




Risk Assessment

CRA01 Information/Data Security

 CRYSTAL Health Group	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	

The following risk assessment is specifically for Crystal Health Group's Information Security and associated activities for all testing and Medical Assessment services.


How was the risk assessment done?

The assessor followed the advice at www.hse.gov.uk. To identify the risks, they:


- reviewed ISO 27001 Information Management System, including the Statement of Applicability;
- talked to staff and contractors to learn from their experience and listen to their concerns;
- talked to key clients to learn from their experience and listen to their concerns;
- reviewed previous non-conformance and audit reports to understand risks that have been previously identified.

They noted what was already being done to control the risks and recorded any further actions required. This includes a review of the Information Security Objectives for 2024.


Review Times for Risk Assessment	
Immediately	Before using a new process/activity Following a major change in process Following an incident/accident
1 Year	For established processes/activities that have not been changed in any way and there have been with no incidents/accidents.

 CRYSTAL Health Group	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	


WHAT IS THE RISK?	WHO/WHAT MIGHT BE AT RISK AND HOW?	EXISTING MEASURES TO CONTROL RISKS	FURTHER ACTIONS REQUIRED TO CONTROL RISKS FROM REVIEW	ACTION BY	STATUS
Hard copy information left unattended (at head office and on-site).	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> See Client Privacy and Information Security Policy. Refer to risk assessment CRA02 Sample Collection Activities. Employee Awareness training provided with regards to Information Security. Annual information security refresher training with quiz assessment. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Major business disruption due to Office Break in / Fire / Flood etc.	<ul style="list-style-type: none"> Loss of data Equipment failure/ destruction 	<ul style="list-style-type: none"> See 'Business Continuity Plan' Policy for details on actions and responses to disaster recovery situations. Specific company policies in place to mitigate the risk of catastrophic events. Annual training and awareness in place of the BCP and relevant policies for all internal staff. Business Continuity Plan now includes annual testing and results. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Visitors to head office	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. Risk of theft of data. 	<ul style="list-style-type: none"> See 'Staff Building Security' Policy. All visitors are accompanied at all times and follow the signing in procedure. Regular reminders at daily operations meetings and team brief regarding the importance of buildings security. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Documentation sent to incorrect postal address.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> Only addresses supplied on the original test booking form will be used. Refer to 'Case Security' in the Client Privacy Policy. Full training given to Clinical Advisors in SOP's and Policies. Cross check between report, test booking form and post code finder. No children under 16 are entitled to copies of test results. DNA results are now standardly sent by email and not post. Regular GDPR and information security briefings provided to all internal staff. Client contact forms in place to ensure correct client data is obtained. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Client password breach on test case.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> See 'Information Security' Policy. Information included on collection and consent and appointment documentation to advise clients on the importance of keeping case passwords safe. Unique client passwords in place sent by SMS rather than email. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Network/PC password breach	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> See 'Information Security' Policy. All staff aware of the password policy. Network passwords are controlled and allocated by the ICT Manager internally. All passwords held on central and secure asset list to ensure compliance with password creation policy. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete

	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	

WHAT IS THE RISK?	WHO/WHAT MIGHT BE AT RISK AND HOW?	EXISTING MEASURES TO CONTROL RISKS	FURTHER ACTIONS REQUIRED TO CONTROL RISKS FROM REVIEW	ACTION BY	STATUS
Information sent to incorrect email address.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> Only email addresses supplied on the original test booking form will be used. Refer to 'Case Security' in the Client Privacy Policy. Password security in place for all email containing personal data. SMS text password messaging in place to minimise risk of data breach. Full training given to Clinical Advisors in SOP's and Policies. Regular communication and awareness briefings for all internal staff stressing the importance of information security and compliance with GDPR. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Password breach for business applications.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> See 'Information Security' Policy and Business Continuity Plan. All internal staff given Information Security briefing on induction and at regular periods thereafter. This includes best practice for password generation and security. Client contact forms now in place to improve data accuracy. 	1. Implement multi-factor authentication (MFA) across applicable systems.	1. Amy Hindhaugh	1. Ongoing
Internal sensitive data disposal (hardcopy).	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> See 'Staff Building Security' Policy. See 'Environmental Management Systems' Manual. All internal hard copy data not required for external archiving is stored and destroyed (shredded) on site. Refer to Archive Policy for retention periods and methods of disposal. Internal staff awareness briefings delivered on a regular basis at daily operations and monthly meetings. Shredding procedure and waste contract in place. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
External sensitive data disposal (hardcopy).	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> Off-site storage data is disposed of through an approved thirty party provider. Refer to approved supplier SLA. Refer to Archive Policy for retention periods and methods of disposal. Regular GDPR and information security briefings provided to all internal staff. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Incorrect test report information to client.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> Only addresses supplied on the original test booking form will be used. Full training given to all internal staff in SOP's and Policies. Cross check between report, test booking form and post code finder. Test reporting is performed one case at a time on a designated workstation by a designated administrator. Client contact forms now in place. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Third party consent failure.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> All staff trained in SOP's regarding Third Party Consent. Refer to process flow in Client Privacy Policy for procedure. When required, third party consent must be in place for all private client testing, regardless of whether the test has been ordered or paid for by Social Services or a Solicitor. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete


	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	

WHAT IS THE RISK?	WHO/WHAT MIGHT BE AT RISK AND HOW?	EXISTING MEASURES TO CONTROL RISKS	FURTHER ACTIONS REQUIRED TO CONTROL RISKS FROM REVIEW	ACTION BY	STATUS
PC Security breach.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. 	<ul style="list-style-type: none"> See 'Information Security' Policy. All PC's are password protected with energy saving and Firewall controls set to optimise security settings. Licensed Bit Defender anti-virus in place for all PCs. PCI compliance in place for card payments. Regular communication and awareness briefings for all internal staff stressing the importance of information security and compliance with GDPR. All passwords held on central and secure asset list to ensure they comply with password creation policy. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Test case paperwork lost.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Business disruption / interruption and delays. 	<ul style="list-style-type: none"> See 'Archiving' Policy. Implementation of documentation flow and filing process. Regular briefings through daily operations and monthly meetings on the importance of organisation and control of documents within the office. General Housekeeping monitoring through health and safety spot checks. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Loss of electronic data.	<ul style="list-style-type: none"> Business disruption / interruption and delays. 	<ul style="list-style-type: none"> See 'Business Continuity Plan' Policy. Details of electronic back-up data processes are detailed in the ISO27001 Statement of Applicability. Annual training and awareness in place of the BCP and relevant policies for all internal staff. 	1. A check has been completed and confirmed that all system back-ups are in place and working.	1. Director	1. Complete
Test samples in transit. (Courier)	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> Contracted courier services used with tracking process in place. Official and correct laboratory sample packaging used for clear indication of contents and correct transit method. Relevant SOPs in place providing instructions on correct methods of transit to use. Courier services regularly monitored in terms of performance. Contingency courier services identified in the case of failure of service. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Staff taking information / data / equipment off-site.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> See Information Security Policy. See CRA09 Information Data Security v01.02.24 (Home working) 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Loss of keys / ID pass	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. Risk of theft of data. Business disruption / interruption and delays. 	<ul style="list-style-type: none"> Key storage cupboard with colour coded key tags in use. Master building keys available for cutting if required. ID passes replaced at short notice. Staff with keys provided with full training on entry and exit to building. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete

	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	

WHAT IS THE RISK?	WHO/WHAT MIGHT BE AT RISK AND HOW?	EXISTING MEASURES TO CONTROL RISKS	FURTHER ACTIONS REQUIRED TO CONTROL RISKS FROM REVIEW	ACTION BY	STATUS
Malicious actions by exiting staff.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. Risk of theft of data. Business disruption / interruption and delays. 	<ul style="list-style-type: none"> See 'Information Security' Policy. See CRA09 Information Data Security v01.02.24 (Home working) DBS checks in place for all new staff. 	<ol style="list-style-type: none"> Working with HR Consultants to implement best practice processes. Extended DBS checking to be implemented for all internal staff. 	1. Operations Manager	1. Ongoing
Unauthorised access to the Swiftcase system.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> Database access is secured via user authentication. Each user has a password that must be of sufficient complexity and obscurity to prevent brute force. User accounts are locked after 5 incorrect attempts. User sessions will time out after 30 mins. All interaction with the database occurs over encrypted HTTPS. Attempts to login to SwiftCase are monitored through Livepoint's data centre. Refer to Information Security Policy, Statement of Applicability and Livepoint SLA Dedicated internal Swiftcase expert users provide support and liaison to approved third party supplier 'Livepoint'. 	<ol style="list-style-type: none"> None at present — as the risk is already well controlled and continuously reinforced. 		1. Complete
Unauthorised access to websites	<ul style="list-style-type: none"> Risk to company reputation and image. Business disruption / interruption and delays. 	<ul style="list-style-type: none"> Website access is secured via user authentication. Each password is of sufficient complexity and obscurity to prevent brute force. User accounts are locked after 10 incorrect attempts. User sessions will time out after 60 mins. All interaction with the websites occurs over encrypted HTTPS. Login attempts to the websites are recorded through additional services such as Jetpacks Wordpress security plugin to monitor frequency of attempts. All interaction with the websites occurs over encrypted HTTPS. Refer to Information Security Policy. Only the Director has access to the websites. New approved third party website developer in place providing an additional layer of security. 	<ol style="list-style-type: none"> None at present — as the risk is already well controlled and continuously reinforced. 		1. Complete
Unauthorised access to the Synology Disk Station and network.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. Risk of theft of data. Business disruption / interruption and delays. 	<ul style="list-style-type: none"> Network Share access is secured via user authentication. Each user has a password that must be of sufficient complexity and obscurity to prevent brute force. The guest account is disabled. The DiskStation will Autoblock suspicious login attempts. Insecure network services are disabled and defaults have been changed. The firewall blocks external access. Refer to Information Security Policy. Only the Director has access to the Synology Disk Station admin. Two-factor authentication now in place for access. 	<ol style="list-style-type: none"> None at present — as the risk is already well controlled and continuously reinforced. 		1. Complete

WHAT IS THE RISK?	WHO/WHAT MIGHT BE AT RISK AND HOW?	EXISTING MEASURES TO CONTROL RISKS	FURTHER ACTIONS REQUIRED TO CONTROL RISKS FROM REVIEW	ACTION BY	STATUS
Recording telephone calls.	<ul style="list-style-type: none"> Client personal information - risk of data breach. Confidential and/or sensitive company information. Client payment and financial details. 	<ul style="list-style-type: none"> See 'Information Security' Policy. See 'Client Privacy Policy'. See ISO 27001 Statement of Applicability. PCI compliance. Data protection registered with the ICO. Full training provided to all relevant personnel regarding call recording and pausing when taking card details. Call recording spot checks completed on monthly basis as part of monthly management meeting. Calls found to be out of compliance, QIR raised and recording deleted. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Unauthorised access to the Daktele CRM system.	<ul style="list-style-type: none"> Client personal information - risk of data breach. 	<ul style="list-style-type: none"> Access is secured via user authentication. Each user has a password that must be of sufficient complexity and obscurity to prevent brute force. All interaction with the database occurs over encrypted protocols (HTTPS, SSL/TLS). In addition, all communication is routed through a central firewall that performs real-time inspection analysis of communication. If the firewall evaluates the traffic as suspicious based on the inspection rules, the source IP address is automatically blocked. Data is regularly backed up and located for geo-redundancy in the aforementioned data centres. Only trained employees who access via a secure communication channel and are authenticated with a username and password have the necessary access to data provided by customers for the purpose of the concluded contract. Daktele has set up internal processes and procedures to protect these accesses. All data centers have 24-hour security. Only authorized and trained employees have physical access to Daktele servers. All accesses are audited and monitored. Dedicated internal Daktele CRM expert user provide support and liaison to approved third party supplier 'Digicomm'. 	1. None at present — as the risk is already well controlled and continuously reinforced.		1. Complete
Unauthorised access via WiFi	<ul style="list-style-type: none"> Client personal data, internal systems, confidential information 	<ul style="list-style-type: none"> No guest WiFi. Visitors use personal hotspots. Staff prohibited from connecting personal devices. Control enforced by Information Security Policy (5.4). 	1. None at present – risk mitigated through policy and training		1. Complete
Misuse of tablets by sample collectors	<ul style="list-style-type: none"> Client data – risk of unauthorised access, loss, or misuse 	<ul style="list-style-type: none"> Tablets issued solely for sample collection. Personal use prohibited. Usage logged and subject to audit. Covered in Information Security Policy (5.7). 	1. Annual refresher training to reinforce policy	1. Director	1. Ongoing

	Crystal Health Group Risk Assessment CRA01 Information/Data Security		Assessor: John McChrystal
	Location:	Head Office, Manchester	