MINISTRY OF HEALTH
SINGAPORE

Guidelines on ceasing the use of NRIC numbers for authentication for healthcare service providers

In consultation with the Personal Data Protection Commission (PDPC) and Cyber Security Agency of Singapore (CSA).

Issued on 02 February 2026

Introduction

1. A person's NRIC number is a unique identifier and used to establish the person's identity where there is a need for a high degree of accuracy. However, it is also not secret and must be assumed to have been disclosed to at least a few other persons. This means that it should not be used as an authenticator (i.e. to prove that the person is indeed who he/she claims to be) or as a password to gain access to privileged information or services.

2. NRIC numbers are considered personal data and are subject to the Personal Data Protection Act 2012 (PDPA) requirements. Organisations, including healthcare service providers, must handle NRIC numbers with care, ensuring that their collection, use, and disclosure of NRIC numbers comply with PDPA requirements. This includes implementing appropriate security measures to protect NRIC numbers in their possession or under their control from unauthorised access, use or disclosure.

Definitions

3. Identification is a declaration of who you are. A name can be used for identification. However, because multiple persons can have the same name, the Government-issued NRIC number serves to uniquely identify each person.

4. Authentication[1] is about proving that you are who you claim to be. Authentication refers to the process of proving that a person is who he claims to be, before granting him access to services or information intended only for him. This differs from identification, where identifiers such as names are used to tell people apart. Authentication can be achieved by providing something only you know (e.g. a strong password), something only you possess (e.g. a security token), or something only you have (e.g. a fingerprint or iris).

5. "Medical information" includes information about an individual that relates to the assessment, diagnosis, treatment, prevention or alleviation of an ailment, a condition, disability, disease or disorder or an injury affecting any part of the human body or mind.

[1] The process of authentication should not be confused with the process of identification in a high-fidelity use case. Identifiers such as name, NRIC number and date of birth can only be used for identification. If authentication is necessary, the person will have to provide something more, in addition to these identifiers, to prove that they are who they claim to be.

Guiding principles on the use of NRIC numbers

6. It is important to distinguish between NRIC *numbers*, and the physical (the actual card) or digital NRIC (in the Singpass app). NRIC numbers cannot be used for authentication. However, the physical or digital NRIC can be used for authentication, specifically, by comparing the person's appearance against his photograph[2] in the physical or digital NRIC.

7. NRIC numbers should be used solely for identification. Any practices involving the use of NRIC numbers for authentication should be stopped as soon as possible, in alignment with the Joint Advisory Against Using NRIC Numbers for Authentication by the PDPC and CSA issued on 26 June 2025.

8. For each scenario, healthcare service providers should first assess whether authentication is necessary.

9. If authentication is assessed to be necessary, healthcare service providers should implement methods of authentication that do not rely on NRIC numbers.

Scenarios in which authentication is necessary

10. The provision of healthcare services involves extensive interaction with members of public (e.g. patients or clients, their next-of-kin (NOK) and/or caregivers). In some scenarios, healthcare service providers must not only identify, but also authenticate, the member of public they are interacting with, for example, to ensure that patient care or patient information is provided to the correct person.

11. Table 1 below sets out the scenarios in which authentication should be conducted. In these scenarios, it will not suffice to obtain the NRIC number of the person (whether the full or partial NRIC number).

[2] Comparing with the person's photograph in his/her passport is also an acceptable alternative.

Table 1: Scenarios in which authentication is necessary

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
1	**Registering patients/clients**[3] This only applies at the first visit[4], and for inpatient admissions [5] and day surgeries[6].	In-person	Authentication can be conducted by sighting the patient's physical NRIC, or the digital NRIC in Singpass, and comparing the patient's appearance against his/her photograph in his/her physical or digital NRIC.	Authentication is required at least at the time of the first visit, and for inpatient admissions [7] and day surgeries, to ensure that investigations, treatment and subsidies are provided to the correct person. Further, many downstream activities rely on the authentication done at the point of initial registration. Similarly, authentication is required at the point of registration for an inpatient admission, when the tamper-proof wrist tag is placed on the patient. Thereafter, to manage the operational burden of repeated authentication and in line with current practices, it may suffice to ask the patient to identify

[3] In non-clinical care settings (e.g. home assessment for care service applications), the requirement to authenticate at the client's first visit/interaction applies correspondingly.

[4] This refers to the first time an individual is registered with the institution, regardless of the setting (e.g. emergency department, polyclinic or specialist outpatient clinic (SOC)). For clarity, a patient who had previously visited an institution (A) in the same Cluster should still be regarded as visiting the new institution (B) under the said Cluster for the first time, if it is his/her first visit at that particular institution (B). Ideally, the patient should also be authenticated at the start of each subsequent visit, and healthcare service providers can choose to do so.

[5] This includes inpatient admissions via inter-hospital transfers.

[6] Where there is no inpatient admissions process, authentication would be required on the day of the surgery.

[7] 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/her family member brings his/her physical NRIC to the hospital).

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
				himself/herself using two or three of his/her identifiers (e.g. name, NRIC number or date of birth) before investigations (e.g. blood tests, ultrasounds) and treatment are provided. Identification also suffices for most follow-up visits (e.g. at a polyclinic or specialist outpatient clinic (SOC)), especially where the clinician or care team is already familiar with and is able to recognise the patient. Healthcare service providers that wish to take a more cautious approach and authenticate patients even at subsequent visits can continue to do so, following the same authentication method in this row.
2	**Updating personal particulars, including contact details**	In-person (at a counter) OR At an e-kiosk OR Using a mobile app or online portal	Authentication can be conducted by sighting the patient's physical NRIC, or the digital NRIC in Singpass, and comparing the patient's appearance against his/her photograph in his/her physical or digital NRIC. For updating of personal particulars (including	Authentication is necessary as the patient's personal particulars (e.g. contact number, email and home address information) will subsequently be used to identify him/her, or to send medical information to him/her. Patients who request to update their personal particulars over the phone (i.e. inbound call to a call centre) should be redirected to manned counters, mobile apps/online portals, or e-kiosks, where authentication can be properly conducted.

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			contact details) at e-kiosks [8], authentication should be conducted either via Singpass/SgID login, or via SMS OTP to the patient's registered mobile number. Patients who are unable to authenticate at e-kiosks should be redirected to manned counters. Alternatively, personal particulars can be updated through an online portal or mobile app[8], after Singpass/SgID login or SMS OTP.	If none of these options are feasible, the healthcare service provider can arrange a video call with the patient, where the patient can show his/her physical or digital NRIC during the call, for authentication by comparing his/her appearance against his/her photograph in his/her physical or digital NRIC.
3	**Discharging newborns/ children/ mentally incapacitated patients into a caregiver's custody** This only applies to the inpatient /day surgery discharge scenario.	In-person	The caregiver's identity should be authenticated, based on the healthcare service provider's records. This can be done by comparing the caregiver's appearance against his/her	Authentication is required to minimise the risk of discharging the child or patient, or sharing the patient's medical information, to the wrong person.

[8] These authentication measures are not applicable if the healthcare service provider does not provide e-kiosks or mobile apps/online portals as avenues for updating personal particulars in the first place.

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			photograph in his/her physical or digital NRIC.	
4	**Accessing digital services** e.g. using a mobile app like HealthHub, or an online portal to access the patient's medical information	Digital	Singpass[9]/SgID login	Authentication is necessary before access can be given to the medical information and other sensitive personal data in the mobile app or online portal.
5	**Release of hardcopy documents[10]** e.g. invoices setting out the treatment given / medication prescribed, and medical reports This row only applies to the release of hardcopy documents as a standalone transaction, for example, when the patient visits the healthcare service provider for the sole purpose of collecting the document.	In-person Or By post	For requests made in person, authentication can be conducted by comparing the patient's appearance against his/her photograph in his/her physical or digital NRIC. For requests made over phone calls etc, authentication must be conducted in accordance	Authentication is necessary before access can be given to medical information and other sensitive personal data, for example, when the patient has a standalone interaction with the healthcare service provider (e.g. patient does not have any appointment with the clinic but visits the clinic to request for a copy of his medical report)[11]. If authentication had been conducted at the start of the patient's visit at the healthcare institution, the release of hardcopy documents to the patient during and immediately after an in-person consultation would not require re-authentication, as the patient's identity would have been established earlier.

[9] Singpass is only required for transactions involving disclosure of medical information or other sensitive personal data to the user. For digital services/specific functions that do not share medical information or sensitive personal data (e.g. for checking clinic opening hours), Singpass login is not necessary.

[10] Hardcopy documents that do not contain patients' sensitive personal data would not require authentication. For example, a hard copy document containing general instructions on wound care would not require authentication.

[11] Where the next-of-kin (NOK) would like to collect the documents on behalf of the patient, the NOK should present his/her own physical/digital NRIC during the collection to enable authentication to be conducted by comparing his appearance against his photograph in his physical/digital NRIC. Healthcare service providers should also require the NOK to produce a letter of authorisation from the patient that clearly states the authorised NOK's NRIC number, and the patient's physical NRIC as part of the collection process. Where authorised personnel (e.g. staff of nursing homes) are collecting documents on behalf of patients as part of their duties, the personnel should produce a letter of authorisation from the patient and/or organisation, a copy of the patient's NRIC, and their own physical/digital NRIC during the collection.

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			with Table 1, row #7 below, before the documents are sent to the patient's registered mailing address.	
6	**Emailing documents** e.g. invoices setting out the treatment given / medication prescribed, and medical reports	Digital	The PDF file should be password-protected with a randomly-generated strong password that is distributed out-of-band (e.g. via SMS to the patient's registered mobile number). Permutations and combinations of patient identifiers other than NRIC number and/or date of birth such as the patient ID number or appointment chit number issued by the healthcare service provider, may also be used as the password. An alternative approach is for the patients to be authenticated and to	Authentication is necessary before access can be given to medical information and other sensitive personal data.

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			confirm their email addresses before the PDF documents are sent to them (without a password).	
7	**Inbound calls and messages from members of public** This applies to calls from members of public enquiring about their medical test results, the status of their applications for financial assistance / grants / nursing home applications etc.	Calls and messages (landline, mobile, commercial messaging platforms, voice-over-IP)	The caller's identity should be authenticated using information that is not commonly available, but available from the healthcare service provider's records, using at least two challenge questions. This may be the name of a family member, the name of the nursing home the patient applied for, or the date (e.g. the month and year) on which the patient submitted his/her application for financial assistance. If the healthcare service provider does not have sufficient information in its records, it can send an	Authentication is required for inbound calls from members of public, as there is a risk that the caller may be wrongfully trying to gather information about another person. Thus, authentication is necessary before any sensitive personal data (e.g. whether their application for a nursing home is successful, whether they tested positive for a disease and whether they have been successfully scheduled for a particular medical procedure) is released over an inbound call. The disclosure of personal data should be kept to a minimum. For example, if the caller is enquiring about the status of his/her application for financial assistance, it suffices to state whether the application is still being processed or has been approved. Unless the caller has been properly authenticated, details of the amount of financial assistance approved should be communicated by email or letter to the patient. If none of the methods of authentication is feasible during the phone call, healthcare service providers

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			SMS OTP to the patient's registered mobile number, for authentication.	may consider alternatives to conduct authentication e.g. arrange a video call with the patient, where the patient can show his/her physical or digital NRIC during the call, for authentication by comparing the patient's appearance against his/her photograph in his/her physical or digital NRIC prior to proceeding with the request. For other interactions over the phone where there is no disclosure of sensitive personal data (e.g. general information about types of healthcare services available or appointment slots available) healthcare service providers may only require identification.
8	**Teleconsultations**	Video conference	Customised links and/or meeting IDs with passwords should be sent to the patient at his/her registered mobile number or email address. An alternative would be for authentication to be conducted by asking the patient to show his/her physical or digital NRIC on screen and comparing his/her appearance against the photograph in	Authentication is necessary before access can be given to medical information and other sensitive personal data. Authentication is also necessary to ensure that care and medical advice are given to the correct patient.

No.	Type of encounter	Mode of interaction	Method of authentication	Comments
			his/her physical or digital NRIC during the video call.	

Use of NRIC numbers for identification

12. Table 2 below sets out examples of scenarios in which it suffices for healthcare service providers to identify the member of public, i.e. authentication is not required. In these scenarios, NRIC numbers can be used for identification of the member of public. To be clear, healthcare service providers can also choose to conduct authentication in these scenarios; if so, authentication measures similar to those in Table 1 should be implemented.

Table 2: Scenarios in which authentication is not required (i.e. NRIC numbers can be used for identification)

No.	Type of interaction	Mode of interaction	Comments
1	**Care delivery** (after initial authentication) e.g. medical consultations, blood taking, clinical procedures, home monitoring programmes	In-person Or Text messages	If authentication had been conducted at the point of the first visit or initial registration for inpatient admissions/day surgeries, identification is generally sufficient to ensure that the correct patient is being treated thereafter. This is typically effected by the healthcare staff asking the patient for at least two identifiers (e.g. name, NRIC number or date of birth), which are checked against the healthcare service provider's official records. For home monitoring programmes (e.g. Mobile Inpatient Care@Home), where the patient submits vital signs data to the care staff via text messages, identification is generally sufficient, if authentication had been done at the outset of communications (e.g. when initiating the chat, or creation of the chat group, or adding a new party such as NOK and/or caregiver to the chat group).

No.	Type of interaction	Mode of interaction	Comments
2	**Outbound calls and messages to members of public**	Calls and messages (landline, mobile, commercial messaging platforms, voice-over-IP)	For outbound calls to members of public, it suffices for the healthcare service provider to ensure that it correctly calls the registered number of the member of public and confirms with the member of public his/her name and NRIC number. The disclosure of personal data should be kept to a minimum. In cases where sensitive personal data needs to be shared with the member of public (e.g. calls to patients for the purpose of pre-surgery administration), authentication similar to that of inbound calls (refer to Table 1, row #7) would be required[12].
3	**Bill payments**	In-person, e-kiosk, digital platforms (online)	Identification is sufficient to ensure that the funds are credited to the correct patient's account. Authentication will be necessary if specifics of the treatment or prescribed medication are disclosed to the payor during the billing process. To clarify, for same-day in-person bill payments at the counter after the appointment, identification will suffice if authentication was conducted earlier. For bill payments via e-kiosks, identification is sufficient if information about the treatment and prescribed medication is generalised in the on-screen display during the payment process (the details can be separately sent to the patient after payment). Authentication will be necessary if specifics of the treatment or prescribed medication are disclosed to the payor in the payment process.
4	**Applications for financial assistance** e.g. caregiving grants, payment of subsidised medical bills, insurance claims	In-person	Where an application for financial assistance is made on behalf of another person, the healthcare service provider should identify both the patient and person applying on his/her behalf.

[12] To minimise patients' possible discomfort in providing the answers to challenge questions during an inbound call, healthcare service providers may wish to direct them to their official website or mobile application for the necessary pre-surgery information.

No.	Type of interaction	Mode of interaction	Comments
5	**Research** e.g. clinical research	In-person	The researcher typically consults the relevant clinician to identify suitable patients to participate in the research study. The clinician will obtain patient consent to proceed before the researcher subsequently approaches the shortlisted patient to share further details on the research study. The researcher may ask the patient to provide his/her NRIC number for identification at this stage. (The research study team typically does not record the patient's NRIC number in study-related documents and the patient should be issued a research ID number to avoid research bias and to preserve patient's confidentiality.)
6	**Issuing medication (inpatient)** This only applies to the administration of medication to inpatients.	In-person	Authentication would not be required for inpatients, because they are wearing a tamper-proof wrist-tag after being authenticated at the point of admission. In this scenario, in accordance with the current practice, it suffices to ask the patient to identify himself/herself using two or three of his/her identifiers (e.g. name, NRIC number or date of birth) before medication is administered.
7	**Collection of medication** This only applies to the collection of medication from pharmacies, pharmacy e-lockers[13], and home deliveries. It does not cover the administration of medication to inpatients.	In-person OR E-lockers OR Home deliveries	Identification is sufficient for the collection of medications at pharmacies, e-lockers, and home deliveries, as the patient would have been authenticated at the point of prescription. For collection via e-lockers, healthcare service providers should ensure that there are sufficient measures (e.g. SMS OTP to unlock the lockers) to ensure the medication is collected by the patient/NOK. The patient's NOK can collect medication on behalf of the patient, by producing the patient's physical/digital NRIC, or a letter of authorisation from the patient together with a copy of the patient's NRIC.

[13] This refers to lockers owned and managed by healthcare service providers for the purpose of enabling the self-collection of medication.

No.	Type of interaction	Mode of interaction	Comments
8	**Inbound email enquiries from members of public**	Email	Inbound email enquiries from members of the public do not require authentication, provided that no personal data is disclosed to the enquiring party in the response. However, in cases where the response would involve the disclosure of sensitive personal data, the enquirer should be redirected to appropriate channels where proper authentication measures are in place or release such information via password-protected documents (refer to Table 1, row #6).

END OF DOCUMENT