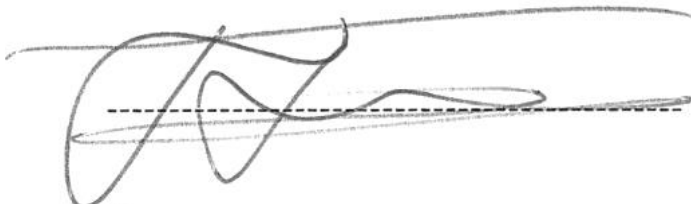


Annex F NGS Data Protection Policy 2020

NGS Data Privacy Impact Assessment (DPIA) Medical and Non-Medical

<p>Privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of processing personal data.</p> <p>The purpose of the PIA is to ensure that privacy risks are minimised while allowing us to achieve our aims and discharge our contractual liabilities. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.</p>		
Assessor's name	Assessor's Appointment	Assessment date
O'H	Operations Director	
NGS Data Protection Officer's name		
Pete Bassill		
Name of process		
Core Business Case Management (Medical and Non-Medical)		
Purpose of processing		
As the contracted Emergency Response Company, NGS has been retained to step in at the request of the client and provide additional resources, crisis management and/or Emergency Response in the event of a crisis or emergency.		
Legal basis for processing the information -		Tick all that apply
Consent		<input type="checkbox"/>
Contract - you need to process someone's personal data to fulfil your contractual obligations to them; or because they have asked you to do something before entering into a contract (e.g. provide a quote).		<input type="checkbox"/>
Legal Obligation - you need to process the personal data to comply with a common law or statutory obligation. You must be able to identify the legal obligation.		<input type="checkbox"/>
Vital Interests - if you need to process the personal data to protect someone's life. You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.		<input type="checkbox"/>
Legitimate Interests - the most "flexible" lawful basis for processing data. There is a three- part test: a. identify a legitimate interest; b. show that the processing is necessary to achieve it; and c. balance it against the individual's interests, rights and freedoms. If you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing, then this basis works. Keep a record of all Legitimate Interests Assessments (LIAs).		<input type="checkbox"/>
Criminal Offence Data - to process personal data about criminal convictions or offences, you need to show one of the five bases above and either legal authority or official authority for the processing of such data.		<input type="checkbox"/>

Retention period
Seven Years to comply with contracted FCA Regulations
Source of the data (if not collected from the data subject)
<ul style="list-style-type: none"> • Client Representative (Manager/HR/Colleague/Insurance Broker/Next of Kin/GP) • Client Contract • Insurance Policy • Medical Facility
In which locations does the processing take place
<ul style="list-style-type: none"> • NGS Ops London • Client Head Office/Regional Office • Service Provider EU • Service Provider outside the EU • Compliant backup data centres in the EU and NA1
Who is impacted by the processing
Data Subject
Any regulated automated decisions taken
No
Process workflow
<ul style="list-style-type: none"> • Data Collection <ul style="list-style-type: none"> • Initial tasking detail • Situation interrogation • Additional information gathers • Consent for medical in confidence • Hardcopy communications portals (post/fax) will be sanitised as soon as required data is transferred to Salesforce casefile. • Storage <ul style="list-style-type: none"> • Calls – VOIP Server – Salesforce casefile and/or account record – Secondary back up servers • Emails – Mail Server – Salesforce casefile, account and contact record - Secondary back up servers • Documents and Reports - Mail Server, Salesforce casefile, account and contact record - Secondary back up servers • Case financials - Mail Server, Xero, Salesforce casefile, account and contact record, Word pay - Secondary back up servers – Hard copy records • Usage <ul style="list-style-type: none"> • Client verification • Situation validation • Resolution options to pre-identified service providers • Client management • Internal/External audit • Accountancy functions, billing and paying • Deletion <ul style="list-style-type: none"> • Full erasure on verified request • Full erasure in accordance with contractual obligations • Full erasure in accordance with legal obligations

What risks are there to the data subject
<ul style="list-style-type: none"> • Inadequate controls increase the likelihood of information being shared inappropriately • Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk • Accuracy of data subject information can pose a physical risk if out of date, incorrect or incomplete • Third Countries outside of the EU may not be compliant with GDPR and sharing information to providers outside the EU may not provide appropriate safeguards for the protection of personal information
Data Subject Access Procedure
<p>Data Subject Access Request forms (DSAR) can be downloaded from our website: www.northcottglobalsolutions.com - *Verbal requests are not valid.</p> <p>Completed forms should be emailed to: dataprotection@northcottglobalsolutions.com</p> <p>Posted to: Data Protection Officer, Northcott Global Solutions, 22 Bevis Marks, London, EC3A 7JB</p> <p>Faxed to: +44 (0)207 183 8919</p> <p>On receipt of completed DSAR form, NGS's Data Protection Officer will verify the request in line with DPA 2018 regulations and action in adherence to regulations and internal policies.</p>
What measures are currently in place to protect the data subject and their rights
<ul style="list-style-type: none"> • Data Protection Policy and Processes are all compliant with ISO27001 • NGS is fully compliant with GDPR Regulations • Service Providers within the EU will also be GDPR compliant. • No automated profiling will be used in the processing of any personal data. • Personal information will only be used for the purpose it was gained and human intervention is the only way NGS will process personal data. • Primary justification falls under the Legitimate Interests of the Data Subject. • Sensitive Information will be processed by Consent. • Contractual Obligations (duty of care liabilities) justify the processing of personal data
What additional measures need to be put in place to ensure all risks are covered
<ul style="list-style-type: none"> • When and wherever possible NGS will attempt to use service providers who comply with GDPR, Regional or Constitutional Data Protection for emergency situations outside the EU. • Vital Interests will be explored and confirmed where the Data Subject's life is at risk and they are unable or incapable of giving consent
Date of next review
<p>Date: 4th March 2020</p> <p style="text-align: center;">EDWARD NORTHCOTT JONES</p>  <p>Signature: _____ CEO</p>