|----------------|---------------|-------------------|-------------------|
| | | Negligible (1) | Limited (2) | Significant (3) | Maximum (4) |
| Likelihood | Maximum (4) | Medium (4) | High (8) | Very High (12) | Very High (16) |
| | Significant (3) | Medium (3) | High (6) | High (9) | Very High (12) |
| | Limited (2) | Low (2) | Medium (4) | High (6) | High (8) |
| | Negligible (1) | Low (1) | Low (2) | Medium (3) | Medium (4) |