DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

## DSCI Sectoral Privacy Guide

# Healthcare

## Disclaimer

The content of the publication has been collected, analysed and compiled with due care based on the information and sources believed by DSCI to be reliable, available at the date of publication. However, DSCI disclaims all warranties as to the accuracy, completeness, or adequacy of such information. DSCI shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. Readers of this publication are advised to seek their own professional guidance before taking any course of action or decision, for which they are solely responsible. It is highly advised to take note of the current Government and Sectoral regulations in place at the time of any practice implementation as they are subject to change from what has been represented now. The material in this publication is copyrighted but allowed for free distribution. You may not, however, modify, reuse or use the contents of the report for commercial purposes, including the text, graphics, presentations, etc. without DSCI's written consent.

# CONTENTS

# 1 BACKGROUND

## ABOUT THE INITIATIVE

Data Security Council of India (DSCI), through its Sectoral Privacy Project, aims to bring data privacy best practices to large enterprises, Small and Medium Enterprises (SMEs), and Start-ups, through the creation of sector specific guidance material. This is envisaged to enable organisations to assess their data practices and implement privacy controls to achieve meaningful compliance. The guidance material will focus on imparting a holistic understanding of data privacy and the nuances of implementing privacy controls.



# OUR APPROACH FOR DEVELOPING THE GUIDE

**Need for sectoral focus**

In our experience and through multiple stakeholder discussions, we have observed the need for a deep dive analysis of privacy implementation considerations and best practices at the sectoral level, to accelerate the adoption of best practices. This guide takes into consideration data privacy related directions and rules enacted by sectoral regulators, sectoral benchmark standards, and globally accepted frameworks and standards. Adoption of such guidance material would help organisations better position themselves to attract new business opportunities and demonstrate compliance to the regulators. As data and privacy become leading topics in the global dialogue of digital services, being transparent about how data is being used in digital products is increasingly getting vital to gain trust among all audiences. The need for such trust is further amplified in the healthcare sector where provision of healthcare services is predicated on provision of patient sensitive data to the entity providing the said services.

**Patient centric approach**

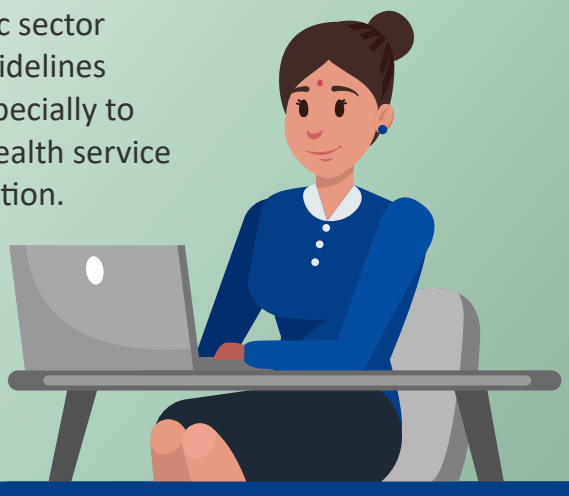
While the healthcare ecosystem, and all the different entities in it, are taking concerted efforts to offer the best possible care to the patients, especially during the digitization era, the one entity that is at the centre of this entire ecosystem is the patient. All the other service providers, and even the government, revolve around the requirements of common individuals, who will, invariably, approach medical care providers multiple times during their lifespan. The entire landscape is, therefore, primed to cater to this one entity, offering them a variety of options and services in an attempt to provide them with optimal healthcare. This guide lays emphasis on the patient's journey in the healthcare ecosystem and identification of specific intervention points for healthcare service providers to alleviate different privacy risks emanating from the different data operations.

**Advisory group**

This guide has been created with the assistance of an advisory group of industry experts consisting of Ms. Deanna DiCarlantonio, Data Protection Officer, United Health Group; Mr. Kumar KV, Chief Information Officer, Narayana Health Group; Mr. Jeyaseelan Jeyaraj, Senior Director, Health Sciences, Oracle Corporation; Mr. Arvind Sivaramakrishnan, Chief Information Officer, Apollo Hospitals and Mr. Suprio Dasgupta, Chief Data Privacy Officer, Dr Reddy Labs.

# WHO SHOULD REFER TO THIS GUIDE?

Health service providers ranging from doctors, private or public sector hospitals to allied health professionals can benefit from the guidelines established in this report. The guide would be of assistance especially to privacy and security professionals that are aligned with such health service providers and constantly handle patient centric health information. It outlines the key practical steps that health service providers should take to embed good privacy in their practice keeping the patient at the heart of the compliance process.



# 2 INTRODUCTION

Access to healthcare services, at the primary, secondary and tertiary care levels, has become of utmost importance in today's day and age. World over, governments are investing in creating health data infrastructures and regulatory policies to enable data availability and use. These policy measures would be imperative in making improvements in care co-ordination and care delivery, and in finding new ways to make systems more productive and sustainable.

The Government is now more focused than ever before on creating a robust and sustainable healthcare model that is poised to mitigate the disease burden. Digital technology is playing a catalytic role in enabling the healthcare ecosystem and taking it towards its goals. Innovative digitization can be used to design an integrated health ecosystem that places healthcare seekers at the centre of the system and offers them quality healthcare solutions that are easily accessible, comprehensive, and, most importantly, cost-efficient.

It is heartening to note that the Government is decisively focused on empowering the healthcare landscape. In August 2020, India's Prime Minister Shri Narendra Modi launched the innovative 'National Digital Health Mission' (NDHM) with an aim to create an "open digital health ecosystem" in the country. The endeavour is to create a shared digital infrastructure that is accessible to both public and private organisations, enabling them to collaborate and offer future-ready healthcare services.

Digitization of the healthcare ecosystem will lead to major and necessary alterations like enhanced information transparency, interoperability, standardized processing of claims, digitized prescriptions, and improved access to services. The digital core will also allow service providers to innovate when it comes to age-old methods of providing healthcare solutions to customers, opening up new grounds for development and progress. With patients becoming increasingly aware of their health issues, and paying more attention to the care being provided, the Indian healthcare ecosystem is ripe for change. Inevitably, technology and digital innovation will play a key role in orchestrating this change.

### Implications for Data Privacy

There has been an increase in the range of health data that is being collected, including clinical, administrative, genetic, behavioural, and demographic data. At the same time, the potential to process and analyse these emerging streams and volumes of data – big data – and to link and integrate them, is growing. However, in the absence of relevant policy measures to safeguard data privacy, there is a risk of missing the opportunity to safely enable data use to improve healthcare quality and outcome.

Health data — or data used for health-related purposes — is currently not regulated by a single national privacy framework. Health data means data related to the state of physical or mental health of the data principal. It includes records relating to the past, present or future state of health of the data principal, data collected in the course of registering for health services, and data associating the data principal to the provision of specific health services. This means that every part of the data collected about the patient (data principal) is vital and providers should maintain the privacy, confidentiality, and accuracy of the data collected in order to establish trust with the patient. When trust is created, patients will share their complete health information with the provider, enabling the provider and the patient to make more informed decisions. In addition to harming patients, breaches of health information can have serious consequences for organizations, including reputational and financial harm. Poor privacy and security practices heighten the vulnerability of patient information in the healthcare information system.

**To help cultivate patients' trust, healthcare service providers should:**

Maintain accurate information in patients' records.

Make sure patients have a way to request electronic access to their medical record and know how to do so.

Carefully handle patients' health information to protect their privacy.

Ensure patients' health information is accessible to authorized representatives, when needed.

# CURRENT REGULATORY LANDSCAPE IN INDIA

India is fast emerging as a global front runner in digital adoption. Digitization and technology are bringing incredible opportunities to the Indian economy and will play a major role in the country's economic and social transformation. The Indian healthcare sector has been at the heart of this transformation, ushering in advancements in diagnosis, treatment, and service delivery mediums. However, the healthcare sector remains nascent in the nature and extent of its interaction with privacy regulations.

The current and evolving privacy framework in India stands on the firm foundation laid down by the Honourable Supreme Court of India, in its landmark judgment in Justice K.S. Puttaswamy v. Union of India & Ors[1]., recognising 'Right to Privacy' as a fundamental right guaranteed under Part-III of the Constitution. The Apex court observed that Information Privacy comes under the scope of Right to Privacy. The said judgement also highlighted the need to draft a data protection legislation for India with the current regime being unable to address evolving privacy concerns. Currently, the latest version of the Indian Personal Data Protection Bill (IPDP), 2019 is being evaluated by a Joint Parliamentary Committee, under the Chairmanship of Shri P. P. Chaudhary.

The nature of data handled in the healthcare sector, i.e., the patient's personal information such as medical history and physiological conditions, are considered Sensitive Personal Data, or (Information under Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[2] Healthcare service providers must, to the extent of applicable regulations, incorporate requirements associated with enabling consent, creating a privacy policy, disclosing information, and implementing the relevant security measures and grievance redressal mechanisms.

For entities involved in NDHM, the health data management policy[3] also serves as a guidance document across the National Digital Health Ecosystem. Further, it sets out the minimum standard for data privacy protection that should be followed across the board in order to ensure compliance with the applicable laws, rules, and regulations.

In this evolving privacy landscape, with national level legislative measures towards a single national privacy framework and supplementary sectoral policy measures, it would become imperative for healthcare service providers to create visibility and transparency around the purpose and usage of personal data of Indian residents and incorporate fundamental principles and best practices as part of their organisational DNA.

[1]Writ Petition (Civil) No 494 Of 2012)

[2]Rule 3, Reasonable security practices and procedures and sensitive personal data or information Rules, 2011

[3]Health data management policy, National Digital health mission (2020) available at: https://ndhm.gov.in/documents/HealthDataManagementPolicy

# 3 PRIVACY AND THE HEALTHCARE ECOSYSTEM

Ecosystems create powerful forces that can reshape and disrupt industries. In healthcare, they have the potential to deliver a personalized and integrated experience to consumers, enhance provider productivity, engage formal and informal caregivers, and improve outcomes and affordability. Healthcare has a direct impact on a country's population, its productivity, and its economic growth. Consequently, it becomes essential to identify the various pain points in a country's healthcare ecosystem and proactively work towards alleviating them.

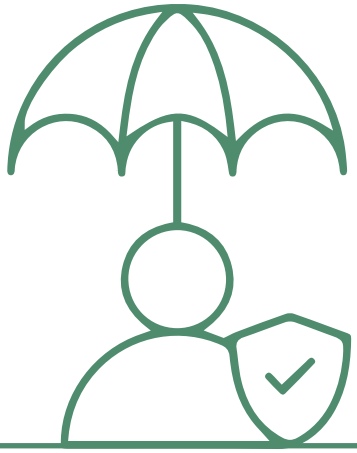
For a healthcare seeker, it is imperative that the healthcare services available in the country are easily accessible, cost-effective, and of good quality. The services they seek could be related to preventive care, primary care, secondary and tertiary, or post-hospitalization event care. In order to cater to these requirements, there is an entire ecosystem of diverse players that enable access to healthcare. This ecosystem broadly includes the following players:

## Healthcare providers

These are the primary and the most visible players in the healthcare ecosystem since they directly interact with the patient. Within healthcare providers, there are a number of diverse entities like corporate hospitals, government hospitals, home care providers, hospitals in tier-II cities, diagnostics, and enablers. Each provides a different quality and type of healthcare, and at varying costs.

## Pharma

These would include the pharmaceutical companies that focus on manufacturing medicines and conducting Research and Development (R&D). In addition to pharmaceuticals, there are the suppliers and distributors that ensure the availability of medication and the retail pharmacies that stock and sell medicines and other healthcare solutions.



## Payers

Considering that quality healthcare comes with a cost, the insurance players play an integral role in the healthcare ecosystem. Health insurance providers enable healthcare seekers to access the required healthcare solutions without having to worry about the cost of treatment. In this category, there are diverse players including private health insurance providers, social health insurance providers, employee health insurance, and third-party administrators (TPAs).

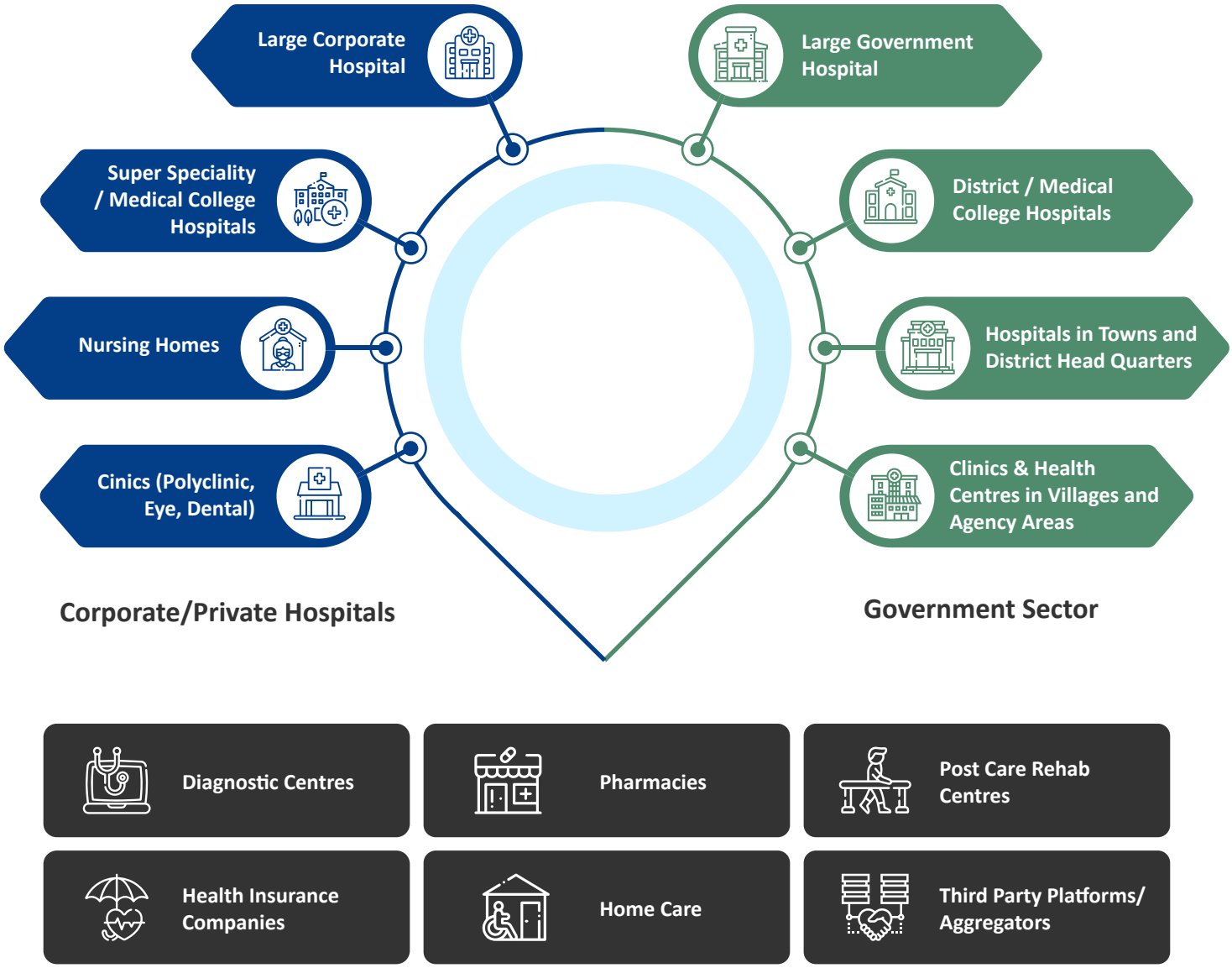



Fig.1 Healthcare ecosystem overview

An ecosystem can be defined as a set of capabilities and services that integrate value chain participants (customers, suppliers, and platform and service providers) through a common commercial model and virtual data backbone (enabled by seamless data capture, management, and exchange) to create improved and efficient consumer and stakeholder experiences, and to solve significant pain points or inefficiencies.[4] At the core of this complex and symbiotic ecosystem lies the patient. The healthcare ecosystems of the future, like other ecosystems, will be centred on the consumer, in this case the patient.

[4]The next wave of healthcare innovation: The evolution of ecosystems. Available at: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-next-wave-of-healthcare-innovation-the-evolution-of-ecosystems# (last accessed 20th May, 2021)

# EVOLVING HEALTHCARE DATA EXCHANGE ECOSYSTEM

The healthcare ecosystem's future will likely be defined by the needs of different patient populations and their associated effective care journeys (including beyond care as well). The consumer-oriented nature of these ecosystems will also increase the number of healthcare touchpoints, with the goal of modifying patient behaviour and improving outcomes. On one end of the spectrum, healthcare ecosystems have emerged to address the needs of healthy patients, who have less consistent medical challenges, but often set personal wellness goals. These patients will likely experience a more digital ecosystem, where patient data and insights are consumed in a highly personalized and meaningful way, such as with wearable devices.

Big healthcare data has considerable potential to improve patient outcomes, predict outbreaks of epidemics, gain valuable insights, avoid preventable diseases, reduce the cost of healthcare delivery, and improve the quality of life in general. Further, interoperability of health data systems will allow patients to share their digital health records across providers, thus making "coordinated care" a reality. Additionally, patients will be able to easily switch providers without losing continuity of care. The digitization of the providers' treatment advice will also ease claim filing and processing for providers and payers. An integrated healthcare ecosystem that allows for the seamless and secure exchange of data can alleviate the several pain points in India's health care ecosystem.

One of the most popular alliances between disparate entities, and one that offers hope for a healthier and more vibrant future for the Indian healthcare ecosystem, is the Swasth alliance[5]. This alliance, aimed at bolstering the public health infrastructure in the country, saw active participation from entities including hospitals, pharmacies, healthcare startups, NGOs, government organizations, and investors, who came together voluntarily to combat the pandemic. Going ahead, this alliance, and many like it, could prove to be the first frontier of care in similar situations as they take concerted efforts to close the gaps between the disparate entities that form the Indian healthcare ecosystem.

In addition, the digital initiative has ensured that all the different entities can partner and collaborate more efficiently and seamlessly, making the Indian healthcare ecosystem more wholesome and better equipped to cater to the patients' needs. Such partnerships can prove to be critical in bridging the divide between the various stakeholders in the healthcare ecosystem and making healthcare accessible to everyone. Even as there are considerable benefits offered by the digital healthcare ecosystem, it is still important to consider the various data privacy implications of digitization. Allowable uses of data while preserving security and the patient's right to privacy is of utmost importance. Individuals may fear adverse impact, both personal and professional, if their undisclosed medical issues are subject to unauthorised disclosure.

[5]Swasth.App. https://www.swasth.app/home. (last accessed 20th May 2021)

**In this ecosystem the patient data is shared for a variety of activities and operations. These can be categorised into the following:**

## Traditional care

Patient provided data/ demographic data is collected and shared to facilitate direct care and administering pharmaceuticals by providers, across traditional sites of care.

## Home and self-care

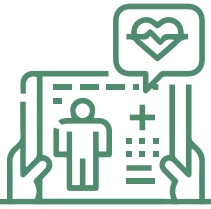
Patient health risk & status data is shared to enable self- and virtual care, remote monitoring, and traditional care that can increasingly be delivered near or in the home.

## Payment & social support services

Patient administrative data is shared for social and community networks related to a patient's holistic health focused on community elements of unmet social needs and to perform financial data operations and financial infrastructure supporting industry care events, including payment and financing solutions.

## Daily life activities

Patient Health and wellness data is utilised and shared to enable wellness and health, including fitness and nutrition.



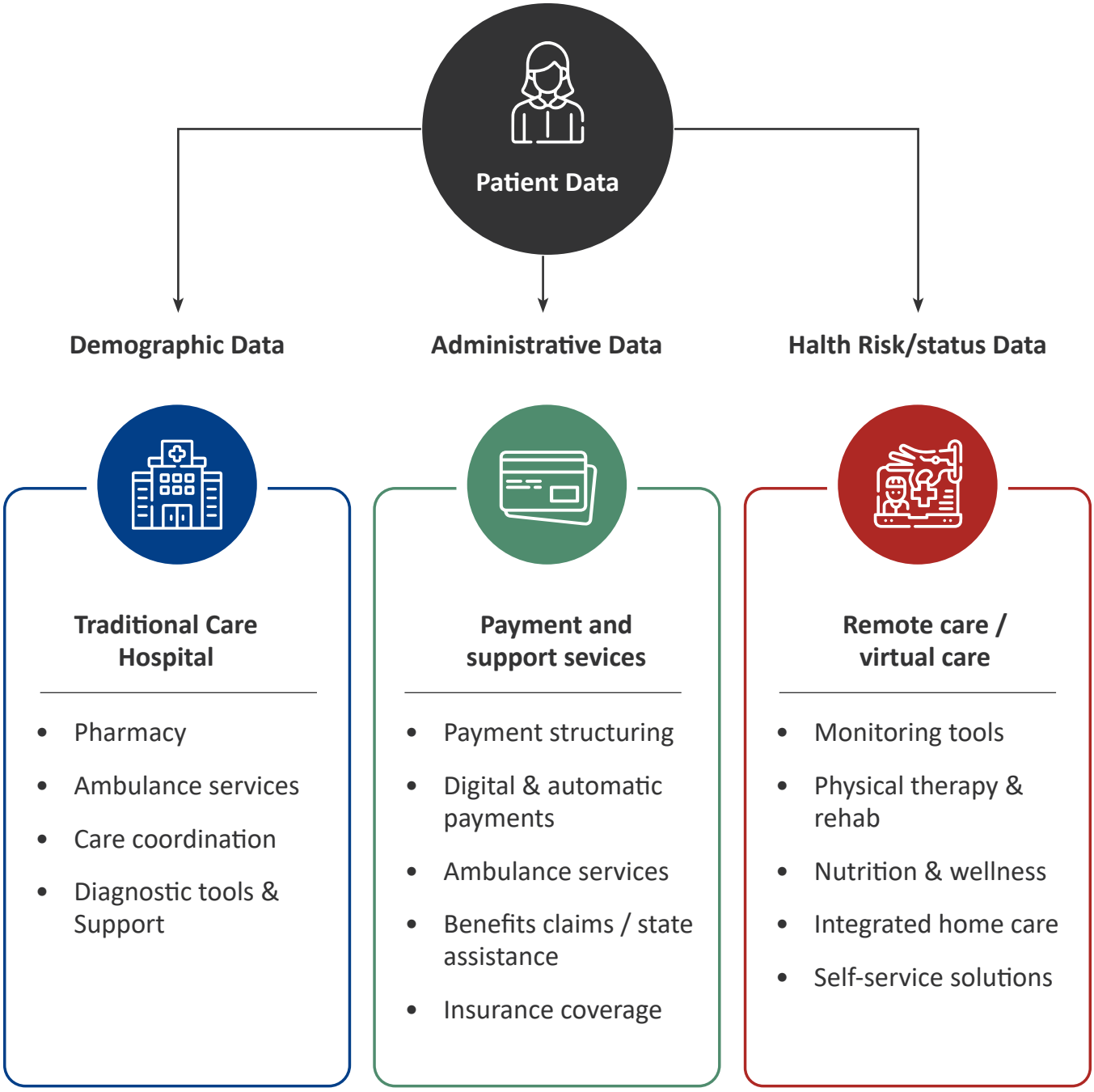



Fig.2 Patient data sharing ecosystem

While such data sharing is advantageous, but the lack of defined procedures and standard protocols could make it difficult to regulate data entry as well as the flow of information from one healthcare provider to the other. Giving rise to instances of excesses and encroachment of privacy rights guaranteed to an individual. These high-risk instances of collection, use and sharing of patient data have been examined in the next section.

# 4 PATIENT HEALTHCARE JOURNEY AND KEY CONCEPTS

While the healthcare ecosystem, and all the different entities in it, are taking concerted efforts to offer the best possible care to the patients, especially during the digitization era, the one entity that is at the centre of this entire ecosystem is the patient. All the other service providers, and even the government, revolve around the requirements of common individuals, who will, invariably, approach medical care providers multiple times during their lifespan. The entire landscape is, therefore, primed to cater to this one entity, offering them a variety of options and services in an attempt to provide them with optimal healthcare. The patient's journey in the healthcare ecosystem is a long and elaborate one, consisting of various steps that take them closer to better health and wellbeing.

The patient's sojourn, from the point of entering a healthcare service environment, to the time of exit, includes a number of steps that lead to the generation of copious amounts of data. For instance, consider the example of a patient approaching a hospital for a surgical procedure. The healthcare journey will start with an outpatient visit and examination at the outpatient clinic. The next step would be to conduct the relevant tests which would lead to diagnosis, medication, and possibly surgery. In case the outcome is a surgery, then in the weeks preceding the surgery the patient will need to conduct some more tests. Post the surgery and after the initial discharge there could be follow-up tests or post-hospitalization care. Throughout this cycle, the patient divulges sensitive and private information which is recorded in the hospital's data repository and shared with other players in the ecosystem.

Thus, it is imperative that the appropriate measures be adopted by healthcare providers to both enhance healthcare outcomes and protect the privacy of the data provided by patients. This will pave the way for a more resilient, agile, and flexible healthcare ecosystem aimed at providing effective care to patients.

# KEY CONCEPTS FOR UNDERSTANDING PATIENT PRIVACY CONSIDERATIONS

## Data

We can broadly categorise data into four different types: onsite, offsite, offline, and inferred data. The types are based on where and how the data is collected and whether the data is provided directly by a user or deduced by other methods.

**Onsite:**
User generated content or observed actions occurring on your organisation premises.

**Offsite:**
Data collected on another business' site or app.

**Offline:**
Data businesses collect and share details of activity in their physical stores.

**Inferred:**
Insights gathered based on all other data inputs.

## Personal Health Data (or Information)

All personal data collected in the course of providing a health service is considered Personal Health Data or information. It can be broadly classified into the following categories:

**Demographic** data consist of facts such as age (or date of birth), gender, race and ethnic origin, marital status, address of residence, names of and other information about immediate family members, and emergency information. Further, information about employment status (and employer), schooling and education, and some indicators of socioeconomic class might also appear.

**Administrative** data include facts about health insurance such as eligibility and membership, dual coverage (when relevant), and required co-payments and deductibles for a given benefit package. With respect to services provided (for example, diagnostic tests or outpatient procedures), such data also typically include charges and perhaps the amount paid as insurance settlement. Administrative data commonly identify providers with a unique identifier and possibly give additional provider-specific facts; the latter might include information about the kind of practitioner (physician, podiatrist, psychologist), physician specialty, and nature of institution (general or specialty hospital, physician office or clinic, home care agency, nursing home, and so forth).

**Health risks** information reflects data related to behaviour and lifestyle (for example, whether an individual uses tobacco product or engages regularly in strenuous exercise) and facts about family history and genetic factors (for example, whether an individual has first-degree family members with a specific type of cancer or a propensity for musculoskeletal disease).

**Health status** is generally reported by individuals themselves. It reflects several domains of health such as physical functioning, mental and emotional well-being, cognitive functioning, social and role functioning, and perceptions of one's health in the past, present, and future and relative to peers.

As the database becomes more comprehensive, it is likely to comprise more recent and sensitive information about individuals. Hence, comprehensiveness inevitably has a direct correlation with concerns about privacy and confidentiality.

## Notice

A privacy notice is a public statement of how the entity applies data protection principles to processing personal information. It is a statement that describes how the entity collects, uses, retains, and discloses the personal information of an individual.

Examples of ways in which organisations might choose to provide a privacy notice include:

- Prominently displaying a brief notice at the check-in counter. This note can cover key information and individuals can be provided a more detailed notice in a leaflet.
- Including a privacy notice on a paper or online form used to collect patients' health information.
- Discussing the information orally during a consultation with a patient. To ensure that all relevant matters are covered, it would be useful to also provide the patient with a written notice in this situation.

## Data Collection

It means gathering, acquiring or obtaining personal information for inclusion in a record or generally available publication. In practice, health information about a patient is collected either directly through the patient or from another source, and then retained in the database.

Examples of data collection include:

Recording patients' inputs or recording your opinion about what a patient has said.

Requiring a patient to complete a form requesting details such as name, address, date of birth, and medical history.

Retaining a specialist report provided by a patient for inclusion in the patient's medical records.

Taking physical or biological samples from a patient and labelling these with the patient's name or other identifier.

Storing video footage, photographs or audio recordings in which a patient can be reasonably identified.

Retaining emails or other correspondence containing personal information about a patient.

## Consent

Consent is given explicitly, either orally or in writing, by an affirmative and unambiguous act. In the context of healthcare emergency services, non-consensual usage of personal data can potentially be carried out, deriving validity from the circumstances and the conduct of the patient.

Consent, as discussed in this guide, applies to patients' decisions about how organisations handle their health information. It does not refer to consent to receiving treatment. **In practice, consent to the handling of health information and consent to treatment often occur at the same time, though they are distinct actions by a patient to different things.**

**The key elements of consent are:**

It is given after the individual has been adequately informed.

It is obtained voluntarily.

It is obtained from an individual who has the capacity to understand and communicate consent.

It is current.

It is specific.

## De-Identification and Anonymisation

### De-identification

Personal data is de-identified once the information is no longer about an 'identifiable individual'.[6] Even though de-identified data cannot be connected to a particular individual; it is still considered 'personal data'. Generally, de-identification includes two steps:

- Removing personal identifiers such as name, address, date of birth or other information that can lead to identification.
- Removing or altering other information that may allow an individual to be identified, for example, due to a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

De-identification may not completely remove the risk of an individual being re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and mitigated. Relevant factors to consider when determining whether information has been effectively de-identified could include the cost, difficulty, practicality, and likelihood of re-identification.

### Anonymisation

Personal Data is anonymised when direct and indirect identifiers are removed or manipulated together with mathematical and technical guarantees to prevent re-identification. Generally, anonymisation should be carried out in a manner to prevent the following:

[6]In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information will allow the individual to be distinguished from others.

**Singling out**
This corresponds with the possibility of isolating some or all records that can potentially identify an individual in the dataset.

**Linkability**
This refers to the possibility of isolating some or all records that can potentially identify an individual in the dataset.

**Inferences**
This refers to the possibility of deducing, with significant probability, the value of an attribute from the values of a set of other attributes.

The anonymisation process must be irreversible in nature, in conjunction with the methods and techniques deemed acceptable by the appropriate regulator.

## Disclosure

Health information is disclosed when it is made accessible to others outside the main organisation and the subsequent handling of that information is released from the effective control of the main organisation that gathered or held the original data. This includes giving health information to a related body corporate.

Examples of disclosure include:


Sharing health information with another health service provider or individual.


Unintentionally providing health information to an unintended recipient.


Erroneously displaying a computer screen such that health information can be read by someone else, for example, at a reception counter or in an office.

## Processing

Health information is considered to be processed when it is handled, managed or used to undertake an activity within an organisation's effective control. Examples of processing include:


Accessing and reading a patient's medical file.


Searching electronic records for a patient's health information.


Making a treatment decision based on a patient's health information.


Sharing the information with other units within the organisation.

Processing covers all operations performed on personal data throughout its lifecycle within the effective control of an organisation.

# 5 PATIENT CENTRIC PRIVACY GUIDE

Developing a best practice guide for privacy requires a deep understanding of not just the regulatory and interoperability requirements, but also an understanding of the user. The purpose of adopting a patient centric approach is to promote specific improvements in privacy measures associated with patient interactions. Through this approach, we aim to highlight challenge areas in healthcare and provide actionable guidance to mitigate the impact of these challenges.

**Accurate and proportional data collection for patient identification:**

Healthcare service providers must strive to improve the process of collecting patients' personal data to ensure that only accurate and necessary information is collected from the patient.

**Effective patient communication:**

Healthcare service providers must provide the patient clear notification with respect to the nature and extent of utilisation, and the relevance of their personal data to the service(s) being provided.

**Informed patient consent:**

Healthcare service providers must take express patient consent through a clear and affirmative action-based manner.

**Use or disclosure of patient personal data:**

Healthcare service providers must use a patient's personal data only to the extent laid down in the purpose or to the extent of the consent provided by the patient.

**Securing patient personal data:**

Healthcare service providers must ensure security of the patient's personal data through administrative and technological controls.

**Enabling access to and correction of personal data:**

Healthcare service providers must allow patients' access to their personal data. This must be done without excessive expense or delay. Patients should also be empowered to request for amendments to their personal data to ensure that it is accurate, relevant, up to date, complete, and not misleading.

**Maintaining patient anonymity:**

Where lawful and practicable, patients should be given the option of not identifying themselves when dealing with health organisations.

# ACCURATE AND PROPORTIONAL DATA COLLECTION FOR PATIENT IDENTIFICATION

***Healthcare service providers must strive to improve patient personal data collection processes to ensure that only accurate and necessary information is collected from the patient.***

## Key Considerations

Healthcare service providers must ensure that relevant processes are established to improve the accuracy of the patient information being collected.

Health information should be collected only after obtaining the patient's explicit consent and only to the extent necessary for delivering healthcare services.

Personal information should be collected only by lawful and fair means (without being unreasonably intrusive).

Unsolicited information (received without asking) must be destroyed unless it would have been lawfully collected in the course of practice.

As per Rule 5(2) and Rule 5(3) of SPDI rules, information should be collected for a lawful purpose connected with a function or activity alone; the collection of such sensitive personal data or information should be considered necessary for that purpose.[7] The subject should also be informed about the nature of information being collected, the identity of the collecting agency, and the intended use of the information.[8]

## Measurable Elements

The personal data being collected should be necessary for the purpose of performing the function or activity.

The personal data being sought and collected must be relevant, accurate, not excessive, and not intrusive.

The personal data should be collected directly from the patient it relates to, as far as it is practical.

Relevant processes should be established to inform the patient about how the data may be used, who may access it, and the consequences of not providing it.

[7]Rule 5(2), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

[8]Rule 5(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

CASE STUDY

# Accurate and Proportional Data Collection for Patient Identification

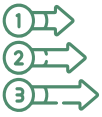
Lata had undergone a knee operation and is currently going through post-operative rehabilitation. Both the operation and the rehabilitation are done at the same hospital. At the time of admission, a set of patient identifiers were collected by the hospital from Lata. These consisted of basic identity details such as her name, data of birth and address, alongside her unique government issued identifier. Throughout the care journey, different health assessment data was collected and included in her medical records to provide a comprehensive picture of the treatment that she had received, and the treatment recommended.

At the hospital rehabilitation centre, she is once again asked to provide a government issued identifier before she can receive treatment. Such unstandardised data collection poses a risk to the accuracy of patient identification and uniformity of medical records and can be categorised as disproportionate.

# EFFECTIVE PATIENT COMMUNICATION

***Healthcare service providers must provide the patient clear notification with respect to the nature and extent of utilisation, and the relevance of their personal data to the service(s) being provided.***

## Key Considerations



Upon collecting health information, the healthcare service provider must take reasonable steps to notify the patient of such collection.

Notified information must include the service details, the purpose for which the information is collected, to whom the health information may be disclosed, and whether it will be disclosed to an overseas recipient (and if so, where).

As per Rule 4 of SPDI rules, a privacy policy for the handling of or dealing in personal information including sensitive personal data or information, should be displayed on the website of the entity and clearly communicated to the provider of information (data subject). This policy should be clear and easily accessible. Further, it should mention the type of personal or sensitive personal data or information being collected and the purpose of collection and usage of such information; disclosure of information including sensitive personal data or information as provided and reasonable security practices and procedures implemented.

## Measurable Elements

Entity should provide a notice which clearly states the type of personal information being collected from the user, especially if it is sensitive personal information like health information, financial information, etc. Notice should also mention the indirect sources of personal information.

Entity should provide a notice which clearly states the purpose of collecting the users' personal information.

Notice should communicate to the user if their personal Information is being transferred to another country and also the purpose of the transfer.

Notice should provide details of mechanism to report misuse/ breach of data privacy and also the contact point of the Grievance Officer for clarification and recourse.

Notice should inform the users of the personal Information retention mechanisms, the duration for which personal information will be retained, and the criteria used to determine the retention period.

Notice should state the information security and safeguard mechanisms deployed to protect the personal information.

CASE STUDY

# Effective Patient Communication

Uma is using an application to book an appointment at a pathology lab. Before asking her to fill her identification details i.e., name, date of birth, and government issued ID card a notification pops up, displaying the companies data usage policy. Uma notices that the policy mentions that her personal data can be used by the pathology lab for an undefined time period. Further, she notices that the same data can be shared with other allied companies of the pathology lab. To understand this better, she tries to locate the details of a grievance officer in the pop up. However, she is unable to find any mention of a grievance officer and only comes across a reference to a customer care email address.

A healthcare services application must take into consideration the apprehension users may have in sharing their data. Accordingly, they should maintain transparency around their activities through the notice and clearly communicate to the user the nature and extent of the usage of data. If the notice is opaque or not comprehensive, then there is a chance that the point of interaction for the user might become a point of friction. As a result, the application might lose an opportunity to cultivate trust.

# INFORMED PATIENT CONSENT

***Healthcare service providers must take express patient consent through a clear and affirmative action-based manner.***

## Key Considerations

Consent signifies any freely given, informed, and unambiguous indication of the data subject's wishes that signal an agreement to the processing of their personal information.

Consent can be obtained by a clear affirmative action.

To provide informed consent, patients must have sufficient information about their own healthcare and the ability to then make appropriate decisions.

However, express consent may not be practical in all instances of processing patient data. There are certain kinds of processing activities which necessitate the need for patients to provide their personal data through non-consensual grounds such as function of state, health emergency, etc.[10] These activities have found place in the discourse around non-consensual processing under the future personal data protection law in India. In the meantime, it is imperative that the healthcare service providers focus on operationalising express informed consent for patients.

## Measurable Elements

Entity should take explicit consent from users that signal their agreement with the privacy policy/notice for the collection of optional/additional personal data which isn't necessary for providing the service.

Entity should clearly demarcate mandatory and optional data when collecting data from the user. Optional data are those data points which are not critical for the service provided by the entity.

For optional/ additional personal data collected from the user, there should be an option to withdraw consent at any point of time and the process to withdraw consent should be easily available and communicated to the user in advance. The request to withdraw consent should be completed within a reasonable amount of time.



[9]Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

[10]Clause 12, The Personal Data Protection Bill, 2019.

CASE STUDY

# Informed Patient Consent

Ashok visits his neighbourhood clinic for a check-up. In the waiting room, he is given a form by the receptionist in which he is required to fill in his personal details along with information regarding his health status. As he is about to finish filling up the form he notices that at the end of the form it is written that the clinic reserves the rights to use this information for assessment and business purposes. He checks the form to see if any information has been provided to explain the usage for business purposes. Unable to find an explanation, he goes up to the receptionist to seek clarification. The receptionist is neither able to answer his query nor is willing to direct him to another individual who can provide an explanation.

The clinic in question failed to provide a clear and complete explanation with respect to the usage of a patient's personal data. Hence, consent obtained by the clinic in this scenario cannot be characterised as informed consent. Obtaining informed consent often requires a special effort to ensure that information is being presented in a way that the patient can understand.

# USE OR DISCLOSURE OF PATIENT PERSONAL DATA

***Healthcare service providers must use patient personal data only to the extent laid down in the purpose or to the extent consented to by the patient.***

## Key Considerations

The primary purpose for collecting health information is to provide healthcare services. Any usage and disclosure of health information should serve this primary purpose.

Health information may be used or disclosed for another 'secondary' purpose in the following instances:

- Where the patient provides explicit consent.
- Where the patient would reasonably expect a use or disclosure related to their healthcare.
- When it is required or authorised by or under law.

The framework laid down under section 43A of Information Technology Act, 2000, clubs the purpose and usage limitation principles under Rule 5 (5). As per this rule, the information collected should be used for the purpose for which it has been collected.[11]

As per Rule 6, disclosure of sensitive personal data or information by the entity any third party shall require prior permission from the provider of such information, unless such disclosure has been agreed to in the contract between the body corporate and provider of information or where the disclosure is necessary for compliance with a legal obligation.[12]

## Measurable Elements

The personal data collected by the entity from the patient is used for the same purposes and context as mentioned in the privacy notice.

Personal data shall be processed only for purposes that are clear, specific, and lawful.

Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.



[11]Rule 5(5), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

CASE STUDY

# Use of Patients' Personal Data

Seema has been visiting the same hospital for many years. Recently, she suffered a stroke and now has to contend with stroke related complications, some of which are likely to be permanent. Seema's healthcare will need a coordinated effort between the healthcare professionals treating her, including her neurologist, rehabilitation team, and practice nurse. Her doctor organises a consultation with her to discuss the benefits of multidisciplinary care so that she can make an informed decision to allow the disclosure of her health information to other health practitioners.

The doctor carefully notes the conversation and records Seema's express consent. Seema's doctor recognises that the primary purpose for using Seema's health information is for him to treat and manage her stroke symptoms. Seema would expect this use as part of her regular healthcare. However, it cannot be assumed that Seema would expect her health information to be disclosed to other health practitioners. This disclosure by Seema's doctor may be considered a secondary purpose, for which Seema's express consent is necessary.

# SECURING PATIENTS' PERSONAL DATA

***Healthcare service providers must ensure the security of the patient's personal data through the relevant administrative and technological controls.***

## Key Considerations

Secure the personal health data in custody to avoid misuse, interference, loss, and unauthorised access, modification or disclosure.

Destroy or de-identify/anonymise personal health data that is no longer needed.

Data Protection Impact Assessment should be undertaken to identify processes involving new technologies or large-scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processes that carry the risk of significant harm to individuals.

**Reasonable security practices should at least include the following:**

Information Communication Technology (ICT) security.

Access security.

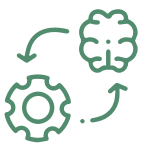
Evaluation of third-party providers.

Data breaches reporting and handling.

Physical security.

Destruction and de-identification.

Implementation of acceptable national/ international security standards.



Healthcare service providers must strive to embed privacy and security by design in their organisation. Managerial, organisational, business practices, and technical systems should be designed in a manner to anticipate, identify, and avoid harm to the individual.

As per Rule 8, the entity must implement relevant security practices and standards, have a comprehensive and documented information security programme, and establish information security policies that contain managerial, technical, operational, and physical security control measures that are commensurate with the information assets.[13]

As per Rule 5(4), sensitive personal data or information should not be retained for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.[14]

## Measurable Elements

Security controls should be deployed to protect and secure personal data during the various stages of the information lifecycle including collection, processing, transmission, storage, and disposal.

Security controls should be deployed to protect the confidentiality, integrity, and availability of personal data during storage.

Security controls should be deployed to protect and secure personal data during data transmission.

Secure coding practices to be adopted in order to ensure that only required permissions are requested from users. Root level access of the device should not be requested from the user. Further, passwords should not be hard coded (if the organisation uses a healthcare application)

Security safeguards should be deployed by the entity to protect users' personal health information in line with the details provided in the notice.

Retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is collected.

Undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.

Where it is not necessary for personal data to be retained, such personal data must be deleted.

Data Protection Impact Assessment should be conducted for high-risk processing activities.

Steps should be taken to operationalise Privacy by Design and Security by Design.

[13]Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

[14]Rule 5(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

CASE STUDY

# Securing Patients' Personal Data

'VISION' is a leading chain of hospitals in India and is a pioneer in the usage of technology to support healthcare services. VISION collects patient data from multiple access points including multiple direct interface points and in various formats. Data once collected is then ported to a centralized database. It also strives to improve its prospects through strategic alliances with key partners - for enhancing customer experience and for improving business opportunities - offering many value-added products and services. Patient health data is shared to achieve this goal by enabling the employees of the strategic partners/ third party service providers to access such data.

It is imperative that VISION ensures that the following are in place to safeguard patient data:

- Create visibility on how personal data is handled across business processes, functions, and operations of the organization.
- Create a map of the users, identifying their roles, that have access to the data against each set of data elements. Validate the access against the access requirements to execute the intended data transaction.
- Ensure that a mechanism exists for quick and efficient provisioning, de-provisioning, and authorisation of access to the information or systems which are exposed to the data.
- Ensure that the relevant technical measures are deployed to detect or report the privacy incidents.
- Ensure that a documented information security policy is in place within the organisation, covering internal and external stakeholders.

# ENABLING ACCESS TO AND CORRECTION OF PERSONAL DATA

***Healthcare service providers must enable patients to access their personal data. This should be done without excessive expense or delay. Patients should also be empowered to request for amendments to their personal data to ensure that it is accurate, relevant, up to date, complete, and not misleading.***

## Key Considerations

Patients must have access to all their personal health information held by the health service providers, subject to statutory limitations.

Healthcare service providers must take reasonable steps to correct the patient health information in their custody if that information is inaccurate, out of date, incomplete, irrelevant or misleading or at the request of the patient.

Healthcare service providers must respond to requests for access within a reasonable time period.

Relevant processes should be established to verify the identity of the requesting patient.

Refusal to grant access must be communicated in writing with supporting reasons. Further, there should be a process for lodging a complaint with a grievance officer.

Through these rights, users can make a specific request and be assured that their personal information is not being misused for purposes other than those for which consent has been provided. As per Rule 5(6), only the right to access and correct has been extended to the data subject.[15]

As per rule 5(9), the entity shall designate a grievance officer and publish his name and contact details on its website. The grievance officer shall redress the grievances expeditiously, within one month from the date of receipt of grievance.[16]

## Measurable Elements

Users shall have the right to access their personal information collected by the entity in a structured, machine-readable format.

Users should be able to access and modify their personal information as and when needed.

The process to access and correct information should be clearly communicated to the user.

Entity shall establish relevant procedures and effective mechanisms to address the grievances of individuals efficiently and in a speedy manner.

The mechanism should provide redressal in a defined time period.

The grievance officer/ data protection officers' contact information should be displayed in the privacy notice of the entity.

[15]Rule 5(6), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

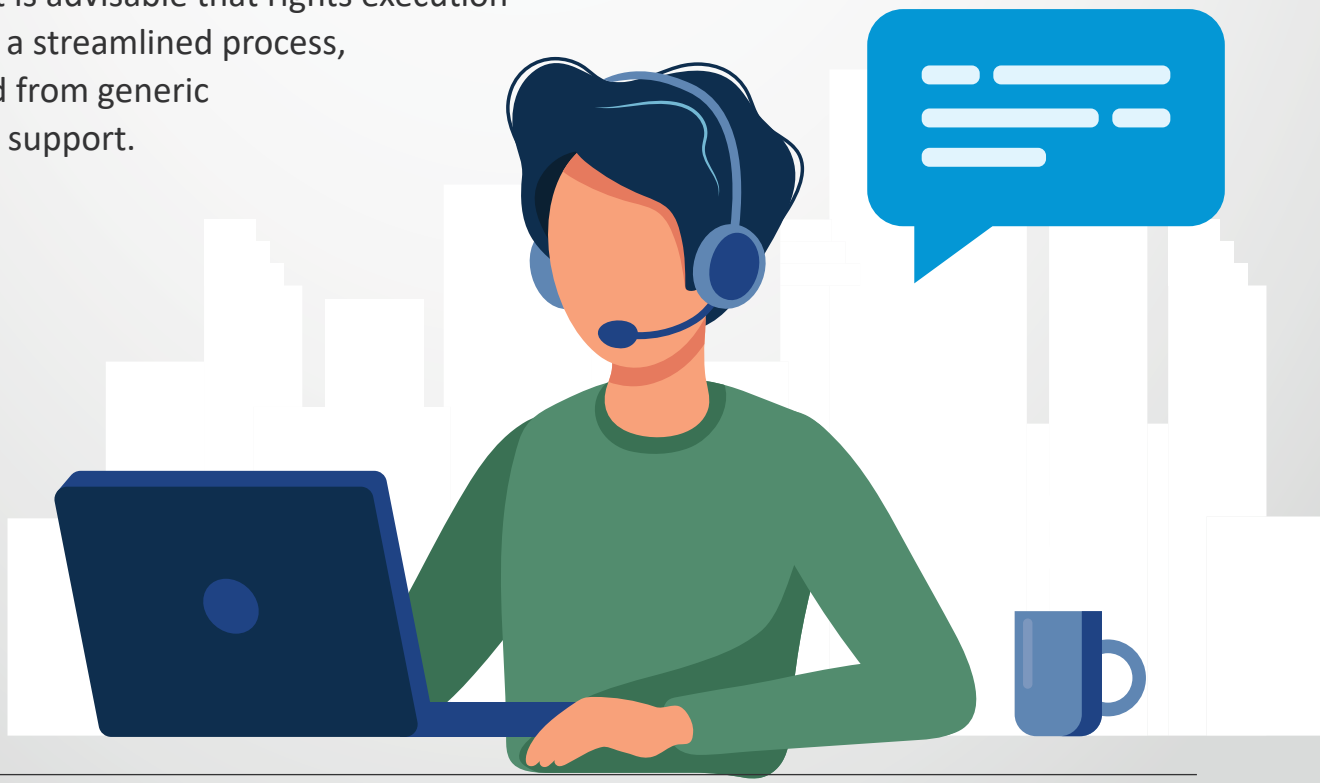
[16]Rule 5(9), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

***CASE STUDY***

# Enabling Access to and Correction of Personal Data

Lalit had undergone a treatment at a well-known medical facility. Now, he wishes to access his medical records that are held by the said medical facility. Unable to find a standard process for handling access requests on the medical facility's website or application, he is forced to reach out to the customer support services. The customer support service is unaware of any such right and nor has an established process to transfer such requests to a grievance department. Lalit's request is dismissed. Upset by this occurrence, Lalit takes to social media to narrate his experience and highlights the gaps in the medical facilities' rights handling processes.

The medical facility should have established a mechanism to handle access and correction requests from patients in a timely manner. The details of the department/ personnel that can be contacted for the evaluation and execution of patients' privacy rights should have been clearly mentioned on the privacy note. Further, it is advisable that rights execution is built as a streamlined process, separated from generic customer support.



# MAINTAINING PATIENT ANONYMITY

***Where lawful and practicable, patients should be given the option of not identifying themselves when dealing with health organisations.***

## Key Considerations

Attribution of personal health data to a unique patient is necessary for the provision of healthcare services. However, considering the sensitivity attached to personal health information, service providers must offer the option of anonymity and pseudonymity as a usual practice, where practical.

Healthcare service providers must also actively adopt acceptable methods of de-identification and anonymisation to reduce the risk associated with processing patient health data, especially with respect to genetic data or children's data.

## Measurable Elements

An option has been provided to the patient to remain anonymous or pseudonymous during the treatment process.

Organisation has adopted acceptable anonymisation/de-identification techniques.

Organisation has performed tests to gauge the possibility of re-identification of data.

CASE STUDY

# Maintaining Patient Anonymity

Suresh is 16 years old and has been addicted to smoking for the past 3 years. He wants to quit smoking but is uncomfortable bringing it up with his parents as he is unsure of how they would react. A friend of his shares with him the contact of a telephonic service that offers assistance in quitting smoking. Still apprehensive, he decides to call the assistance hotline for help.

The counsellor tells Suresh that his identity would be kept anonymous and the details of sessions won't be shared with anybody, without his consent.

In such scenarios, the healthcare service providers and associated health advice and counselling service providers, must give the user the option of remaining anonymous. The data collected as part of such services should also be kept in anonymised form, protected against any risk of re-identification.

# PATIENT CENTRIC PRIVACY SELF-ASSESSMENT GUIDE

1

## Actionable Area

Accurate and proportional data collection for patient identification

## Standard

*Healthcare service providers must strive to improve patient personal data collection processes to ensure that only accurate and necessary information is collected from the patient.*

## Assessment Elements

- [ ] The collection of personal data should be necessary to perform the function or activity.
- [ ] The personal data being sought and collected must be relevant, not excessive, accurate, and not intrusive.
- [ ] Personal data should be collected directly from the patient it relates to, as far as it is practical.
- [ ] Processes should be established to inform patients about how their data may be used, who may access it, and the consequences of not providing it.

## Implementation References

### Indian Statute

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 5(2)
- Rule 5(3)

### Standard

Unavailable

### Framework

DSCI Principle Based Assessment Framework-

- Collection limitation

2

## Actionable Area

Effective patient communication

## Standard

*Healthcare service providers must provide the patient clear notification w.r.t the nature and extent of utilisation, and relevance of their personal data to the service(s) being provided.*

## Assessment Elements

- ☐ Entity should provide a notice which clearly states the type of personal information being collected from the user, especially when related to sensitive personal information like health information, financial information, etc. Notice should also mention the indirect sources of personal information.
- ☐ Entity should provide a notice which clearly states the purpose of collecting the users' personal information.
- ☐ Notice should communicate to users if their personal Information is being transferred to another country and also the purpose of the transfer.
- ☐ Notice should provide details of mechanisms to report misuse/ breach and also the contact point of the grievance officer for clarification and recourse.
- ☐ Notice should inform the users of the personal information retention policy, the duration for which personal information is retained, and the criteria used to determine the retention period.
- ☐ Notice should state the information security and safeguard mechanisms deployed to protect the user's personal information.

## Implementation References

**Indian Statute**

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 4

**Standard**

Unavailable

**Framework**

a) DSCI Principle Based Assessment Framework-

- Notice

b) DSCI Privacy Framework-

- Privacy Policy & Procedures (PPP)

3

## Actionable Area

Informed patient consent

## Standard

*Healthcare service providers must take express patient consent through a clear and affirmative action-based manner.*

## Assessment Elements

- [ ] Entity should take consent from the users that signal their agreement with the Privacy Policy/Notice for collection of optional/additional personal data which isn't necessary for providing the service.
- [ ] Entity should clearly demarcate mandatory and optional data when collecting data from the user. Optional data are those data points which are not critical for the service provided by the entity.
- [ ] For optional/ additional personal data collected, the user should have the option to withdraw consent at any point of time and the process to withdraw consent should be easily available and communicated to the user in advance. The request should be addressed within a reasonable amount of time.

## Implementation References

**Indian Statute**

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 5

**Standard**

Unavailable

**Framework**

DSCI Principle Based Assessment Framework-

- Consent

4

## Actionable Area

Use or disclosure of patient personal data

## Standard

*Healthcare service providers must use patient personal data only to the extent laid down in the purpose or to the extent consented to by the patient.*

## Assessment Elements

- [ ] The personal data collected by the entity from the patient is used for the same purposes and context as mentioned in the privacy notice.
- [ ] Personal data should be processed only for purposes that are clear, specific, and lawful.
- [ ] Personal data should be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.

## Implementation References

**Indian Statute**

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 5(5)
- Rule 6

**Standard**

Unavailable

**Framework**

DSCI Principle Based Assessment Framework-

- Use limitations
- Disclosure to third parties

5

## Actionable Area

Securing patient personal data

## Standard

*Healthcare service providers must ensure security of the patient personal data through administrative and technological controls.*

## Assessment Elements

- [ ] Security controls should be deployed to protect and secure personal data during the various stages of the information lifecycle including collection, processing, transmission, storage, and disposal.
- [ ] Security controls to be deployed to protect the confidentiality, integrity, and availability of personal data during storage.
- [ ] Security controls to be deployed to protect and secure personal data during data transmission.
- [ ] Secure coding practice to be adopted in order to ensure that only required permissions are requested from users. Root level access of the device should not be requested from the user. Passwords should not be hard coded. (if the organisation uses a healthcare application)
- [ ] Security safeguards should be deployed by the entity to protect users' personal health information in line with the details provided in the notice.
- [ ] Personal data should be retained for only as long as may be reasonably necessary to satisfy the purpose for which it is processed.
- [ ] Undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.
- [ ] Where it is not necessary for personal data to be retained, such personal data must be deleted.
- [ ] Data Protection Impact Assessment should be conducted for high-risk processing activities.
- [ ] Steps should be taken to operationalise Privacy by design and Security by Design.

## Implementation References

**Indian Statute**

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 5(4)
- Rule 8

**Standard**

ISO 27701: 2019

- Clause 5.2.3
- Clause 5.2.4

**Framework**

a) DSCI Principle Based Assessment Framework-

- Security

b) DSCI Privacy Framework

- Visibility over Personal Information (VPI)
- Personal Information Security (PIS)
- Information Usage & Access (IUA)
- Privacy Monitoring & Incident Management (MIM)

6

## Actionable Area

Enabling access and correction of patient personal data

## Standard

*Healthcare service providers must enable patients' access to personal data about them. This must be done without excessive expense or delay. Patients should also be empowered to request that their personal data be amended to ensure that it is accurate, relevant, up to date, complete and not misleading.*

## Assessment Elements

- [ ] Users shall have the right to access their personal information collected by the entity in a structured, machine-readable format.
- [ ] Users should be able to access and modify their personal information as and when needed.
- [ ] The process for access and correction should be clearly communicated to the user.
- [ ] Entity shall establish proper procedures and effective mechanisms to efficiently and speedily address grievances.
- [ ] The mechanism should provide redressal in a defined time period.
- [ ] The Grievance officer/ Data Protection Officers' contact information should be displayed in the privacy notice of the entity.

## Implementation References

**Indian Statute**

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Rule 5(6)
- Rule 5(9)

**Standard**

Unavailable

**Framework**

a) DSCI Principle Based Assessment Framework-

- Access & Correction

6

## Actionable Area

Maintaining patient anonymity

## Standard

*Where lawful and practicable, patients should be given the option of not identifying themselves when dealing with health organisations.*

## Assessment Elements

- [ ] Patient should be provided with an option to remain anonymous or pseudonymous during the treatment process.
- [ ] Organisation has adopted acceptable anonymisation/de-identification techniques.
- [ ] Organisation has performed tests to gauge the possibility of re-identification of data.

## Implementation References

| Indian Statute | Standard | Framework/ Code |
|---|---|---|
| - | - | • Anonymisation: managing data protection risk code of practice, UK Information Commissioner's Office<br>• Guide to basic data anonymisation techniques, Personal Data Protection Commission-Singapore<br>• Opinion 05/2014 on Anonymisation Techniques, Article 29 Working Party |

# REFERENCES


1. Justice K.S. Puttaswamy v. Union of India & Ors, (Writ Petition (Civil) No 494 Of 2012)
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
3. The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019)
4. Health data management policy, National Digital health mission (2020) available at: **https://ndhm.gov.in/documents/HealthDataManagementPolicy**
5. Joint Commission International Accreditation Standards for Hospitals including Standards for Academic Medical Center Hospitals 7th edition. (2020)
6. DSCI Privacy Framework, Data Security Council of India (2010)
7. DSCI Principles Based Assessment Framework, Data Security Council of India (2012)
8. Electronic Health Record (EHR) Standards for India (2016) available at: **https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf**
9. Privacy and managing health information in general practice, Royal Australian College General Practitioners (2017) available at: **https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Protecting%20practice%20information/Privacy-and-managing-health-information-in-general-practice.pdf**
10. Privacy Manual for Health Information, New South Wales, Ministry of Health (2015) available at: **https://www.health.nsw.gov.au/policies/manuals/Documents/privacy-manual-for-health-information.pdf**
11. Guide to Health Privacy, Australian information Commissioner (2019), Available at: **https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-health-privacy/guide-to-health-privacy.pdf**
12. Anonymisation: managing data protection risk code of practice, UK Information Commissioner's Office (2012) available at: **https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf**
13. Guide to basic data anonymisation techniques, Personal Data Protection Commission-Singapore (2018) available at: **https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf?la=en**
14. Opinion 05/2014 on Anonymisation Techniques, Article 29 Working Party (2014) available at: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf**

## Acknowledgement

On behalf of DSCI, we would like to extend our heartfelt gratitude to all the organizations and individuals for their valuable time and support without which this guide would not have been possible. This guide is the result of directions and expert inputs of our esteemed advisory group, consisting of Ms. Deanna DiCarlantonio, Data Protection Officer, United Health Group; Mr. Kumar KV, Chief Information Officer, Narayana Health Group; Mr. Jeyaseelan Jeyaraj, Senior Director, Health Sciences, Oracle Corporation; Mr. Arvind Sivaramakrishnan, Chief Information Officer, Apollo Hospitals and Mr. Suprio Dasgupta, Chief Data Privacy Officer, Dr Reddy Labs.

We would also like to thank Omidyar Network India for their support.

## About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: **www.dsci.in**

## Supported By

Omidyar Network India invests in bold entrepreneurs who help create a meaningful life for every Indian, especially the hundreds of millions of Indians in low-income and lower- middle-income populations, ranging from the poorest among us to the existing middle class. To drive empowerment and social impact at scale, we work with entrepreneurs in the private, non-profit and public sectors, who are tackling India's hardest and most chronic problems. We make equity investments in early-stage enterprises and provide grants to non-profits in the areas of Digital Identity, Education, Emerging Tech, Financial Inclusion, Governance & Citizen Engagement, and Property Rights. Omidyar Network India is part of The Omidyar Group, a diverse collection of companies, organizations, and initiatives, supported by philanthropists Pam and Pierre Omidyar, founder of eBay.


**www.omidyarnetwork.in**


A NASSCOM® Initiative

# DATA SECURITY COUNCIL OF INDIA

**NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303**

**For any queries, contact:**

P: +91-120-4990253 | E: info@dsci.in | W: www.dsci.in

DSCI_Connect  dsci.connect  dsci.connect

data-security-council-of-india  dscivideo