NRIC Guidelines
Frequently Asked Questions

This document is intended as an additional resource to provide clarifications on the interpretation and implementation of the NRIC Guidelines.

Any queries relating to this document may be addressed to moh_nric_enquiries@moh.gov.sg.

FAQ Table of Contents

First issued: 02 February 2026

A. Authentication vs Identification

[FAQ 1.1]
What is the difference between identification and authentication in healthcare settings? When is each required?

[Ans 1.1]
The definitions of "identification" and "authentication" are elaborated in the Joint Advisory Against Using NRIC Numbers for Authentication by PDPC and CSA against using NRIC numbers for authentication.

MOH has also published Guidelines on ceasing the use of NRIC numbers for authentication by healthcare service providers ("NRIC Guidelines"), as well as this set of Frequently Asked Questions (FAQs) setting out common healthcare scenarios where healthcare service providers need to conduct identification and authentication respectively.

[FAQ 1.2]
What are the considerations to setting challenge questions when authenticating over phone calls?

[Ans 1.2]
When formulating challenge questions for authentication over phone calls, healthcare service providers may wish to consider the following principles to ensure security and practicality.

- **Knowledge-based authentication principles**: Effective challenge questions should be based on information that is truly private and not easily discoverable through public records or social media. Questions may draw from recent activity (e.g. which grant/scheme are you applying for, what is the name of the Next-of-Kin (NOK) or caregiver you appointed and informed us of recently, at which Specialist Outpatient Clinic (SOC) was your last appointment, what was the last billed amount).
- **Question design and variety**: Design questions that have specific, unambiguous answers (e.g. what is your mother's maiden name) rather than subjective responses that might vary depending on interpretation. Maintain a diverse pool of potential questions across different categories such as recent activity, registered contact details. This variety prevents predictability and reduces the risk of social engineering[1] attacks.
- **Practical implementation**: Consider the cognitive load on legitimate users, particularly the elderly who may need more time to recall specific details or access information. Structure questions in a logical sequence, starting with simpler checks before progressing to more detailed queries. Ensure that questions remain relevant and answerable - avoid asking about very old

[1] Social engineering is a type of manipulation where someone tricks you into giving away information or doing something that benefits them, usually for malicious purposes. Instead of using technical hacking methods, social engineers exploit human psychology and trust to get what they want.

appointments or services. Additionally, establish clear protocols for situations where patients cannot answer questions due to legitimate circumstances, such as poor recall or recent changes to their personal information.

- **Risk-based approach**: Strike an appropriate balance between security and patient experience by taking a risk-based approach - use more rigorous authentication measures for higher-risk transactions or when suspicious circumstances are detected.
- **Training using corporate manuals, SOPs**: Train staff to recognise when additional authentication may be warranted and when flexibility might be appropriate, while maintaining consistent security standards across all patient interactions.

B. Interactions with Third Parties

[FAQ 2.1]
What should healthcare service providers do when someone other than the patient (e.g. family members, friends, couriers) collects medication, test results, or referral letters on the patient's behalf?

[Ans 2.1]
We have set out guidelines for such scenarios in the NRIC Guidelines. Please refer to the following examples in the Guidelines –

- Table 1, row #5 on collection of documents on behalf of the patient.
- Table 2, row #7 on collection of medication on behalf of the patient.

[FAQ 2.2]
Do healthcare service providers need to authenticate insurance companies requesting patient information? What checks should apply?

[Ans 2.2]
Healthcare service providers should establish policies and practices to ensure that the disclosure of patient information to external parties such as insurance companies is appropriate and in accordance with prevailing legislation such as the Personal Data Protection Act 2012 (PDPA) and other requirements such as the Healthcare Services Act 2020 (HCSA), the Singapore Medical Council Ethical Code and Ethical Guidelines and the Singapore Dental Council Ethical Code and Ethical Guidelines (ECEG).

Suggested measures include confirming the identity and legitimacy of the insurer personnel requesting information by using official business contact details; obtaining and checking that appropriate patient consent that specifically covers the requested information and purpose has been given; maintaining records of all disclosures, consent forms, and authorisation documents. Healthcare service providers should also practise data minimisation (i.e. limit the personal data collection, use and disclosure to what is directly relevant and necessary to accomplish the notified purpose). You may refer to MOH Circular No. 02/2026 on Guidance on Disclosure of Patient Medical Records to

Insurers for more information regarding the appropriate disclosure of patient medical records to insurers.

[FAQ 2.3]
When company HR departments require diagnoses on invoices for reimbursement, what guidelines should healthcare service providers follow?

[Ans 2.3]
Please refer to FAQ 2.2.

In general, healthcare service providers should provide the health records and invoices to their patients, for their patients' onward submission to their HR departments. Public healthcare patients can also download their health records and invoices from HealthHub.

Where patients request healthcare service providers to submit their health records and invoices directly to their HR departments, healthcare service providers need to check and ensure that the patients have given appropriate consent for the disclosure of their personal data to their HR departments and that such disclosure otherwise complies with the PDPA and other requirements such as HCSA and the relevant ECEG before doing so.

[FAQ 2.4]
Do the NRIC Guidelines apply to third-party vendors that act on healthcare service providers' behalf in processing personal data?

[Ans 2.4]
The NRIC Guidelines apply to healthcare service providers' third-party vendors where they are processing personal data for and on behalf of the healthcare service providers.

[FAQ 2.5]
How will the NRIC Guidelines affect healthcare service providers and patients?

[Ans 2.5]
The NRIC Guidelines are contextualised from the PDPC-CSA Joint Advisory, and are intended to provide guidance to healthcare service providers on the appropriate and safe use of NRIC numbers in healthcare settings.

The care provided to patients will not be affected by the NRIC Guidelines, although patients and their caregivers/NOK can expect some adjustments to healthcare service providers' operational processes to align with the NRIC Guidelines.

C. Specific Patient Segments

[FAQ 3.1]
How should authentication measures accommodate patients with varying technological literacy, particularly elderly patients?

[Ans 3.1]
Authentication measures to be adopted should balance security with operational needs, e.g.

- Offer tiered or multiple authentication channels that allow tech-savvy patients to use app-based authenticators or biometrics, while those less comfortable with technology can rely on methods such as SMS One Time Password (OTP) email and in-person assistance;
- Consider allowing formally registered caregivers or family members to assist with authentication through caregiver accounts with appropriate patient consent and audit trails, and ensure easy access to helpdesk support for guided assistance; and
- Apply risk-based authentication that matches security requirements to the sensitivity of the personal data to be disclosed or the importance of the transaction.

[FAQ 3.2]
How should healthcare service providers handle authentication for unconscious patients or those with diminished mental capacity?

[Ans 3.2]
Please refer to footnote 7 of the NRIC Guidelines on the approach to handling unconscious patients. In an emergency scenario where the patient is unable to authenticate himself/herself (e.g. patient is unconscious), the patient should not be denied care due to this. A temporary number should be issued for the patient, until the healthcare service provider is able to properly authenticate the patient's identity and reconcile any records as soon as practicable (e.g. his family member brings his/her physical NRIC to the hospital)).

For patients who lack capacity, the Mental Capacity Act 2008 applies.

D. Data Protection and Documentation

[FAQ 4.1]
Can healthcare service providers retain copies of patients' NRIC/birth certificates/passports in patient records for subsequent visits?

[Ans 4.1]
Healthcare service providers may retain copies of patients' NRIC/birth certificates/passports in their patient records, in accordance with the requirements set out under prevailing legislation such as HCSA and PDPA.

[FAQ 4.2]
How should healthcare service providers protect patient data while meeting authentication requirements?

[Ans 4.2]
Healthcare service providers may refer to the PDPA on protection of personal data - Advisory Guidelines on Key Concepts in the PDPA (Chapter 17). Please refer to Footnote 2 for additional resources[2].

[FAQ 4.3]
What advice can MOH provide for sending PDF documents to patients, insurers, or other healthcare service providers?

[Ans 4.3]
We have provided guidance in the NRIC Guidelines on the sending of PDF documents to other parties. Please refer to Table 1, row #6 on emailing PDF documents.

E. Operational Concerns

[FAQ 5.1]
Should healthcare service providers retain discretion in determining authentication levels based on their clinical settings and patient safety requirements?

[Ans 5.1]
In general, healthcare service providers should consider their business and operational needs when determining appropriate authentication measures.

The NRIC Guidelines expand on the PDPC-CSA Joint Advisory, by explaining when authentication is required and how authentication should be conducted in common healthcare scenarios. Healthcare service providers can conduct authentication in more scenarios, or implement stricter authentication measures, than those set out in the Guidelines.

[FAQ 5.2]
Why must healthcare service providers comply with the NRIC Guidelines?

[Ans 5.2]
Organisations have an existing obligation under the PDPA to make reasonable security arrangements to protect the personal data in their possession or under their control, and

[2] Additional CSA and PDPC resources:
- Enable 2FA and use strong passphrase
- SingCERT Password Checker
- SG Cyber Safe cybersecurity toolkits for organisations
- Advisory Guidelines on Key Concepts in the PDPA (see especially chapter 17 on the Protection Obligation)
- Data Protection Practices for ICT Systems

non-compliance can result in enforcement actions. Ceasing the use of NRIC numbers for authentication is part of the implementation of this protection obligation, and the NRIC Guidelines provide guidance on when authentication is required and how authentication should be conducted in common healthcare scenarios.

In general, the NRIC Guidelines help healthcare service providers to protect personal data and reduce security vulnerabilities caused by reliance on NRIC numbers for authentication. Compliance also helps build public trust and maintain patient confidence.

[FAQ 5.3]
When do the NRIC Guidelines come into effect?

[Ans 5.3]
The NRIC Guidelines take effect once they are issued. Healthcare service providers should implement the Guidelines as soon as possible.

[FAQ 5.4]
Are there any exceptions to the NRIC Guidelines?

[Ans 5.4]
There are no exceptions to the NRIC Guidelines.

Healthcare service providers are to incorporate the recommended authentication measures in the NRIC Guidelines. Healthcare service providers may implement stricter authentication measures than those recommended, based on their specific business and operational assessments.

F. Public Education and Awareness

[FAQ 6.1]
What guidance will be provided to help patients understand when and how to update their contact details with healthcare service providers?

[Ans 6.1]
Healthcare service providers may communicate these changes to patients through various channels such as Electronic Direct Mail (EDM), email notices, and their websites.

G. Email and Digital Communications

[FAQ 7.1]
How should healthcare service providers handle email enquiries containing sensitive patient information?

[Ans 7.1]
Please refer to the NRIC Guidelines for information on how to handle electronic communications involving NRIC numbers and other sensitive health information, e.g. Table 2, row #8.

[FAQ 7.2]
What checks should be followed for digital communications with patients and third parties?

[Ans 7.2]
Please refer to the NRIC Guidelines for information on how to handle electronic communications involving NRIC numbers and other sensitive health information, such as Table 1, row #7 and Table 2, row #2.

-END OF DOCUMENT-