USE CASE 1
NATIONAL HEALTHCARE

A Use Case and Issue Brief
Prepared by CIPIT

Strathmore University
Centre for Intellectual Property and Information Technology Law

01

BACKGROUND

Nationalized health care is a common way for countries to fulfil their obligations toward the health of citizens. National health care systems typically involve a combination of public and private care providers, and account for substantial percentages of national budgets.

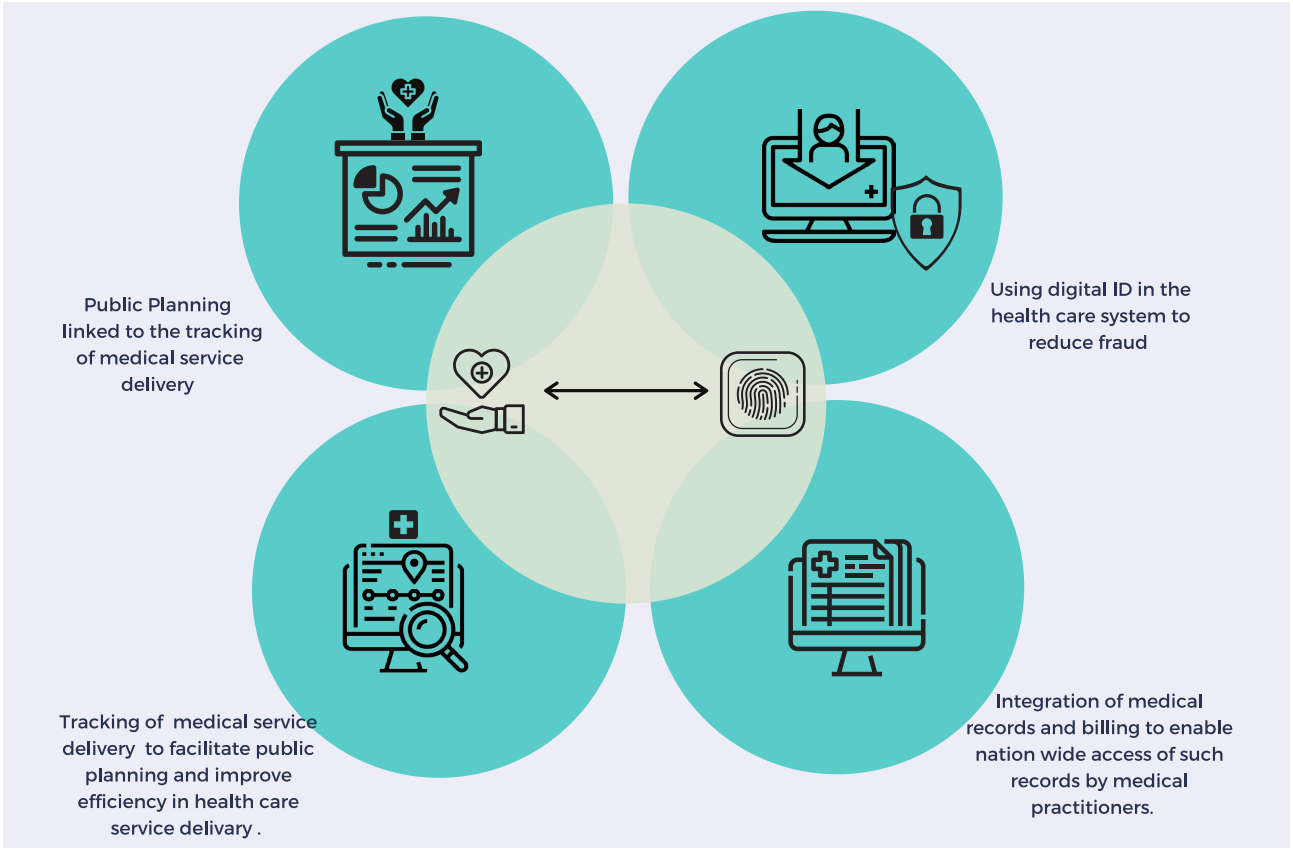
Digital Identity (DID) systems have become increasingly popular in Africa, and new DID systems for foundational ID are in the planning or implementation phase in many countries. Once a national foundational DID system is in place, it is common for countries to attempt to integrate the national health care system as a use case extension for the DID system. Even before the existence of a digitized foundational ID system, countries may try to implement a DID system specifically for the delivery of health care.

Given the highly sensitive nature of the involved data, the use of DID for implementing a national health care system must be closely scrutinized.

JUSTIFICATIONS FOR THE USE CASE

In the use case of public healthcare service delivery, the issues raised for which Digital ID is often proposed as a solution are:

1. Reduction of fraud
2. Tracking of service delivery for public planning and improving efficiency
3. Integration of medical records and billing, and nationwide access of such records by medical providers.



DATA INVOLVED IN THE USE CASE

The data that are collected for DID in the use case of public healthcare may include:

1. Identification information (foundational ID information, also family relations, etc.)
2. Healthcare history, health records (e.g., appointment history, diagnoses, medications ordered and collected, test results, etc.)
3. Biometric data for verification

RISKS INVOLVED IN THE USE CASE

The risks associated for Digital ID in the use case of public healthcare are:

1. Susceptibility of the DID system to fraud (inflated claims, bogus claims, etc.)
2. Loss of highly sensitive health data about individuals
3. Use of the data by government for purposes that are not consistent with human rights norms

Healthcare is clearly a use case where the risks of using DID are very high. The highly sensitive nature of the data involved means that data breaches are exceptionally damaging to the human rights of the data subjects. Also, there is a substantial threat of misuse of the data by government authorities. Nevertheless, the large amounts of money and other resources allocated to national healthcare systems means that even small increases in efficiency have large impacts.

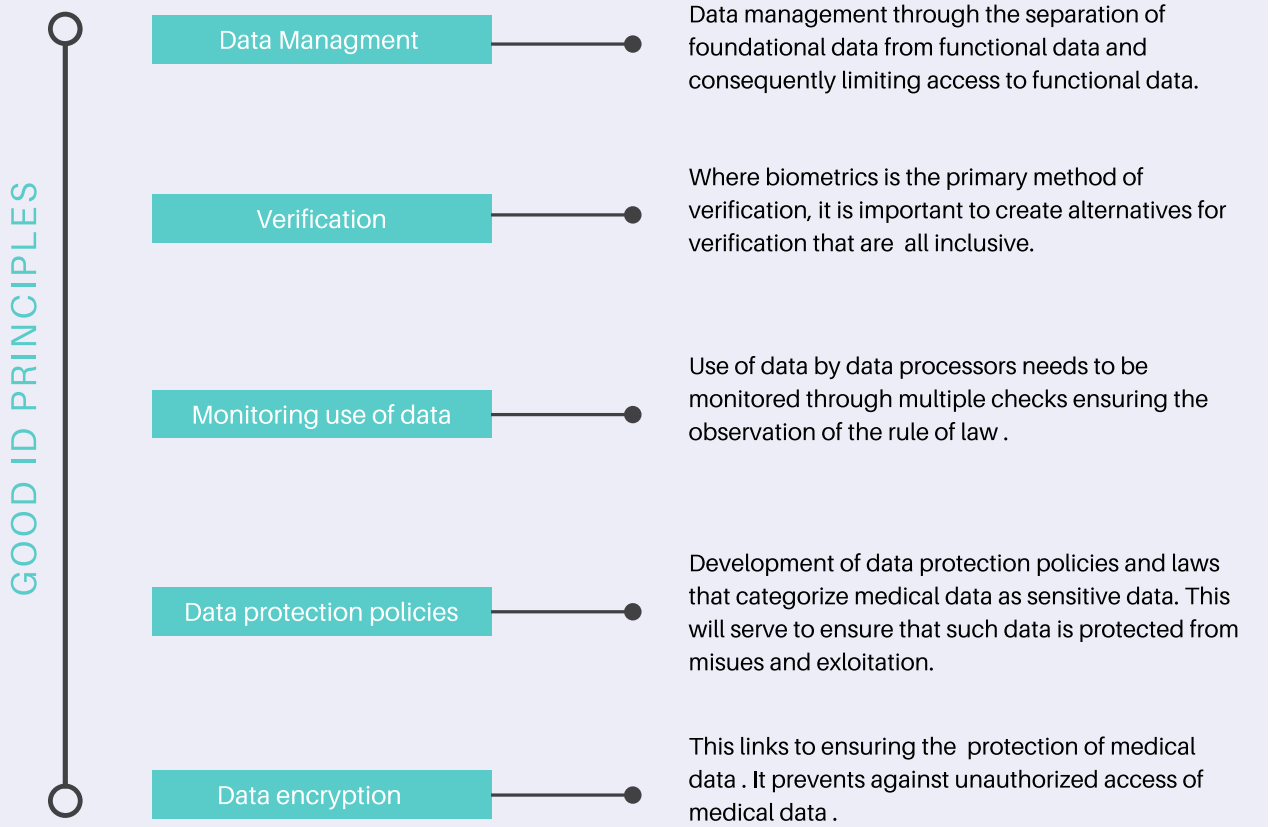
02

ANALYSIS

The use of biometric authentication or verification can increase the complexity of the system, but is common in modern systems currently being implemented. The experience of the Aadhaar system in India with respect to false positive and false negative verifications is illustrative: such errors resulted in denial of service to individuals, and in the case of health care, denial of service could be life-threatening.

The example of Kenya (see case study on the following pages) shows the importance of enabling individuals to access and correct the records stored in the DID system. Without access, for example, individuals cannot monitor their accounts for improper charges. Kenya is also an example showing the important role of the courts in ensuring that DID systems do not go too far in collecting sensitive information about individuals (e.g., HIV status) that can be used to violate the rights of those individuals.

Reduction of fraud is often a primary justification for DID in health care. There is little evidence that DID provides this benefit, as DID systems are not infallible. In situations where there is a lack of accountability and rule of law, fraud remains an issue even when DID is implemented.



GOOD ID PRINCIPLES IN THE USE CASE

1. Separation of the foundational data from the functional health care data, and highly limited access to the functional data.

2. Availability of alternative methods for verifying an ID when a patient is seeking services. This is particularly important where biometrics are used as the primary method of verification.

3. Multiple strong checks on the use of data by data processors. Such checks include a functioning judiciary, government oversight committees, and strong civil society organizations. Respect for the rule of law is critical in this regard.

4. A data protection legal regime that specifically lists medical data as highly sensitive data.

5. Mandatory encryption of data, and mandatory use of PKI.

03

CONCLUSION

Alternatives to centralized DID should be considered and explored for this use case. The primary alternative is a stand-alone system, not linked to any other public or private systems, that exclusively manages national health care.

04

ADDENDUM: KENYA AS A CASE STUDY.

The National Hospital Insurance Fund (NHIF) is a public social welfare scheme. It was established in 1966 as a health insurance provider for formal employees. In 1972, the fund was expanded to incorporate those in informal employment but it was not until the NARC administration that the Fund reached out to the unemployed as well as self-employed.

NHIF is now a statutory corporation. It administers several social welfare programmes such as Linda mama under which the government complements maternity care; cover for public secondary schools; Health Insurance Subsidy Programme (HISP) where government covers very poor, orphans and vulnerable children; and Inua Jamii which covers people over the age of 70 and persons with severe disabilities. NHIF also manages health insurance schemes for some public bodies. The current administration has been piloting universal health care in conjunction with NHIF in selected counties.

Prior to reforms during the NARC administration, NHIF membership comprised mainly of workers in formal employment, as this is mandatory. The number has steadily increased, for several reasons. One, the fund is open to all persons, making it possible for even a significant number of those in informal employment to enrol. Two, the fund alleviates social pressure associated with community fundraising for sick relatives. Many have found it easier to enrol their relatives who need constant medical care such as renal services and therapy. Three, the fund is adopted to Kenyan realities, allowing each member to enlist up to 10 children. Four, with devolution of health services, the fund has partnered with many county hospitals, advancing the reach of healthcare. According to its 2018 annual report, NHIF had enrolled over 7.7 million principal members, covering about 25 million people.

However, the fund has faced many challenges. The increased number of people, coupled with the government's plan for universal health care, means that the fund has to be more efficiently managed. The fund is one of the few parastatals retained after the liberalisation period, and it has had to leverage on technology in order to deliver services competitively. With liberalisation of other insurance services, NHIF has found itself at loggerheads with the insurance regulator, IRA. IRA has questioned NHIF's provision of medical insurance to certain public agencies. NHIF has also faced cases of fraud, where hospitals overrated procedures, leading to wastage of funds.

Digitalisation in general can resolve the problems associated with efficiency. For example, NHIF services are delivered in about 67% of public hospitals and 20% of private hospitals and a small number of mission hospitals.

NHIF serves a diverse clientele through its different programmes. For example, civil servants are entitled to a wide package compared to self-employed who are matched to specific hospitals for outpatient services. There is also the question of emergency health services. Article 53 of the Constitution provides for the right to emergency care. Hospital matching makes it difficult to deliver these services. According to persons who had emergencies far from their specified facilities, they had to pay in order to access the nearest NHIF accredited facility then later make a claim to NHIF.

In 2015, NHIF procured a smart system from global digital ID vendor Genkey. The rationale for the system was reduction of fraud, where patients would register and be authenticated using biometrics. This would be an upgrade from the current practice where patients produce their national ID and NHIF cards. Under the new system, hospitals would also make claims electronically and in real time after the patient

receives the services. This requires facilities to have good power and internet connections.

Reports in 2018 indicate that the system had been rolled out in 500 facilities in Nairobi. To enhance the accuracy of data, NHIF also begun collecting proof of marriage for spouses registered as beneficiaries. This is normally in form of a marriage certificate or affidavit. Children are registered using birth notifications or certificates.

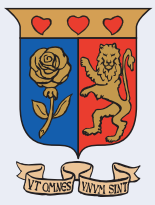
With the national digital ID system Huduma Namba, NHIF will be a functional ID database that will be linked to the centralised digital ID system. It is expected that national ID numbers will be verified against the centralised database. It is not clear whether this will be done on a one-off basis or every time a member accesses NHIF services.

NHIF inevitably collects sensitive health data of its members. From this data, it is possible to deduce important information for national planning such as trends in diseases and their treatment, population and migration as well as future health needs. Such information can either be used beneficially or to harm. It can be used to improve efficiency of service delivery or to profile parts of the population that are prone to certain health conditions. Health rights civil society organisations in 2018 successfully advocated against collection of biometrics for HIV patients, decrying the intrusiveness of the proposed data. They feared that such data could be criminalised, thereby dehumanising HIV/AIDS patients as well as sex workers, men who have sex with men and people who inject drugs.

Collection of biometrics as planned by NHIF should therefore be subjected to the test in the new Data Protection Act. The Act requires carrying out of a data protection impact assessment prior to collection and processing of data. Such an assessment would help to determine how much data is required from members in order to process their claims efficiently.

A problem identified by many NHIF members is the lack of information about their accounts. For example, they are not informed when hospitals make claims on their behalf, or when their premiums are due. Notably, NHIF charges penalties for late payments and those on self-employed packages who pay their premiums whenever they can afford often find themselves either having to physically visit NHIF offices or cybercafes in order to get a statement of their accounts.

Those in formal employment whose private insurance companies insist on cost-sharing with NHIF also have to follow up with fund to ensure their employers have been remitting their dues. NHIF has a portal through which limited self services such as registration, payment and change of hospitals can be accessed. They also have a USSD service for members to query. However, the information service could be improved through NHIF sending relevant information, such as when premiums are due or when a claim is made from a member's account.



Ole Sangale Rd, Madaraka Estate.
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612
Email: cipit@strathmore.edu | Website: https://cipit.strathmore.edu