



A **NASSCOM**® Initiative

COVID-19 DATA PRIVACY OUTLOOK

DSCI Advisory



Introduction

The world today grapples with the COVID-19 pandemic and nations, businesses and individuals are working incessantly to keep the fight going on all fronts, including but not limited to, healthcare, economy, operations, essential services and supply chain. A cautious but formidable approach is indeed being adopted by all governments, authorities and other stakeholders. Amidst all this, data privacy assumes new dimensions as large amount of health related and other personal data is being collected and shared, of individuals, who have been potentially affected by the pandemic or who may be potential carriers or transmitters of the virus (contact tracing), are being tracked.

World over, the Data Protection regulators are unanimous over the fact that no Data Protection legislations, guidelines or rules should be an impediment to the management of this infectious disease. However, it does make sense to be mindful of the fundamental tenets and principles of Data Privacy, to strike a fine balance, even in these unprecedented times.

The DSCI Privacy Outlook endeavours to reflect upon and succinctly capture the Privacy implications of COVID-19 for different set of stakeholders and touch upon some of the basic hygiene focussed Privacy and Data Protection practices. Although DSCI has come out with a few advisories that cater to the Cyber Security aspects in context of Work from Home for organizations, and other Industry specific security guidelines; this document looks at the Data Protection piece of the puzzle.



Healthcare Privacy Considerations

The Indian Healthcare sector is although at par with international standards in its methods of diagnosis, treatment and the use of contemporary technology, is still nascent in the nature and extent of its interaction with data privacy considerations. The following present few considerations that healthcare service providers should keep in mind during the provision of services and especially during public health emergencies.

- Notify the patient of all types of information that is collected, in terms of both personal data as well as medical history.
- Have specific protocols in place to ensure that the consent of the patient is taken at every stage of the procedure.
- The patient should have an option of refusal for providing any information that may not be mandatorily required for the treatment.
- The information collected from the patient is used solely for the purpose that the patient has been informed of.
- Medical records of the patient can only be disclosed to authorized agencies with the prior approval of patient.
- Have internal and external audit mechanisms in place to check the efficacy of privacy measures.



Expectations from Governments & Agencies

All government departments, authorities and agencies are at the forefront of the crisis management and containment. Constant efforts are being undertaken to identify the affected individuals and the people they might have come in contact with. This process inevitably entails collection of personal data of individuals from different sets of stakeholders. In the context of data collection, it is vital that the internationally recognised Privacy principles and practices are adhered to. The authorities, while collecting the data, must take cognizance of the fundamental principles of collection limitation and use limitation so as to ensure that collection of personal data is necessary and proportionate to achieve a specified and legitimate aim that is consistent with the tenets of data privacy.

- 
- Majority usage of personal data should be made once it's been converted to Aggregated Non-Identifiable Data.
- 
- Maintain transparency with the public about the usage of personal and Aggregated Non-Identifiable Data and the applicable legal framework. Usage of such data should be lawful and fair.
- 
- Clearly describe the purpose for which personal and Aggregated Non-Identifiable Data is being shared and prevent it from being re-used for any alternative purpose not related to combatting the spread of COVID-19.
- 
- Enforce a strict rule prohibiting the re-identification of Aggregated Non-Identifiable Data, except as permitted by law and with notice to the identified individuals.
- 
- Conduct a data privacy impact assessment in respect of any Aggregated Non-Identifiable Data received.
- 
- Delete any Data collected from individuals after a defined period or once it is no longer needed for the agreed health-related purpose.
- 
- Provide evidence that they have acted in accordance with the assurances given. Establish an independent oversight board to monitor adherence to these principles.

Work from Home considerations for Employers and Employees

Majority of the organizations, for the first time, have adopted policies and remote work practices which requires their employees to completely work from home. This presents a new set of challenges for the employers who must strategize to take care of the Data Protection implications arising out of these novel operating models. Also, some of the employers may have the onus of collection and usage of personal health related data of the employees, which again entails Privacy considerations.

The principles of proportionality, Transparency, Accountability assume special significance in the current context.



Perspective for Employers

- Organizations need to revisit their Data Protection strategies and ensure that the personal data being managed by it always remains secured.
- It is also vital for organizations to remain in conformance with the statutory obligations such as the EU GDPR, HIPAA and other data protection legislations that arise from handling customer data. Employers are expected to implement reasonable safeguards to protect the personal data.
- It may behoove businesses to carry out Data Protection Impact Assessment (DPIA) to clearly ascertain the risks to the rights and freedom of their employees, customers and business partners. The exercise may assist organizations in identification of the necessary technical and other controls that would always need to be implemented in order to safeguard the data.
- Privacy awareness and sensitization trainings need to be conducted for the employees so that they can sense the sensitivity of information and are always cognizant and mindful of data obligations and liabilities.

Perspective for Employees

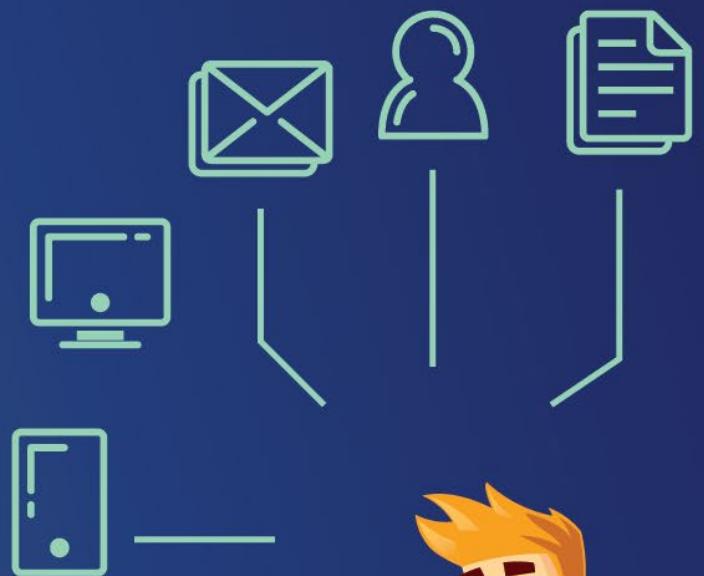
- Employees have a rather bigger responsibility to be in absolute compliance with Data Protection and Data Privacy principles.
- Extra caution needs to be exercised by the employees entrusted with Personal data of customers. A conscious effort must be made by all employees to avoid becoming the reason of data leakage.
- Essentially, employees must impart utmost care towards upholding and respecting the rights associated with Data.
- Employees must maintain adherence to statutory compliances emanating from handling customer data from various geographies.



A **NASSCOM**® Initiative

Data Security Council of India

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



[dsci.connect](#)



[DSCI Connect](#)



www.dsci.in



[dsci.connect](#)



[dscivideo](#)



[Data-Security-Council-of-India](#)

