GOVERNMENT OF NCT OF DELHI
DELHI DISASTER MANAGEMENT AUTHORITY

No. DDMA/COVID-19/2020/215 Dated: 03.06.2020

ORDER

Whereas, the Delhi Disaster Management Authority (DDMA) is satisfied that the NCT of Delhi is threatened with the spread of COVID-19 epidemic, which has already been declared as a pandemic by the World Health Organization, and has considered it necessary to take effective measures to prevent its spread in NCT of Delhi;

And whereas, Delhi Disaster Management Authority has issued various orders/instructions from time to time to all authorities concerned to take all required measures to appropriately deal with the situation;

And whereas, it has been understood that the persons of the age of 60 years and above are more vulnerable to a severe COVID-19 infection, especially if they have a co-morbid condition such as hypertension, diabetes, asthma or cancer; necessitating additional measures to protect them from catching the infection;

Now therefore, in exercise of powers conferred under Section 22 of the Disaster Management Act, 2005; the undersigned, in his capacity as Chairperson, State Executive Committee, DDMA, GNCTD, hereby directs following authorities to take action for pre-emptive identification and protection of senior citizens from COVID-19, **as per annexed Standard Operating Procedure (SOP) (Annexure-I)** including the following directions:

(a) Office of Divisional Commissioner shall collect the available database of senior citizens from various departments of GNCT of Delhi such as Food & Supply Department (ration card holders as well as those without ration cards registered on *jantasamvaad* portal), Social Welfare Department (Old age Pension), all three Municipal Corporations as well as NDMC, and Delhi Police. Such departments shall provide this database in soft copy to the office of Divisional Commissioner immediately. This database shall be populated on the portal (Senior Citizens Portal) after de-duplication through the IT team.

(b) The IT Team of the office of the Divisional Commissioner, GNCTD shall be responsible for development and maintenance of web-based portal (Senior Citizens Portal) and a Dashboard as per the guidelines prescribed in annexed SOP for this purpose and shall grant access of the same to all BLOs and District Nodal Officers at control room. The IT team shall carry out the data analysis and shall generate & provide list of "at high-risk patients" and other useful actionable reports / data to District Nodal Officers / BLOs. Shri Sandeep Jain, Scientist, NIC shall assist the IT Team of Office of Divisional Commissioner in the said work.

(c) The Divisional Commissioner Office will adhere to the general guidelines for securing identity information and sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000, issued by Department of Information Technology on 11.09.2018. Copy of the general guidelines is enclosed as **Annexure-II**.

(d) Booth Level Officers (BLOs) who have also been appointed as "Corona Foot Warriors" for health surveillance, shall be allocated mobile numbers of a set of senior citizens. They shall call up their respective set of numbers; gather all requisite information in respect of "Senior Citizen Form" and upload the same on the web-based portal. BLOs will be responsible for their catchment areas and frequently call and check the health condition of the senior citizens and shall update the details on the portal and take further action as per annexed SOP. It is clarified that they shall not visit the residence of senior citizens and shall collect/gather this information through phone only.

(e) A dedicated call number shall be operationalized by office of Divisional Commissioner where such senior citizens who wish to register their details on the portal (Senior Citizen Portal) may give a missed call. The repository/database of these numbers would be allotted to the concerned BLOs who shall call up these senior citizens and help them by registering their details on the portal on their behalf.

(f) A 24x7 Control Room (in three shifts) shall be established in each District for this purpose, which will be headed by District Social Welfare Officer as the Nodal Officer who will report to the DM concerned. The Control Room will have the Dashboard depicting details uploaded on the portal. The Nodal Officers and medical/paramedical professionals will monitor the Dashboard and shall take required action as per annexed SOP as well as according to the protocol laid down by the H&FW Department, GNCTD for dealing with such patients. The duties of the Control Room are described in annexed SOP.

(g) H&FW Department, GNCTD shall depute 2-3 medical/paramedical professionals in each shift at District Control Rooms who shall assist the Nodal Officers to monitor the "at high-risk" persons. They will study the dashboard and take necessary cognisance of critical changes in the database. If any adverse development or symptoms of COVID-19 are noticed in any senior citizen, the control room shall strictly follow the protocol laid down by the H&FW Department, GNCTD for dealing with such patients.

(h) Health & Family Welfare Department shall also establish a state level Centralized Control Room (24x7) with a toll-free number to supervise as well as provide support and assistance to the District Control Rooms. This Control Room shall also be responsible to provide adequate telemedicine services, particularly in tertiary care, to the needy Senior Citizens in accordance with the guidelines laid down in this regard.

(i) The Office of the Divisional Commissioner will conduct training of all BLOs / District Nodal Officers/ medical/paramedical professionals and other ground staff involved in

this process. Health & Family Welfare department shall assist in the same. NGOs may also be engaged for imparting training.

(j) Targeted messaging to old persons for awareness and education campaigns shall also be carried out by the IT Team of the office of the Divisional Commissioner, GNCTD.

(k) The Revenue Department shall strengthen the 1077 system with graded increase in personnel and call lines as is necessary to cope up with the requirement, as the same has been notified as the dedicated senior citizen helpline of GNCTD.

(l) Reputed NGOs/Civil Society Organisations working in this field may also be engaged by the Revenue Department on a pro-bono basis at any stage wherever deemed appropriate for collaboration and partnership.

Encl: - As above.

(Vijay Dev)
Chief Secretary, Delhi

Copy for compliance to:

1. Commissioner of Police, Delhi
2. Pr. Secretary (Social Welfare), GNCTD
3. Chairperson, NDMC
4. Pr. Secretary (Revenue)-cum-Divisional Commissioner, Delhi.
5. Pr. Secretary (H&FW), GNCTD
6. Commissioner (SDMC/EDMC/North DMC)
7. All District Magistrates of Delhi.
8. Shri Sandeep Jain, Scientist, NIC.
9. All District Social Welfare Officers, GNCTD
10. All BLOs/ Corona Foot Warriors (through DMs concerned)

Copy for information to:-

1. Pr. Secretary to Hon'ble Lt. Governor, Delhi.
2. Addl. Secretary to Hon'ble Chief Minister, Delhi.
3. Secretary to Hon'ble Dy. Chief Minister, Delhi.
4. Secretary to Hon'ble Health Minister, Delhi.
5. Secretary to Hon'ble Labour Minister, Delhi.
6. Secretary to Hon'ble Transport Minister, Delhi.
7. Secretary to Hon'ble Social Welfare Minister, Delhi.
8. Secretary to Hon'ble Food & Supply Minister, Delhi.
9. Addl. Chief Secretary (Home), Delhi.
10. System Analyst, O/o Divisional Commissioner, Delhi for uploading the Order on website of Delhi Government.
11. Guard File.

Annexure-I

GOVT. OF NCT OF DELHI

Standard Operating Procedure (SOP) for Pre-emptive identification and Protection of Senior Citizens from COVID-19

COVID-19

The Coronavirus Disease of 2019 (COVID-19) is an infectious viral disease that is caused by a string of the coronavirus known as the SARS-Cov-2. The first known case was discovered in late 2019 from Wuhan, China. The disease is highly infectious and has caused a global pandemic with over 74,281 infections and 2,415 deaths in India as of May 13, 2020. Globally, nearly 4.3 million people have been infected and 2,94,511 have tragically died. The cases are continuing to rise globally, especially in India. The National Capital Territory of Delhi currently has the fourth highest number of cases among all States and highest among cities. The fatality rate in Delhi though remains at one of the lowest at 1.32% of detected infections. It is imperative that the fatalities be kept under check by protecting the citizenry most vulnerable to catching a severe infection.

Vulnerability of Senior Citizens

Research into the disease suggests that adults 60 years and older are more likely to have a severe COVID-19 infection, especially if they have a co-morbid condition such as hypertension, diabetes, asthma or cancer. GNCTD has, therefore, identified as its top priority, efforts to pre-emptively identify such persons and undertake all necessary steps to protect them from catching the infection.

Process for Pre-emptive Action:

1. A web-based portal and a dashboard shall be developed by IT team of the Office of Divisional Commissioner. This Portal shall contain an application form i.e. 'Senior Citizen Form', consisting of following **mandatory** fields:
    a) Name
    b) Mobile Number
    c) Address
    d) Pin Code

e) Age
f) Gender
g) Assembly Constituency No. (as mentioned in Voter ID card)
h) Polling Station No. (as mentioned in Voter ID card)
i) Co- morbidities*
j) Any COVID-related symptoms*
k) Whether has been in contact with someone who has tested positive for COVID-19 (Yes/No)
l) Are you residing with your children (Yes/No)
m) Kind of assistance required by you during COVID-19 (Grocery/Medicines/ Others)?
n) Have you downloaded "Aarogya Setu" App? (Yes/No)

(*To be determined in consultation with Department of H&FW, GNCTD).

2. Data on Portal to be populated through the available database from wherever available. At initial stage, the data (along with mobile number) of Delhi residents of the age of 60 years and above, available with various departments of GNCT of Delhi such as Food & Supply Department (ration card holders as well as those without ration cards registered on *jantasamvaad* portal), Social Welfare Department (Old age Pension), all three Municipal Corporations as well as NDMC, and Delhi Police, through system of Beat Constables and Senior Citizen Scheme, shall be obtained for this purpose after de-duplication. If data of more than 18 lakhs senior citizens registered in the electoral rolls of Delhi will be received from ECI/CEO, Delhi; it would also be populated on the portal, AC and PS wise.

3. (a) GNCTD has appointed 13,800-odd teams led by Booth Level Officers (BLOs) as "Corona Foot Warriors" at the beginning of the crisis. One of the primary tasks of the "Corona Foot Warriors" is health surveillance within their areas. In the absence of polling-station wise database in the beginning, the BLOs shall be allocated serial number wise mobile numbers of a set of senior citizens each. They shall then call up their respective set of numbers; gather all the requisite information and upload the same on the web-based portal.

(b) However, for senior citizens whose mobile numbers are not available with us, they can register on their own by using this portal.

(c) The senior citizens not covered in (a) and (b) above could give a missed call to a dedicated number to be operationalized by the office of Divisional Commissioner, to express their interest for registration on this Senior Citizen

Portal. The repository/database of these numbers would be allotted to the concerned BLOs and each BLO shall call up these senior citizens and help them by registering their details on the portal on their behalf.

4. A Dashboard shall be created by the IT Team of Office of the Divisional Commissioner based upon the above said portal, giving the summary of people registered and their individual details. Similarly, the dashboard shall have a separate window for accessing the details of all three categories of high-risk patients. The statistical analytical reports of the patients shall also be made available on the dashboard for tracking, monitoring and consequent action.
5. BLOs shall be responsible for their catchment areas and frequently call and check the health conditions of the senior citizens allocated to him/her and update the details on the portal. Another field to be updated after each call shall be whether any of his family members have tested positive for COVID-19?
6. 2-3% of data collected by each BLO will be sampled, at random, for a quality and accuracy test.

7. **Segregation of subset with co-morbidities and symptoms**

   Once the data has been collected/uploaded, it will be cleaned and analysed to identify senior citizens with:

   a. Co-morbid conditions associated with severity of COVID-19 infection. Some of the common co-morbidities are heart disease, hypertension, diabetes, cancer, obesity and asthma;
   b. Any underlying symptoms associated with COVID-19, such as, persistent fever, sore throat, breathing difficulty, and diarrhoea.
   c. Senior citizens who are living alone.

8. **Identification and tagging of high-risk groups**

   Of the entire sub-set of senior citizens with co-morbidities and certain underlying symptoms, the following will be tagged as **"at high-risk"**:

   a. Those at age 80 or above
   b. Those in the age-group of 60-79 with severe co-morbid conditions
   c. Those with COVID-19 related symptoms
   d. Those who are living alone/by themselves

A 24x7 control room (in three shifts) shall be set up at district level headed by District Social Welfare officer under the overall supervision of District Magistrate concerned. The control room will have two to three medical/paramedical professionals (in three shifts) to take care of the consultation to the senior citizens about their health/COVID19 status. They shall be responsible for regular review and monitoring of the status of the registered senior citizens on the dashboard. They will also be responsible for regular communication with high-risk patients and to facilitate them in getting the prescribed health services as per the standard protocol prescribed by the H&FH department. The control room will perform the following tasks:

a. Have a dashboard with details of the three categories of "at high-risk" seniors in their district. The details filled by the BLOs will appear in the dashboard.
b. The nodal officers and medical/paramedical professionals will study the dashboard several times every hour and take cognisance of critical changes in the database such as any change in symptoms of a senior citizen or a family member of a senior citizen getting infected by Coronavirus and other such indicators;
c. After taking cognizance of an adverse development in the condition of a senior citizen or in case COVID-19 is suspected, the control room shall strictly follow the protocol laid down by the Health Department for dealing with such patients;
d. While doing their regular call check-ins, BLOs will also emphasize the precautions to be taken by senior citizens to stay safe from COVID-19;
e. NGOs like Helpage India and Indus Action may be engaged, on pro-bono basis, to conduct the training of BLOs and other ground staff involved in this process

9. **24x7 Central Control Room with a toll-free number will be set up by the Department of H&FW** to function as centre for providing telemedicine services w.r.t COVID and non-COVID diseases of senior citizens. The hospitals and the Ambulance system to be sensitized about the existence of such a network so that the response is expeditious.

10. The Revenue Department shall strengthen the 1077 system with graded increase in personnel by engaging the CDVs (both male and female in equal numbers). In the first instance 6 CDVs (in each shift of 8 hours) shall be deputed, which will be an increase over and above the present strength. In the meanwhile, the capacity of the 1077 control room to be increased to house 100 personnel in a shift. Thereafter, 6 personnel per shift to be added per month till we reach the capacity of attending all calls. Calls received at the HQ level on 1077 would be diverted to District control rooms. Subsequently, it may be utilized as a one-stop call center for all senior citizen related social welfare/ health services.

11. Other actions

The database of senior citizens that the aforementioned process will generate, to be used for the following purposes as well,

a. Data analysis to gauge the following aspects among others,
   i. Senior citizen demographics (general)
   ii. Senior citizen demographics vis-a-vis co-morbidity
   iii. Senior citizen demographics vis-à-vis their dependence.
   iv. Senior citizen location data (general)
   v. Senior citizen location data vis-a-vis infection detection
   vi. Senior citizen infection detection vis-à-vis economic level
   vii. Senior citizen infection detection vis-à-vis symptoms

b. Targeted messaging for awareness and education campaigns shall also be linked to the data collected from this exercise and may take into account:
   i. Location-based vulnerability data – For instance: prioritise messaging based on location.
   ii. Co-morbidity-based vulnerability data – For instance: developing message relevant to people with a specific co-morbidity as it has been found to be the most prevalent and may have certain specific responses to coronavirus.

iii. Dependence based vulnerability data – for instance prioritizing messaging based on whether they are living alone/by themselves or they have support of their children/any caretaker in their residences.

iv. Use of messaging tools based on economic levels

v. Use of messaging tools based on gender

12. All calls/consultations to be logged in the system to generate a **comprehensive database** of the senior citizens dependent on the Government for taking their care. The data can be analysed by the data scientists for **analyzing bigger trends** for further policy interventions.

Annexure-2

89

Government of NCT of Delhi

Department of Information Technology

9th Level, B-Wing, Delhi Secretariat

F.No. E-13014/2/2015-Development/3591-3665 Date: - 11 /09/2018

To

All Pr. Secretaries/ Secretaries/HoDs
Government of NCT of Delhi

Subject: General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000.

Sir/Madam

I am directed to inform that it has been observed that some Departments are uploading documents containing sensitive personal information like Aadhaar numbers, Mobile Numbers, etc. on their websites. IT department has been frequently receiving warnings/communication from CERT-In regarding **Information Disclosure Vulnerability in Domain "delhi.gov.in"**.

2. All departments/agencies are therefore advised to adhere to the provisions of Aadhaar Act 2016 and Information Technology Act 2000. The "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 framed under the IT Act are enclosed for reference (Annexure 'I'). In this regard, 'General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000.' issued by the Ministry of Electronics and Information Technology Government of India are also enclosed for ready reference (Annexure 'II').

3. Departments are requested to review the contents already uploaded on their websites and remove sensitive information (if any) immediately. The

contents to be uploaded on the website must be reviewed and approved by HODs/ senior officers to ensure compliance of said Acts, Rules and Guidelines.

4. A confirmation letter by the Department stating that the Department's website does not contain any sensitive information may kindly be sent to IT Department latest by September 15, 2018.

(Ajay Chagti)
Spl. Secretary (IT)

Encl: Draft confirmation letter.

Copy to

1. Director General, CERT-IN, Electronic Niketan, CGO, New Delhi

or encryption or decryption keys that one uses to gain admittance or access to information;

(i) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

4. Body corporate to provide policy for privacy and disclosure of information.— (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule 3;

Confirmation Letter

<Name of Department>

It is to certify that the <website> pertaining to <department> has no sensitive information as per the Aadhaar Act 2016 and Information Technology Act 2000. The guidelines issued by the Ministry of Electronics and Information Technology Government of India has been complied with.

<Signature of Head of Office>
<date>

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. **Short title and commencement** — (1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions** — (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

(c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;

(d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.

6. Disclosure of information.— (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, 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 of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information 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..

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

85/c

General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000

1. Objective

The objective of this document is to assist the various government departments that collect, receive, possess, store, deal or handle (jointly referred to as "handle" or "handled" or "handling" in this document) personal information including sensitive personal information or identity information to implement the reasonable security practices and procedures and other security and privacy obligations under the IT Act 2000, section 43A (Information Technology rules, 2011 - Reasonable Security practices and procedures and sensitive personal data or information) and Aadhaar Act 2016.

2. Definitions

For the purpose of this document, the definitions as given in the IT Act 2000 and Aadhaar Act 2016 have been used. These are provided here for sake of clarity.

i. ***Personal information*** *means any information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*

ii. ***Sensitive personal data or information*** *means such personal information which consists of information relating to:*

- *Password;*
- *financial information such as Bank account or credit card or debit card or other payment instrument details;*
- *physical, physiological and mental health condition;*
- *sexual orientation;*

2 of 6

- *medical records and history;*
- *biometric information*

iii. ***Identity information*** *in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information; wherein* ***biometric information*** *means photograph, finger print, Iris scan, or such other biological attributes of an individual; and* ***demographic information*** *includes information relating to the name, date of birth, address and other relevant information of an individual.*

3. Document structure

This document is structured to provide general guidelines to various Government departments that are handling Personal information or sensitive personal data or information as per the IT Act 2000, section 43 A and Aadhaar Act 2016.

4. Intended audience

The intended audience for this document from the various government departments that are handling personal information or sensitive personal data or information or identity information as defined above are provided as follows:

i. Information Technology department or division or function
ii. Technology department or division or function
iii. Legal department or division or function
iv. Information security department or division or function
v. Chief Information Security officer
vi. Chief Technology officer
vii. Chief Information Technology officer

84/c

5.0 Basic Actions Departments should undertake should include:

5.1 Organisation Structure, Awareness and Training

i. Identify and deploy an officer responsible for security in your organization/ department
ii. An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.
iii. Ensure all officials involved in any IT related projects read Aadhaar Act, 2016 and IT Act 2000 along with its Regulations carefully and ensure compliance of all the provisions of the said Acts.
iv. Ensure that everyone including third parties involved in Digital initiatives is well conversant with provisions of IT Act 2000 and Aadhaar Act, 2016 along with its Regulations as well as processes, policies specifications, guidelines, circular etc issued by the authorities from time to time.
v. Create internal awareness about consequences of breaches of data as per IT Act 2000 and Aadhaar Act, 2016.
vi. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

5.2 Technical and Process Controls

i. Follow the information security guidelines of MeitY and UIDAI as released from time to time.
ii. Informed consent – Ensure that the end users should clearly be made aware of the usage, the data being collected, and its usage. The user's positive consent should be taken either on paper or electronically.
iii. Ensure that any personal sensitive information such as Aadhaar Number, Bank Account details, Fund transfer details, Gender, Religion, Caste or health information display is controlled and only displayed to the data owner or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
iv. Verify that all data capture point and information dissemination points (website, report etc) should comply with IT Act and UIDAI's security requirements.

v. If agency is storing Aadhaar number or Sensitive personal information in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using Hardware Security Modules (HSMs). If simple spreadsheets are used, it must be password protected and securely stored.

vi. Access controls to data must be in place to make sure sensitive personal information including Aadhaar number and demographic data is protected.

vii. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number based index.

viii. Regular audit must be conducted to ensure the effectiveness of data protection in place.

ix. Identify and prevent any potential data breach or publication of personal data.

x. Ensure swift action on any breach of personal data.

xi. Ensure that the system generates adequate audit logs to detect any breaches

xii. Ensure no sensitive personal data is displayed or disclosed to external agencies or unauthorized persons.

xiii. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure that all Aadhaar holders are able to use it effectively.

xiv. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.

xv. In case department is using Aadhaar Authentication, it should follow exception handling mechanism on following lines-

a. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.

b. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.

c. If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.

number if required to be printed, should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed

v. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar Act. The purpose of use of Aadhaar information needs to be disclosed to the resident

vi. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.

vii. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room

viii. Do not permit any unauthorized people to access stored Aadhaar data

ix. Do not share Authentication license key with any other entity.

****

d. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.

xvi. All access to information, or authentication usage must follow with notifications/receipts of transactions.

xvii. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, SMS, physical-center, etc.).

xviii. Get all the applications that collect personal sensitive information audited for application controls and compliance to the said Acts & certified for its data security by appropriate authority such as CERT-IN empanelled auditors.

xix. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

xx. Check all IT infrastructure and ensure that no information is displayed and in case it is displayed, please remove them immediately.

xxi. Ensure that adequate contractual protection is in place in case third parties are involved in managing application/ data centers

5.3 Data Retention and Removal

i. Ensure that the department has developed a data retention policy
ii. Ensure that you do not store personal sensitive information for a period more than what is required
iii. Delete/ remove/ purge the data after a specified period

5.4 Aadhaar Specific precautions

i. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc.
ii. Do not store biometric information of Aadhaar holders collected for authentication.
iii. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
iv. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar