
Document Processing System for CKD Screening &
Intervention Programme (GP Clinics)

Requirement Specifications

Version 5.2

Date Prepared: April 2026

Table of Contents

1.0	Introduction	3
2.0	Scope	4
3.0	Functional Specification (Mandatory)	6
4.0	Functional Specification (Optional)	8
5.0	Non-Functional & Compliance Considerations	9
6.0	Information on Third Party Security Evaluation	10
	Appendix A – High Level Process Flow	11
	Appendix B – Data Extraction Fields (Authoritative)	14
	Appendix C – Statistics for the Solution	15
	Appendix D – Cost Schedule	16
	Appendix E – Third-Party Security Evaluation	17
	Appendix F – Non-Disclosure Agreement (NDA)	22

1.0	Introduction
1.1	Purpose
	The National Kidney Foundation (NKF) invites qualified vendors to submit quotation for the provision of Intelligent Document Processing (IDP) services¹ to support NKF's kidney screening operation. Vendors to submit the following: • Mandatory quote for Intelligent Document Processing (IDP) solution in Section 3. • Optional quote for requirements in Section 4. • Quote for Year 1 maintenance [Mandatory]. • Quote for Year 2 maintenance [Optional]. NKF will evaluate the submitted proposal for awards. The objective is to define a single, vendor-ready functional specification for a solution supporting approximately 250 General Practitioner (GP) Clinics submitting screening documents to the NKF Outreach Team for processing, validation, and follow-up. After procurement closure, shortlisted vendors may be required to deliver presentations or system demonstrations, and to clarify their proposed solutions. All such activities shall be conducted at no additional cost to NKF. For demonstration purposes, up to 50 patient records will be provided to shortlisted vendors. Shortlisted vendors will be given at least three (3) weeks' advance notice prior to the presentation. Within this period, vendors are required to submit a duly signed Appendix F – Non-Disclosure Agreement (NDA). Access to GP clinic records will only be granted upon receipt of the fully executed NDA. All records provided for demonstration must be strictly used for the intended purpose and must be permanently deleted immediately after the session. Vendors are required to provide written acknowledgement via email confirming the deletion of all records (one week after the demonstration/presentation session).

¹ **Intelligent Document Processing (IDP)** is a smart way of handling documents like PDFs, scanned forms, or emails by using technology to read, understand, and organise their content automatically. It builds on Optical Character Recognition (OCR), which converts text from images into editable text, and Document Processing Services (DPS), which help sort documents and extract key information such as names, dates, IDs, or Company Names or medical lab numbers. IDP goes a step further by using AI to interpret the meaning of the content, recognise different document types, and pull out the right data with minimal human effort—essentially acting like a digital assistant that can read, understand, and process documents for user.

1.2	Background
	NKF runs a CKD² screening program with the GP clinics to provide complimentary kidney screening to high-risk individuals as part of its prevention efforts. GP clinics will send encrypted patient documents (i.e., Patient Consent Forms, Laboratory Test Report/Results and GP Clinic Invoices) to NKF by email. These documents (i.e., Patient Consent Forms and Laboratory Test Report/Results) must be processed, validated, and transformed into structured data for operational use. GP clinic invoices will not be processed for this scope of work. The current manual process is resource-intensive and error-prone, prompting the need for an IDP-based document processing solution.
2.0	Scope Overview
	In-Scope GP Clinic Submissions
2.1	Process Overview: Section 3.x defines required tasks for steps 5 and 6. <u>Refer to Appendix A – High Level Process Flow</u>, and <u>Appendix B – Data Extraction Fields (Authoritative)</u> for the fields to be collated. [1] Patient visits GP clinic (signs the consent form and does the kidney screening (blood and urine test). [2] GP clinic will receive the lab reports and doctor will request for a review for patients with abnormal results. A second kidney screening may be ordered by the doctor. [3] GP clinic will bill NKF at the start of the new month for preceding month. GP clinic will send the collated invoice together with patients consent form and lab reports. Documents will be encrypted. [4] NKF will receive & decrypt the files. [5] Validation & Quality Check by NKF (check completeness) [6] Master Tracking / Data Consolidation [7] Payment Processing (PR Submission)
2.2	Each GP clinic submission may include: a) Patient Consent Forms (including doctor assessment on risk factor) b) Laboratory Test Report/Results (e.g. blood and urine) Documents may be received in PDF, JPEG, PNG, Word, or Excel formats, either consolidated or as individual files, and across multiple emails. The GP clinic may send these patient files on different dates if they were not available earlier. These files may contain images taken by GP clinic staff on mobile phones.

² **Chronic Kidney Disease (CKD)**. Refer to <https://nkfs.org/kidney-failure/chronic-kidney-disease-ckd/>

2.3	The Contract Period shall comprise the following: a) Onboarding Period: Up to a maximum of six (6) months. b) Subscription Period: One (1) year commencing upon successful completion of the onboarding period, with an option to extend for an additional one (1) year, for a total subscription period of up to two (2) years.
	Solution Scope
2.4	• Mandatory: Intelligent Document Processing System • Optional: System integrated with the solution, to be exercised during the contract validity. • Optional: Enhancements for duplicate record detection, secure document upload, patient profile and appointment management, notifications, consultation notes, reporting capabilities, and a secure GP Clinic portal for document submission. The portal may also support encrypted document handling, automated document processing, workflow routing, and audit logging to strengthen security, efficiency, and traceability.

3.0	Functional Specification (mandatory)
3.1	Below consolidates and formalises the functional specifications. <u><i>Refer to Appendix C</i></u> for functional specification statistics.
	Document Ingestion
3.2	System shall automatically classify documents by type (Patient Consent Forms and Laboratory Test Report/Results). <u><i>Refer to clause 2.2.</i></u>
3.3	The documents may be uploaded at different times, as GP clinics can submit them in separate months. Once all two types (Patient Consent Forms and Laboratory Test Reports/Results) are matched for a patient, the record is Complete and authorised users can download and process it.
3.4	Authorised users shall be able to manually reclassify incorrectly identified documents. Audit trace will be enabled for all changes.
3.5	Upload methods may include file browse and drag-and-drop.
3.6	The system shall support placement of the scanned documents (Patient Consent Forms and Laboratory Test Report/Results) received into designated folders or repositories, for sorting by GP clinics, date of upload, etc.
	Format Support
3.7	The system shall support IDP processing for the following file formats: a) PDF (including scanned/image-based PDFs); b) JPG; c) PNG; d) Word documents containing image-based content; and e) Excel file (it may also be an Image-based file). The formats listed above are standard for GP clinics (based on past 12 months). If the proposed solution requires extra effort for configuration or incurs additional costs for alternative file formats, please specify these requirements clearly in your proposal, including any applicable charges in the Cost Schedule as an optional item.
3.8	Each file shall support a maximum size of up to 5 MB. Note: Based on data from the past 12 months, approximately 95% of files have a size of less than 1 MB. Notwithstanding this, certain GP clinics may consolidate multiple documents into a single file.
3.9	Any limitations on file size, resolution, storage, or file count shall be clearly stated in the vendor proposal.
	IDP Processing
3.10	The system shall support IDP for image-based documents within supported file formats, including laboratory reports and consent forms. Such documents may contain structured data (e.g. alphanumeric tables and

	graphical elements) as well as occasional handwritten annotations by clinicians. Based on analysis of the past 12 months, approximately 95% of files primarily contain printed or structured content. The IDP capability shall prioritise accurate extraction of printed and structured data, while supporting detection and processing of handwritten entries, ticked selections, circled responses, and annotations where feasible.
3.11	The IDP process shall convert detected text into machine-readable text without interpretation or transformation.
	IDP Output
3.12	The IDP output shall be provided in CSV and/or Excel as defined in Appendix B .
3.13	The output shall represent only the recognised text content, without tagging, field mapping, or additional classification (other than those mentioned in this specification).
	Batch Execution
3.14	The system shall support execution of IDP on multiple documents in a single batch run.
3.15	Batch execution refers strictly to processing efficiency and shall not include cross-document analysis, comparison, or aggregation.
	Storage
3.16	The system shall securely store: a) Original source documents b) Corresponding IDP output files - c)
3.17	Appropriate access controls shall be enforced to restrict access to authorised users only. <u>Refer to clause 5.1.9 on 2FA</u> .
	Export & Data Ownership
3.18	All original documents and IDP output shall remain the property of NKF.
3.19	The system shall allow full export of original documents and IDP output upon request or contract termination.
3.20	No proprietary lock-in shall be imposed on IDP output formats.
	Confidence Scoring
3.21	The system may provide confidence scores for extracted data fields. Authorised Users shall be able to easy navigate to records with low confidence scores.
3.22	The system shall flag missing, inconsistent, or low-confidence data for manual review and correction.
	Searching & Retrieval
3.23	The system shall support search and retrieval of documents and extracted data using configurable key fields such as NRIC, GP clinics, date of visit or completed records (<u>refer to clause 3.4</u>).

4.0	(Optional) Functional Specification / Enhancements
4.1	The following outlines and formalises the optional NKF's functional specification for future enhancements. NKF will conduct assessment and validation during the contract evaluation phase.
4.1.1	Duplicate Detection - System shall detect duplicate submissions across documents, patients, GP clinics, and claim periods using configurable matching rules (e.g. NRIC, patient name, visit date).
4.1.2	Document Ingestion - The system shall enable NKF to efficiently upload scanned documents through the vendor's secure web portal, preferably drag and drop.
4.2	Appointment Management System
4.2.1	Patient Profile Management - System shall create, update, and manage patient profiles based on IDP-extracted data.
4.2.2	Duplicate Patient Detection - System shall detect and manage duplicate patient records using configurable identifiers (e.g. NRIC).
4.2.3	Appointment Scheduling - System shall support scheduling, rescheduling, cancellation, and tracking of follow-up appointments.
4.2.4	Notifications - System may support automated email and/or SMS appointment notifications and reminders.
4.2.5	Visit Management - System shall record visits as episodes, including attendance status and visit history.
4.2.6	Consultation Notes - System shall support capture of consultation notes for Dietitians, Exercise Specialists, or other roles (up to two modules).
4.2.7	Reporting - System may provide operational and management reporting capabilities.
4.3	GP Clinic Web Portal – Secure Document Submission
4.3.1	The system shall provide a web-based portal for GP clinics to securely submit patient related documents (e.g. Patient Consent Forms and Laboratory Test Report/Results).
4.3.2	The portal may allow GP clinics to upload password protected or encrypted documents (e.g. PDF files secured with a document level password).
4.3.3	The system may support controlled document decryption , whereby: • Document passwords are submitted via a secure input mechanism separate from the file upload; • Passwords are not stored in plain text; and • Decryption is performed server side within the system's secure processing environment.
4.3.4	The system may automatically process decrypted documents for: • IDP and data extraction; and/or • Routing into downstream workflows, subject to configured validation rules.
4.3.5	Appropriate audit logging may be maintained for document upload, password submission, decryption, and access activities, including timestamp and user/system identifiers.

5.0	Non-Functional & Compliance Considerations
5.1	Non-Functional Requirements
5.1.1	Security & Compliance - Solution shall comply with PDPA and all applicable personal data protection and healthcare data regulations, including controls for data access, retention, and secure disposal.
5.1.2	Data Security - Solution shall implement encryption for data at rest and in transit, role-based access control, and audit logging for all access to personal and medical data. Access to the system shall require authentication and authorisation. Vendors shall state any certifications or security standards supported.
5.1.3	Availability - Solution shall be designed for high availability suitable for operational processing, with vendor to state target uptime and service levels.
5.1.4	Performance - Solution shall support concurrent processing of submissions from multiple GP clinics without material degradation in performance.
5.1.5	Scalability - Solution shall be scalable to support increases in GP clinics, document volume, and data fields without major architectural changes.
5.1.6	Data Residency - Vendor shall clearly state where data is hosted and processed, including primary and backup locations.
5.1.7	Hosting Model - Hosting model (SaaS/Cloud) shall be proposed by the vendor, including security controls and operational responsibilities.
5.1.8	Interoperability - Solution shall align and be compatible with NKF's Microsoft-based environment (Email, SharePoint, Power Platform) without requiring extensive custom integration.
5.1.9	Authentication - Mandatory Two-Factor Authentication (2FA) at least for all administrative and privileged users.
5.1.10	Backup & Restoration - Requires automated backups. Vendors must declare: a) Backup frequency b) Retention period c) Recovery Time Objectives (RTO)
5.1.11	Data Retention - Requires configurable retention (by default, up to 90 days) policies. After the age of the retention policies, system shall auto purge the records (i.e. Complete record – <u>refer to clause 3.4</u>) and keep an audit trail of the purging record.
5.2	General Compliance Considerations
5.2.1	The following non-functional specifications define NKF's expectations for solution performance, security, scalability, and operational resilience. Vendors shall address these requirements in their proposals.
5.2.2	Compliance with PDPA and all applicable personal data protection and healthcare data regulations, including requirements on data access, retention, and disposal.
5.2.3	Secure handling, transmission, and storage of personal and medical data, including encryption at rest and in transit, role-based access control, and audit logging.
5.2.4	Hosting model (SaaS/Cloud) to be proposed by the vendor, with clear articulation of data residency, security controls, and operational responsibilities.

5.2.5	Alignment and compatibility with NKF's Microsoft-based environment, including Email, SharePoint, and Power Platform, without requiring extensive custom integration.
6.0	Information on Third Party Security Evaluation
6.1	The Tenderers shall submit the required Information on NKF Third Party Information Security Evaluation Form using the template (<u>Appendix E - Third-Party Security Evaluation</u>) in procurement document.

Appendix A – High Level Process Flow

This document outlines the end-to-end process flow for the [Kidney Screening at GP clinics](#) program. Steps 5, and 6 are mandatory requirements to streamline the manual processing defined in section 3. Other enhancements are optional; vendors may quote if they have relevant experience. NKF will review all proposals and may consider them for future implementation during the contract period.

Also refer to **Appendix D – Cost Schedule**.

Steps	Activity Description
1	[GP Clinic] Patient visits GP clinic (signs the consent form and does the kidney screening (blood and urine test)). • Patient visits GP clinic for NKF-sponsored screening • Clinic staff: ◦ Registers patient ◦ Explains program ◦ Obtains signed consent form • Patient is officially enrolled in the NKF screening program
2	[GP Clinic/Partner] GP clinic will receive the lab reports and doctor will request for a review for patients with abnormal results. A second kidney screening may be ordered by the doctor. • GP clinic conducts required tests: ◦ Serum creatinine (blood test) and ◦ Microalbuminuria tests (urine test) • Doctor performs clinical assessment • Outputs generated per patient: ◦ Consent form (signed with doctor assessment on risk factor) ◦ Lab test results
3	[GP Clinic] GP clinic will bill NKF at the start of the new month for preceding month. GP clinic will send the invoices together with patients consent form and lab reports. Documents will be encrypted. • At the start of each month, GP clinic: ◦ Compiles all patients who completed tests in the previous month ◦ Organises documents per patient • Files are: ◦ Encrypted using NKF-provided password ◦ Sent via email to NKF Outreach Team

4	[NKF Outreach] NKF (Outreach Team) will receive & decrypt the files. • NKF Outreach team: ◦ Receives email submissions from GP clinics ◦ Downloads attachments ◦ Decrypts files ◦ Sorts documents into structured folders (e.g., by clinic / patient)
5	[NKF Outreach] Validation & Quality Check By NKF (check completeness) • NKF team reviews each patient record: ◦ Ensure all required documents are present: ▪ Consent form (signed) – include doctor assessment on risk factor ▪ Lab/test results ◦ Check for completeness and correctness ◦ Update Master Excel Tracker • Incomplete or incorrect submissions: ◦ Flagged for follow-up with GP clinic
6	[NKF Outreach] Data Consolidation & Tracking • Validated records are entered into a Master Excel Tracker ◦ Patient-level tracking ◦ Clinic-level tracking ◦ Status (e.g., complete, pending, rejected) • This file becomes the single source of truth
7	[NKF Outreach/Finance/Procurement] Payment Processing (PR Submission) • Following the validation and consolidation of all GP clinic submissions for the month: ◦ The NKF Outreach Team verifies the final count of completed patient screenings and consultations and updates the Master Excel Tracker. ◦ Payment is calculated based on number of completed patient screenings and consultations. ◦ • The NKF Outreach Team prepares and manually submits the Purchase Requisition (PR) in the NKF Finance System (Oracle Fusion) for processing of payment to GP clinics.
8	[NKF Outreach] Optional Enhancements (Future-State Ideas) To improve this process later:

	• Replace email with secure portal upload • Automate: ◦ File validation (check completeness) ◦ Decryption workflow • Replace Excel with: ◦ Database or case management system • Introduce: ◦ Dashboard for tracking status & payments
--	---

Appendix B – Data Extraction Fields (Authoritative)

This appendix defines the **authoritative and mandatory list of data fields** to be extracted by the IDP solution. Any field not listed below shall be considered out-of-scope unless explicitly proposed by the vendor as value-added.

SN	Fields	Data Type	Data Format	Field Size	Description	Validation	Example	Data extracted from	To match with
1	Full name	VARCHAR	-	50	Patient's full name.	Not null	Shakir Bin Md Yunus	Consent Form	Lab Report
2	NRIC	VARCHAR	-	9	Patient's NRIC.	Not null, format: one letter + 7 digits + one letter	S1234567Z		NA
3	Contact number	VARCHAR	-	8	Patient's contact number.	Not null, numeric only, 8 digits	91234567		Lab Report
4	Gender	VARCHAR	-	10	Patient's gender.	Not null, must be: Male, Female	Male		NA
5	DOB	DATE	DDMMYYYY	-	Patient's date of birth.	Not null, valid date, not a future date	15/03/1975		Consent Form
6	Age (as of screening year)	INT	-	3	Patient's age as of the screening year.	Not null, range: 1 to 120	49	Lab Report	
7	Race	VARCHAR	-	10	Patient's race.	Not null, must be: Chinese, Malay, Indian, Others	Chinese	Consent Form	NA
8	Family_Diabetes	INT	-	1	Ticked Family history risk factor.	Either 1 of this boxes must be ticked, else flag	1		
9	Family_Hypertension	INT	-	1	Ticked Family history risk factor.		0		
10	Family_CKD_ESRD	INT	-	1	Ticked Family history risk factor.		0		
11	Cardiometabolic_Cardiovascular	INT	-	1	Ticked Cardiometabolic risk factor.		0		
12	Cardiometabolic_Diabetes	INT	-	1	Ticked Cardiometabolic risk factor.		0		
13	Cardiometabolic_Hypertension	INT	-	1	Ticked Cardiometabolic risk factor.		0		
14	Cardiometabolic_Obesity	INT	-	1	Ticked Cardiometabolic risk factor.		1		
15	Cardiometabolic_Metabolic	INT	-	1	Ticked Cardiometabolic risk factor.		0		
16	Renal_hereditary	INT	-	1	Ticked Renal risk factor.		0		
17	Renal_historyAKI	INT	-	1	Ticked Renal risk factor.		0		
18	Renal_recurrent_kidneystone	INT	-	1	Ticked Renal risk factor.		0		
19	Renal_multi	INT	-	1	Ticked Renal risk factor.		0		
20	Other_hyperuricaemia	INT	-	1	Ticked Other risk factor.		0		
21	Other_nephrotoxic	INT	-	1	Ticked Other risk factor.		0		
22	Other_smoking	INT	-	1	Ticked Other risk factor.		1		
23	Date of visit	DATE	DDMMYYYY	-	Date of the screening visit. Data is not always entered chronologically so reports may not be fully accurate by date.	Not null, valid date, not a future date	03/06/2024	Lab Report	NA
24	Creatinine (umol/L)	DECIMAL	-	5	Creatinine reading in umol/L.	Positive number, either in umol/L or mg/dl	88.5		
25	Creatinine (mg/dl)	DECIMAL	-	5	Creatinine reading in mg/dL.	Positive number, either in umol/L or mg/dl	1.00		
26	eGFR (CKD-EPI/MDRD)	DECIMAL	-	5	eGFR result, calculated using CKD-EPI or MDRD formula.	Not null	72.3		
27	Abnormal eGFR?	INT	-	1	Flags whether eGFR is abnormal (1 = Yes, 0 = No). Threshold eGFR of 60-89.9 ml/min/1.73m ² may be considered as normal **Based on values from line #26	Not null, must be: 0, 1	0		
28	Ur Alb/Cre Random (mg/mmol)	DECIMAL	-	5	Urine albumin-creatinine ratio in mg/mmol.	Positive number, either in mg/mmol or ug/mg	1.8		
29	Ur Alb/Cre Random (ug/mg)	DECIMAL	-	5	UACR in ug/mg.	Positive number, either in mg/mmol or ug/mg	15.9		
30	Abnormal UACR	INT	-	1	Flags whether UACR is abnormal (1 = Yes, 0 = No). Threshold Mens 2.5 mg/mmol = 0, Women ≤ 3.5mg/mmol = 0 OR Mens 22 ug/mg = 0, Women 53ug/mg = 0 **Based on values from line #28/29 (depending on available data unit & gender)	Not null, must be: 0, 1	0	Lab Report	NA
31	Abnormal EGFR or UACR	INT	-	1	Combined flag for whether either result is abnormal (1 = Yes, 0 = No) **Based on values from line #27 and #30 (if either value =1)	Not null, must be: 0, 1	0		
32	GP clinic	VARCHAR	-	50	Name of the GP clinic.	Not null	Raffles Medical		

Appendix C – Statistics for the Solution

Current	Statistics	Remarks
Kidney health screening's GP Clinics	250 approximately	As of 01 May 2026
Patients processed monthly	650	As of 01 May 2026
Total pages process annually	32,000	As of 01 May 2026
Document Types received from GP Clinic	1. Patient Consent Forms – include doctor assessment on risk factor 2. Laboratory Test Report/Results (e.g. blood and urine)	As of 01 May 2026
User Accounts	2 (by default) <i>Note:</i> • <i>to add three (3) additional users in the future after the solution has achieved steady state. I.e., total five (5) user account.</i>	As of 01 May 2026

Appendix D – Cost Schedule

Please include price details for below Cost Schedule. **Refer to Appendix C – Statistics for the Solution** and include the necessary optional costing for additional services or scope of work.

S/N	Item Description	Quantity (A)	Unit Price (B)	Price Per Year (A*(B*12)	Total Price (2 Years) (A*(B*12) *2
1	One-Time Setup / Implementation including minimum 2 User licenses activated. (One-time effort leading to system go-live into production)	1	S\$	S\$	S\$
2	Year 1 Application Maintenance [Mandatory]	1	S\$	S\$	S\$
3	Year 2 Application Maintenance [Optional]	1	S\$	S\$	S\$
4	Professional services / man-day (*4 & *7 below)	1	S\$	S\$	S\$
5	Three (3) additional user licenses post go-live	3	S\$	S\$	S\$
TOTAL				S\$	S\$

Note:

1. Please read the requirements specification carefully before quoting the price.
2. All prices are to be quoted in Singapore dollars.
3. All itemised costs shall exclude GST.
4. The Professional services/ man-days shall be consumed anytime during the Contract.
5. The vendor shall provide the cost breakdown of the respective subscription (e.g., license fee, support and maintenance fee, etc.).
6. If the vendor proposes any other software (including third-party software), the vendor shall indicate the cost itemised in the table above. Justification should be provided in the proposal for needing the license, whether it is mandatory or optional.
7. Upon exercising the option for the Professional Service / Change Request (CR), the NKF will issue a PO based on the agreed contractor's CR effort (man-day cost) by multiplying the unit price (S\$).

Appendix E – Third-Party Security Evaluation

The purpose of conducting a Third-Party Security Evaluation is to ensure that any solution, system, or service proposed by a vendor meets the organisation's security, compliance, and risk-management requirements before adoption. Specifically, this evaluation aims to:

1. Assess the Security Posture of the Proposed Solution, and
2. Identify Potential Risks and Vulnerabilities.

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Part I

NKF Third Party Information Security Evaluation Form

Name of Company	
Person Completing the Form	
Email Address	
Phone Number	
Company Website	
Date of Assessment	

Data Controls	3 rd Party Response (Yes / No / Partially Implemented)
1. Will store all NKF data in Singapore.	
2. Maintains an audit log for the location of all NKF data.	
3. Will not access NKF data from outside of Singapore.	
4. NKF data will be promptly deleted when retention is no longer necessary for legal or business purposes.	
5. NKF data is permanently erased when deleted.	

3 rd Party's Business Associates	3 rd Party Response (Yes / No / Partially Implemented)
1. Will any 4th parties have access to NKF data?	
2. Confidentiality agreements have been signed before proprietary and/or confidential information is disclosed to the 3 rd party's business associates.	
3. 3 rd party's business associate agreements document the agreed transfer of NKF data when the relationship terminates.	
4. 3 rd party performs periodic review on business associates that have access to NKF data.	

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Access Controls	3rd Party Response (Yes / No / Partially Implemented)
1. Has a policy to protect NKF information against unauthorised access.	
2. Has a policy that prohibits sharing of individual accounts and passwords.	
3. Has a policy that implements the need-to-know and separation-of-duties principles.	
4. Implements multi-factor authentication in order to access NKF resources.	
5. Immediately removes or modifies access when personnel terminate, transfer, or change job functions.	
6. Ensures that critical data, or systems, are accessible by at least two trusted and authorised individuals, in order to limit having a single point of service failure.	

Network Security	3rd Party Response (Yes / No / Partially Implemented)
1. NKF data are not directly accessible from the internet unless the NKF data is encrypted	
2. Servers holding NKF data connected to any network must run host-based firewalls configured to block all connections to the system other than the specific types of connections needed to perform the approved functions.	
3. Documented practices are in place and followed on maintaining the configurations of host-based firewalls.	
4. NKF data must be encrypted when it traverses any network (outside of a switch in a secure information centre).	
5. NKF data must never be sent via email except in encrypted files.	
6. All users who need to transfer NKF data must make use of a secure transfer method (e.g. encrypted email).	

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

Physical Security	3rd Party Response (Yes / No / Partially Implemented)
1. Controls access to secure areas.	
2. Controls access to server rooms and follows the principles of least privilege and need-to-know.	
3. Safeguards in place (e.g., cipher locks, restricted access, room access log, card swipe access control).	
4. Shreds or incinerates printed confidential information.	
5. Escorts visitors in computer rooms or server areas.	
6. Implements environmental controls to mitigate the environmental threats to equipment.	

Contingency Planning	3rd Party Response (Yes / No / Partially Implemented)
1. Has written and tested backup procedures.	
2. Maintains a documented and tested disaster recovery plan.	
3. Has a written contingency plan for critical computing operations.	

Incident Response	3rd Party Response (Yes / No / Partially Implemented)
1. Maintains incident response procedures, including notifying NKF in the event of a breach involving NKF data.	
2. Has cyber security / liability insurance coverage.	

Appendix E – Page 3 of 4

CONFIDENTIAL – FOR THIRD PARTY EVALUATION ONLY

NKF Data Requirement					
As part of the outsourcing / contracted service arrangement, the service provider may collect, use, process or store the following types of data (please ☒ tick where applicable):					
Risk Level	Data Type	Collect	Use	Process	Store
High	☐ Personally Identifiable Information (PII)	☐	☐	☐	☐
	☐ National Registration Identity Card (NRIC) Number	☐	☐	☐	☐
	☐ Payment Card Information	☐	☐	☐	☐
	☐ Sensitive Research Data	☐	☐	☐	☐
	☐ NKF Mission Critical Information	☐	☐	☐	☐
Medium	☐ NKF Business Confidential Information	☐	☐	☐	☐
	☐ Anonymised Research Data	☐	☐	☐	☐
	☐ Other Confidential Information (Please indicate)	☐	☐	☐	☐
Low	☐ Non-Sensitive / Non-Confidential Information (Please indicate)	☐	☐	☐	☐
Additional Documents Furnished					
☐ Network Diagram ☐ Incident Management Plan ☐ Security Architecture ☐ Business Continuity Plan ☐ Security Assessment Results ☐ Disaster Recovery Plan ☐ Security Policies ☐ Cyber / Liability Insurance Certificate ☐ SOC 2, ISO Reports ☐ All relevant test report(s) ☐ Change Management Policy ☐ All relevant certification(s) ☐ Backup and Restoration Procedures ☐ Other relevant document(s)					

Appendix F – Non-Disclosure Agreement (NDA)

Note:

The Non-Disclosure Agreement (NDA) is intended to protect the confidentiality of the sample data shared with vendors and to ensure that it is used solely for evaluating the proposed solution during the shortlisted evaluation and presentation stage. NKF will notify vendors of the procurement presentation date and provide instructions for returning the signed NDA. Vendors must sign and return the NDA to NKF before the sample data is released.

NON-DISCLOSURE AGREEMENT	
This Agreement is made on [INSERT DATE]	
between:	
(1)	THE NATIONAL KIDNEY FOUNDATION, (Company Registration No.: 2000104750M) a company incorporated in the Republic of Singapore and having its registered office at 9 Raffles Place #26-01 Republic Plaza, Singapore 048619 and its principal place of business at 81 Kim Keat Road Singapore 328836 (hereinafter referred to as "NKF" or "DISCLOSING PARTY"); and
(2)	[INSERT COUNTERPARTY'S REGISTERED NAME] (Company Registration No.: [insert UEN]), a company incorporated in the Republic of Singapore and having its registered office at [Insert Address] (hereinafter referred to as " [insert initials] " or "RECEIVING PARTY")
(each, a "Party" and collectively, the "Parties").	
WHEREAS:	
(A)	The Disclosing Party may have disclosed and wish to further disclose certain information in relation to the Purpose (as defined in Clause 1 below).
(B)	The Parties wish to define their rights and obligations with respect to the said information and to protect the confidentiality thereof and proprietary features contained therein.
NOW IT IS HEREBY AGREED AS FOLLOWS:	
1.	<u>PURPOSE</u>
The Parties desire to evaluate the feasibility of [insert purpose] ("Purpose"). For such Purpose, and in consideration of the Receiving Party's agreement to keep confidential such Confidential Information, as defined below, the Disclosing Party may disclose Confidential Information to the Receiving Party under the terms and conditions set forth herein. The Party originally disclosing Confidential Information shall be referred to as "Disclosing Party" and the Party who receives information shall be referred to as "Receiving Party". The Confidential Information to be disclosed and the time of such disclosure shall be at the sole discretion of the Disclosing Party.	
2.	<u>DEFINITIONS</u>
2.1	"Confidential Information" shall mean all information disclosed by a Party (the "Disclosing Party") whether transmitted orally, in writing, electronically or in other form (and in each case, whether or not marked in writing as "confidential"), to the other Party (the "Receiving Party") relating to or in connection with the Purpose, including:
(a)	All personal data, including patient data and information;
(b)	all commercial, marketing and business information, strategic and development plans, forecasts, intentions, any matter concerning the Disclosing Party, its affairs, business, operations, shareholders, directors, officers, business associates, clients or any other person or entity having dealings with the Disclosing Party;
Page 1 of 10	

- (c) information relating to the financial condition of the Disclosing Party, its accounts, audited or otherwise, notes, memoranda, documents and/or records in any form whatsoever, whether electronic or otherwise;
- (d) scientific, technical, intellectual or other information in any form whatsoever, whether electronic or otherwise, relating to methods, processes, formulae, compositions, systems, techniques, product information, inventions, know-how, trade secrets, design rights, machines, computer programs, software, development codes and research projects; business plans, co-developer/collaborator identities, data, business records of every nature, customer lists and client database, pricing data, project records, market reports, sources of supply, employee lists, business manuals, policies and procedures, information relating to technologies or theory and all other information which may be disclosed by the Disclosing Party to the Receiving Party which the Receiving Party may be provided access by the Disclosing Party, whether stored electronically or otherwise; all information which is deemed by the Disclosing Party to be Confidential Information or which is generated as a result of or in connection with the business of the Disclosing Party and which is not generally available to the public; and all copies, reproductions and extracts thereof, in any format or manner of storage, whether in whole or in part, together with any other property of the Disclosing Party made or acquired by the Receiving Party or coming into their possession or control in any manner whatsoever;
- (e) Notwithstanding any other provision to the contrary in this Agreement, any information relating or pertaining to the patients of the Disclosing Party shall be deemed to be Confidential Information of the Disclosing Party.

2.2 "Permitted Persons" shall mean directors, officers, employees, servants, agents, representatives, consultants, independent contractors, and professional advisors (including tax, accounting and legal professionals) who are required to have the Confidential Information in relation to the Purpose.

3. LIMITATIONS OF CONFIDENTIALITY

Confidential Information does not include information:

- (a) which is or becomes public knowledge and public property through no fault of the Receiving Party or in any way without breach of this Agreement by the Receiving Party;
- (b) which the Receiving Party can show has been known or has been developed by or for the Receiving Party at any time independently of the information disclosed to it by the Disclosing Party;
- (c) which is and/or was disclosed or made available to the Receiving Party from a source other than the Disclosing Party (including through the Receiving Party's own research) without breach by the Receiving Party or such source of any obligation of confidentiality or non-use towards the Disclosing Party;
- (d) which is hereafter made generally available by the Disclosing Party or a third party or is disclosed by the Disclosing Party to a third party without a duty of confidentiality or without restriction on disclosure or use, including without limitation, by way of the publication of a patent specification;

- (e) which is disclosed by the Receiving Party with the prior written approval of the Disclosing Party; or
- (f) in respect of which the confidentiality survival period set out in this Agreement has expired.

provided however that the foregoing exceptions shall not apply to information relating to any combination of features or any combination of items of information merely because information relating to one or more of the relevant individual features or one or more of the relevant items (but not the combination itself) falls within any one or more of such exceptions.

4. HANDLING OF CONFIDENTIAL INFORMATION

4.1 In consideration of the mutual exchange and disclosure of Confidential Information, each party undertakes in relation to the other party's Confidential Information:

- (a) to maintain the same in confidence and to use it only for the Purpose and for no other purpose and in particular, but without prejudice to the generality of the foregoing:
 - (i) not to make any commercial use thereof;
 - (ii) not to use the same for the benefit of itself or of any third party other than pursuant to a further agreement with the Disclosing Party; and
 - (iii) not to use the same for the purpose of guiding or conducting a search of any information, materials or sources, whether available to the public, for any purpose whatsoever, including without limitation, for the purpose of demonstrating that any information falls within one of the exceptions in Clause 3;
- (b) not to copy, reproduce, or reduce to writing any part thereof except as may be reasonably necessary for the Purpose and that any copies, reproductions or reductions to writing so made shall be the property of the Disclosing Party;
- (c) not to upload any Confidential Information unto any artificial intelligence tools for any evaluation or analysis or advice;
- (d) to immediately notify the Disclosing Party in the event of any known unauthorised, unlawful, and/or unintended access, collection, use, disclosure, disposal, copying, modification, loss, or destruction of Confidential Information received from the Disclosing Party and cooperate with the Disclosing Party's requests to investigate and remediate such incidents and provide appropriate response and redress;
- (e) not to disclose the Confidential Information to any third parties except in confidence to such Permitted Persons, provided that such Permitted Persons are bound to terms no less stringent than this Agreement;
- (f) in relation to patients, the Receiving Party shall ensure that none of the patients of the Disclosing Party can be identified in any reports, submissions and publications of the Receiving Party;
- (g) to be responsible for the performance of sub-clauses (a) to (f) above on the part of such Permitted Persons to whom the same is disclosed pursuant to sub-clause (e) above; and

- (h) to apply thereto no lesser security measures and degree of care than those which the Receiving Party applies to its own confidential or proprietary information of similar nature and which the Receiving Party warrants as providing adequate protection of such information from unauthorised disclosure, copying, or use.

4.2 The Receiving Party shall cause such Permitted Persons involved in the Purpose to observe or be similarly bound by the terms of Agreement. The Receiving Party as the principal party shall be responsible and held liable for any breach of this Agreement by any of the Permitted Persons.

4.3 Notwithstanding the foregoing, the Receiving Party shall be entitled to make any disclosure required by law of the Disclosing Party's Confidential Information but shall give the Disclosing Party not less than two (2) business days' notice of such disclosure and shall consult with the Disclosing Party prior to such disclosure with a view to avoiding such disclosure if legally possible. Where possible, the Receiving Party shall also assist the Disclosing Party to obtain a protective order requiring the Confidential Information so disclosed to be kept in confidence and use only for the purpose for which such order was issued.

5. RETURN OF CONFIDENTIAL INFORMATION

5.1 Each party shall:

- (a) within one (1) month of completion of the Purpose destroy or upon receipt of a written request from the other party, return to the other party all documents and materials (and all copies thereof) containing the other party's Confidential Information and certify in writing to the other party that it has complied with the requirements of this sub-clause; and
- (b) notwithstanding the completion of the Purpose or return of the documents and materials as aforesaid, continue to be bound by the undertakings set out in Clause 4.

5.2 Any Confidential Information which the Receiving Party is mandatorily required by laws or by any governmental or other regulatory authority to retain custody of shall continue to be bound by the terms of this Agreement for the period such Confidential Information is retained.

6. DATA PROTECTION

6.1 Each Party shall comply with all the obligations under the Personal Data Protection Act 2012 and all subsidiary legislation including any re-enactments, supplements and amendments etc. ("PDPA") at its own cost including but not limited to the following,

- (a) only process, use or disclose personal data in accordance with the Disclosing Party's instructions and the purposes for which the personal data was disclosed, or when required by law or an order of court, but shall notify the Disclosing Party as soon as practicable before complying with such law or order of court at its own costs;
- (b) protect the personal data in its possession or under its control by making reasonable security arrangements to prevent any accidental loss or unauthorised access, collection, use, disclosure, destruction, disposal, copying and modification of the personal data, and the loss of any storage device or medium on which personal data is stored;
- (c) provide to the Disclosing Party access to the personal data that the Receiving Party has in its possession or control, as soon as practicable upon the Disclosing Party's written request;

- (d) not transfer the personal data to outside Singapore without the Disclosing Party's prior written consent. If the Disclosing Party provides consent, the Receiving Party shall provide a written undertaking to the Disclosing Party that the personal data transferred outside Singapore will be protected at a standard that is comparable to the PDPA. If the Receiving Party transfers the personal data to any third party overseas, the Receiving Party shall procure the same written undertaking from such third party.

- 6.3 The Receiving Party shall permit the Disclosing Party to conduct audits on its premises and systems to ensure that the collection, use and disclosure of the personal data are in accordance with the above requirements. The Receiving Party shall render all necessary assistance to the Disclosing Party for the purpose of such audits.

7. DISCLAIMER AND WARRANTY

- 7.1 The Disclosing Party warrants that it has the right to disclose Confidential Information to the Receiving party and to authorise the Receiving Party to use the same for the Purpose.

- 7.2 The Parties agree that any Confidential Information is made available "as is" and that no representation or warranties of any kind are granted or implied with respect to the quality of Confidential Information, including but not limited to, its fitness for any purpose, accuracy, completeness or correctness. The Confidential Information does not constitute, nor should the Confidential Information be taken as, a recommendation or inducement, or form part of any offer or invitation to sell or issue, or any solicitation of any offer to purchase any assets, nor shall it or any part of it form the basis of, or be relied on in connection with, any contract or investment decision.

8. CONFIDENTIALITY OF THIS AGREEMENT

Each Party agrees to keep the existence and nature of this Agreement confidential and not to use the same or the name of the other Party or of any other company in the Group of Companies of which the other Party may form a part in any publicity, advertisement or other disclosure with regard to this Agreement without the prior written consent of the other Party, such consent not to be unreasonably withheld.

9. DAMAGES NOT AN ADEQUATE REMEDY

The Receiving Party and the Disclosing Party both acknowledge that the Confidential Information has been developed or obtained by one another through the investment of significant time, effort and expense, and that such Confidential Information provides the Receiving Party with a significant competitive advantage over its competitors. The Receiving Party and the Disclosing Party both understand and agree that any breach of this Agreement will result in irreparable harm to the Disclosing Party and because of the unique nature of the Confidential Information, monetary damages may not be an adequate remedy in the event of such a breach or threatened breach of this Agreement. Accordingly, the Disclosing Party and Receiving Party agree that the Disclosing Party shall be entitled to seek equitable relief, including injunctive relief and specific performance, in the event of a breach or threatened breach of this Agreement in addition to all other remedies available to the Disclosing Party at law or in equity, without the necessity of proving actual damages and without the need to post bond or other security.

10. NO GRANT OF INTELLECTUAL PROPERTY RIGHTS

- 10.1 All Confidential Information remains the property of the Disclosing Party.

10.2 The Disclosing Party reserves all rights in the Confidential Information and no rights or obligations other than those expressly recited herein are granted or to be implied from this Agreement. In particular, no license is hereby granted directly or indirectly under any patent, invention, discovery, copyright or other industrial property right now or in the future held, made, obtained or licensable by the Disclosing Party.

10.3 The Receiving Party shall not file any copyright registrations, patent applications or similar registrations of ownership on the Confidential Information. In the event that the Receiving Party does so in breach of this Agreement, the Receiving Party shall assign absolutely to the Disclosing Party such registrations and applications without any cost to the Disclosing Party.

11. LIMITATION OF LIABILITY

In carrying out their respective obligations under this Agreement, the Parties shall comply with all laws and regulations applicable thereto, and save for willful acts, default, or gross negligence on their respective parts, neither Party shall be liable to the other party for any indirect, incidental, special, punitive or consequential damages however caused, including any loss of profits or business interruption costs and under any theory of liability, including but not limited to contract, strict liability and negligence; whether or not the other Party has been advised of the possibility of such damage.

12. NOTICES

12.1 All notices, communications, demands, requests, approvals or consents required to be given or made under this Agreement by either Party must be in writing and shall be effective only if either personally delivered, sent by registered mail, sent by facsimile, or sent by electronic mail to the address and persons indicated below:

For NKF

Address: 81 Kim Keat Road, Singapore 328836

Fax : +65-63569002

Email : [insert email]

Attention : [insert name and title]

For [Counterparty]

Address: < Address >

Tel : < Tel >

Fax : < Fax >

Email : < Email >

Attention : < Attention >

12.2 Every notice or communication so sent shall be deemed to have been properly served and validly made, if by hand when delivered to the recipient's address, if sent by registered post, two (2) days after posting, notwithstanding the fact that the letter may be returned by the Post Office undelivered, or if sent by electronic mail, immediately when the notice is sent without any notification that the delivery had failed.

13. DURATION AND TERMINATION

Notwithstanding the execution date as first hereinabove written, this Agreement shall **retroactively** come into effect on _____ ("Effective Date") and shall continue in full force and effect for a period of **5 (FIVE) years** with an option for the Parties to renew the term mutually in writing, unless terminated by the Parties with a thirty (30) days written notice. Notwithstanding the

expiration or termination of this Agreement, Clauses 1 to 12, 15 to 22, and 24 shall continue to be effective for a period of **[insert]** from the date of expiration or termination of this Agreement.

14. NON-ASSIGNMENT

Subject to the other provisions of this Agreement, all the terms and conditions of this Agreement shall be binding upon and inure to the benefit of the Parties and their respective permitted assigns and successors-in-title except that:-

- (i) neither Party shall transfer or assign all or any of its rights, obligations or benefits hereunder in whole or in part to any third party, without the prior written consent of the other Party, which consent shall not be unreasonably withheld;
- (ii) any permitted assignee or transferee shall agree in writing to comply with all terms and conditions of this Agreement; and
- (iii) any assignment shall not exceed the existing scope of this Agreement.

15. SEVERABILITY

- 15.1 In the event that any term, condition or provision contained in this Agreement or the application of any such term, condition or provision shall be held by a court of competent jurisdiction to be wholly or partly illegal, invalid, unenforceable or a violation of any applicable law, statute or regulation of any jurisdiction, the same shall be deemed to be deleted from this Agreement and shall be of no force and effect; whereas the remaining terms and provisions of this Agreement shall remain in full force and effect as if such term, condition and provision had not originally been contained in this Agreement, unless the severed provisions render the continuing performance of this Agreement impossible, or materially change either party's rights or obligations under this Agreement; in which event such Party may give written notice of its intent to terminate this Agreement to the other Party.
- 15.2 Notwithstanding the aforesaid, in the event of such deletion, the Parties hereto shall negotiate in good faith in order to agree to terms of mutually acceptable and satisfactory alternative provisions in place of the provision(s) so deleted.

16. WAIVER

- 16.1 No waiver of any breach of any covenant, condition, stipulation, obligation or provision contained or implied in this Agreement shall operate or be interpreted as a waiver of another breach of the same or of any covenant, condition, stipulation, obligation or provision in this Agreement.
- 16.2 Any time or other indulgence granted by a Party under this Agreement shall be without prejudice to and shall not be taken as a waiver of any of that Party's rights under this Agreement nor shall it prejudice or in any way limit or affect any statutory rights or powers from time to time vested in or exercisable by that Party.

17. DISPUTE RESOLUTION

- 17.1 In the event of any dispute or difference arising out of or in connection with or in relation to this Agreement or the existence, validity, termination, application or interpretation of this Agreement or any of its provisions, both Parties shall use their best endeavours to settle the dispute informally by agreement between them. Both Parties shall always act in good faith and co-operate with each other to resolve any disputes.

17.2 If the dispute is not settled in accordance with Clause 17.1 above within fourteen (14) days of the dispute arising, then Parties may commence legal proceedings in the Singapore Courts. Parties agree that the Singapore Courts are the most appropriate and convenient forum to settle any such disputes, and no Party shall argue to the contrary.

18. PROFESSIONAL FEES

In any suit or other proceeding relating to the subject matter of the Agreement, the prevailing Party shall be entitled to recover from the other Party all reasonable costs, fees and expenses by accountants, solicitors and other professionals for services rendered to the prevailing Party in connection with the suit or other proceeding, including costs, fees and expenses of preparation and appeal.

19. ENTIRE AGREEMENT

The Parties expressly acknowledge that they have read this Agreement and understood its provisions. The Parties agree that this Agreement and all Schedules annexed to the same constitute the entire agreement between them with respect to the subject matter of this Agreement and that it supersedes all prior or contemporaneous proposals, agreements, negotiations, representations, warranties, understandings, correspondence and all other communications (whether written or oral, express or implied) or arrangements entered into between the Parties prior to this Agreement in respect of the matters dealt with in it. No promise, inducement, representation or agreement other than as expressly set forth in this Agreement has been made to or by the Parties.

20. NO PARTNERSHIP

Nothing contained in or relating to this Agreement shall be deemed to constitute a partnership or agency relationship between the parties and no party shall have any authority to act for or assume any obligation or responsibility of any kind, express or implied on behalf of the other party or bind or commit the other party for any purpose in any way whatsoever.

21. GOVERNING LAW

This Agreement shall be deemed to be made in Singapore and subject to, governed by, and construed in all respects in accordance with the laws of the Republic of Singapore (without reference to principles of conflicts of laws).

22. THIRD PARTY RIGHTS

A person who is not a party to this Agreement has no rights under the Contracts (Rights of Third Parties) Act 2001 to enforce any term of this Agreement, but this does not affect any right or remedy of a third party which exists or is available apart from the said Act.

23. COUNTERPARTS

23.1 This Agreement may be executed in one (1) or more counterparts by the duly authorised representatives of the Parties, each of which when so executed shall be deemed to be an original and all of which taken together shall constitute one and the same agreement provided that this Agreement shall be of no force and effect until the counterparts are exchanged.

23.2 This Agreement and any counterparts may be executed and delivered electronically by emailed portable document format (PDF) document (or other mutually agreeable document format) and such electronic version shall be treated as an original.

24. MISCELLANEOUS

24.1 Words incorporating the masculine gender only shall include the feminine and/or neuter genders and vice versa, and words incorporating the singular meaning shall include the plural meaning and vice versa and words denoting natural persons shall include bodies corporate, incorporate, associated partnerships, firms, trusts, associations, joint ventures, governments, governmental agencies or departments or any other entity, and all such words shall be construed interchangeably in that manner.

24.2 References to clauses, schedules and annexes shall be references to Clauses of and the Schedules and Annexes to this Agreement. The Schedules and Annexes are to have effect and be construed as an integral part of, and shall be deemed to be incorporated into, this Agreement.

24.3 References to statutory provisions shall be construed as references to those provisions as respectively amended, consolidated, extended or re-enacted from time to time and all statutory instruments or orders made pursuant to them.

24.4 References in this Agreement to anything which any party is required to do or not to do shall include its acts, defaults and omissions, whether direct or indirect, on its own account, or for or through any other person and those which it permits or suffers to be done or not done by any other person.

24.5 In the event of a conflict between any of the terms of this Agreement, including any Schedules and Annexes, the conflict will be resolved in the following order of priority: (1) the Clauses of this Agreement; (2) the Schedules and Annexes.

24.6 In the event the Parties enter into a substantive agreement in relation to, or arising out of, the Purpose of this Agreement, the Parties may elect to incorporate the terms of this Agreement into such subsequent agreement, notwithstanding the duration and survival provisions set out herein.

IN WITNESS WHEREOF the duly authorised representatives of the Parties hereto have executed this Agreement as of the day and year first above written.

Signed for and on behalf of
The National Kidney Foundation

Signed for and on behalf of
[Insert Counterparty's name]

By: **[Enter Name Here]**
[Enter Designation Here]

By: **[Enter Name Here]**
[Enter Designation Here]

In the presence of:

In the presence of:

Name: [Enter Name Here]
Designation: [Enter Designation Here]

Name: [Enter Name Here]
Designation: [Enter Designation Here]