Dr Peter Homa CBE DBA
Director General of the Defence Medical Services

Headquarters Joint Medical Group

Coltman House,
Defence Medical Services Whittington,
Tamworth Rd
Lichfield, WS14 9PY

Tel. No.: 01543 434621
E-mail: allison.orchard100@mod.gov.uk

Fiona Deans, COO
Government Digital Service
Cabinet Office
70 Whitehall
London
SW1A 2AS

Ref:: 20200529-DG_DMS_LTR_GDS-CO

Date: 09 June 2020

Dear Fiona

Terms of Release of Defence Medical Services (DMS) Vulnerable Patient List Contact Details for COVID-19 Vulnerable Patients Online and Telephone Service

Background
Government Digital Service (**GDS**), acting as part of the Cabinet Office, has been commissioned by the Prime Minister to develop an online and telephone service for extremely vulnerable patients. Information about the service is here: https://www.gov.uk/coronavirus-extremely-vulnerable.The service will provide those individuals with a way to seek help and support whilst they are self-isolating to protect themselves from the COVID-19 virus, including by providing a means to ask for social care support and essential food and supplies (the **Service**).The Cabinet Office is the Controller (as defined in the General Data Protection Regulation 2016 (**GDPR**)) for the personal data processed as part of the Service.

The Defence Medical Services (DMS) has produced an Extremely Vulnerable Patient List (**DMS List**) which contains the name, address, date of birth (**DOB**), phone number and NHS number for those individuals who have been identified by clinicians as being extremely vulnerable in relation to the COVID-19 virus as a result of their pre-existing medical conditions. The DMS is writing to those patients to let them know that they have been identified as extremely vulnerable and to offer them advice. The letter will include their NHS number and details about the Service and will invite them to contact the Service.

Confidential nature of the information to be shared
Ministry of Defence is the Data Controller for the DMS List. The DMS List is identifiable confidential patient information about the individuals on it, as it is comprised of information that has been obtained by the DMS, in confidence from the patients on the list. It also provides information about the health of the patients as by virtue of being on the list, it is known that those individuals are extremely vulnerable to the COVID-19 virus and at risk of the virus having a more serious effect on them due to pre-existing medical conditions. The information in the DMS List is also therefore confidential information and subject to a duty of confidence under the common law.

Agreed purposes for which the information is to be shared.
It has been agreed that DMS will share the information in the DMS List with the Cabinet Office for the following agreed purposes only (the **Agreed Purposes**):

a) The Service will use name, DOB, and postcode from the DMS List for verifying that those individuals who contact the Service are on the DMS List, and to verify the identity of the individuals when they make contact.

b) The Service has established an outbound call centre, to be operated on behalf of the Cabinet Office by the Department of Work and Pensions (**DWP**), as a Processor (as defined in DPA18), to call those DMS patients who have a telephone number and who have received a letter from the DMS, but who have not yet contacted the Service. This outbound call service will offer those patients support through the Service, including a delivery of essential food supplies. This Service will also use name, DOB, postcode, and NHS Number to verify the identity of the patient with whom it is making contact. DWP will cross check that data with its Customer Information System (CIS) and other sources of information agreed with the Cabinet Office via any permitted sub-Processors for the sole purposes of identifying:

   - deceased persons, to remove them from call lists;
   - missing or additional phone numbers, so as to contact those on the DMS List; and
   - patients with physical, social or financial vulnerability or visual impairment, in order to prioritise calls by the outbound call centre to those patients on the DMS List who may have the most difficulty contacting the Service themselves, or who are considered to be most vulnerable and in need of support.

c) The Service will co-ordinate support for patients in the form of essential food and other supermarket supplies, where the patient has requested support for this, via the Department for the Environment, Food and Rural Affairs (**DEFRA**), by providing information which will allow wholefoods suppliers and supermarkets to deliver essential food and other supermarket supplies to patients at their homes. The information that will be shared with DEFRA is not information from the DMS List, but information provided to the Service by individuals asking for support. DEFRA will also provide information which will allow supermarkets to prioritise these patients for their online delivery services. Data to be shared for this purpose will include name, address and mobile phone number of the patient which has been obtained from those patients, solely for the purposes of arranging such supermarket shopping deliveries. The NHS number will not be used for this purpose and will not be shared with DEFRA or supermarkets or with any intervening organisation in the supply chain relating to this purpose.

d) The Service will co-ordinate logistical support in relation to the provision of food and other essential supplies and may share anonymous aggregate information regarding the number of patients on the DMS List in each local area with the Ministry of Defence and any other organisations who require this information as part of the Service for this purpose. The Cabinet Office will not and will ensure that the organisations with whom it shares such information will not, publish anonymous and aggregate data about the DMS List.

e) The Service, in conjunction with the Ministry of Housing, Communities and Local Government (**MHCLG**), may also co-ordinate support for patients from their local authorities for those patients who:

   - have requested support from their local authority through the Service in response to receiving the letter or the text message; and/or
   - who have not yet contacted the Service.

f) The Service will therefore provide local authorities with the following two datasets:

   i. information obtained from those patients and verified against the DMS List, to each local authority for those patients in their area (the **Incoming Local Authority Datasets**). This will include name, address, DOB, telephone number and NHS Number.

Local authorities will be able to use the Incoming Local Authority Dataset to verify the identity of the patient as a resident in their area and to contact the patient to offer them support from the local authority, in co-ordination with the Service.

ii. information from the DMS List about patients resident in each local authority area, including those who have not yet been in touch with the Service, which will also include name, address, DOB, telephone number and NHS Number (**DMS List Local Authority Datasets**). Local Authorities will be able to use this information to prioritise contacting those individuals to offer them help, social care and support, working in coordination the Service and other relevant organisations in the area as part of the local COVID-19 response as set out below.

g) Local authorities may:

i. within a tiered council structure (e.g. County, District and/or Town/Parish), share their full DMS List Local Authority Dataset with the other local authorities across these tiers in their region;

ii. share relevant information from the DMS List Local Authority Dataset with care homes, contracted social care providers and other similar organisations providing care to those patients, about their patients who are on the list;

provided that local authorities ensure the information they share above is from the latest DMS List Local Authority Dataset; this information is shared safely and securely with those who need this information to provide support to the patients on the list and who have a legal basis to receive it; that local authorities work with the Service and those organisations with whom they share information to ensure that contact with patients is co-ordinated; and that the local authorities feedback regularly to the Service about the patients with whom they have made contact.

Privacy Notice
The Service will explain about how the patient's data will be used by the Service, including referring patients to the online Privacy Notice at https://coronavirus-vulnerable-people.service.gov.uk/privacy (the **Privacy Notice**).

The Privacy Notice will provide further details to patients about how their personal data will be used and shared by the Cabinet Office, including who it will be shared with and for what purposes. This includes sharing relevant data with local authorities and other government departments.

Legal Basis for DMS to Share the Disclosed Data
This power is subject to DMS satisfying the common law duty of confidence, as we are sharing patient information. We consider it is strongly in the public interest to share this information for the Approved Purposes above (i) due to the urgent need to put in place services to help extremely vulnerable patients in the community to protect themselves from the risk of Covid-19 and (2) to ensure they have a means of seeking support for essential services, including social care support from local authorities and food, which is currently a significant issue due to shortages in supermarkets and demand for online delivery services.

We have discussed other alternatives to sharing information from the DMS List but, in the timescales, and due to the urgency of the response that is required, there is no alternative. Failing to share the personal data with the Service may result in harm to the extremely vulnerable patients on the DMS List as they may not be able to evidence their entitlement to use the Services or to verify their identity to the Service, or access the Service and would consequently be deprived of vital help and support they need.

Under GDPR, DMS is relying on Article 6(1)(d) – vital interests and Article 6(1)(e) public task to share information with the Cabinet Office for the Agreed Purposes above. As this is health

information and therefore special category personal data DMS is also relying on Article 9(2)(g) – substantial public interest and para 6 of Schedule 1 DPA – governmental purpose to share this data for the Agreed Purposes.

DMS will publish details about the sharing of information on the DMS List with the Cabinet Office in its local data registers where relevant and will update its privacy notice to reflect the sharing of this data for COVID-19 purposes.

Legal Basis for Cabinet Office to Receive and Process the Disclosed Data
The Cabinet Office is exercising Governmental functions in delivering the Service and processing information from the DMS List for the Agreed Purposes. It also relies on the above public interest grounds for the processing it carries out of the confidential patient information unless patient consent is obtained, whereupon it will rely on express consent. In relation to sharing the DMS List Local Authority Dataset with local authorities, the Cabinet Office is entitled to share this information with the local authorities, who have a legal function to process it for COVID19 purposes under the notice dated 20th March 2020 issued to them by the Secretary of State for Health and Social Care under Regulation 3(4) of Health Service Control of Patient Information Regulations 2002 (the **COPI Notice**).

Under GDPR, the Cabinet Office is also relying on Article 6(1)(d) – vital interests and Article 6(1)(e) public task to process the information on the DMS List for the Agreed Purposes unless patient consent is obtained, whereupon it will rely on Article 6(1)(a) - consent. As this is health information and therefore special category personal data, the Cabinet Office is also relying on Article 9(2)(g) – substantial public interest, and para 6 of Schedule 1 DPA – governmental purpose to process this data for the Agreed Purposes.

The Cabinet Office has published a Privacy Notice for the Service on the Service website which will provide full details to individuals about how their data will be processed by the Service, including the sharing of the DMS List Local Authority Dataset with local authorities.

Agreement to share data from the DMS List
DMS is the Controller of the DMS List and has agreed to provide the Cabinet Office with the following personal data from the DMS List: name, address, date of birth, telephone number and NHS number for each patient on the list (**Disclosed Data**) for the Agreed Purposes above.

1. The Cabinet Office will be the Controller of the Disclosed Data once disclosed. Newton Europe and Amazon Web Services (**AWS**) are both Processors of the Cabinet Office, who may process the Disclosed Data on behalf of and in accordance with the instructions of the Cabinet Office, solely to the extent necessary for providing the Services and for the Agreed Purposes. Newton Europe and AWS will not use or process the Disclosed Data for any other purpose.

2. The DWP is also a Processor of some of the Disclosed Data, for the sole purpose of calling patients who are on the DMS List and who have been sent a letter from the DMS, but who have not yet contacted the Service. The DWP may call those patients to tell them about the Service and offer them support and advice through the Service. The DWP will do so solely on the instructions of the Cabinet Office and when calling patients will identify themselves as calling from the Service and not as the DWP. This is referred to in this Letter as the **Outbound Calling Service**. The DWP will receive name, DOB, postcode and telephone number for this purpose, are authorised to carry out the cross-checks on the data against the data held in CIS and in other data sources agreed with the Cabinet Office (including by way of sub-Processors to DWP agreed by the Cabinet Office), for the Agreed Purposes only. DWP and any approved sub-Processors will be required to carry out such cross-checking in a secure segregated system separate from CIS and from those other permitted data sources, and DWP must securely delete the Disclosed Data once it has been used for the Agreed Purposes and require

that any approved sub-Processors do the same. The DWP and its sub-Processors will not be permitted to use the Disclosed Data for any other purpose.

3. The Disclosed Data will be provided by secure transfer as agreed by Colette Jackson, DMS Medical Information Manager on behalf of DMS and those individuals previously agreed with Ian Tester as authorised to receive it on behalf of the Cabinet Office. The transfer between DMS and the Cabinet Office will use a Secure Electronic File Transfer solution, which uses 2 factor authentication and applies 256b encryption of data in transit. The initial transfer of Disclosed Data will take place on or after 25 May 2020. Subsequent transfers of updated Disclosed Data taken from the DMS List (as the same may be updated by DMS) will be on the dates to be agreed by DMS and the Cabinet Office. Once received, the nominated individual who has received this on behalf of the Cabinet Office will process the received data on a GDS encrypted device to extract NHS number, postcode, mobile phone number and date of birth for the full patient cohort. That Disclosed Data will be uploaded to a secure AWS Virtual Private Cloud (VPC) environment and loaded to a Dynamo DB datastore and will be held by AWS in this datastore as a Processor for and on behalf of the Cabinet Office, on its instructions for the Agreed Purposes. All data processed during the intermediate transfer step will then be securely deleted by the Cabinet Office.

4. The Cabinet Office may provide a daily cut of the Disclosed Data to the DWP for the purposes of it delivering the Outbound Calling Service via a secure and encrypted transfer mechanism to be agreed with the Data Protection Officer of the MOD. This cut of the Disclosed Data will only contain the details of those patients on the DMS List who have been sent a letter from the DMS but who have not yet contacted the Service.

5. The Cabinet Office will provide the DMS List Local Authority Datasets via a secure and encrypted two factor authentication mechanism (to be agreed between Colette Jackson, DMS Medical Information Manager), to the lead local authority for each of the local authority hubs. The lead local authority will act as a Processor for each other local authority in the hub for the purposes of securely transferring each DMS List Local Authority Dataset directly on to the relevant local authority. GDS will provide the DMS List Local Authority Dataset to local authorities under terms and conditions which make it clear:

    a. the Dataset contains confidential patient information, is provided in confidence, and must be maintained and handled by the local authorities as confidential;
    b. that each Dataset was produced based on information held in DMS central records at a specific point in time and could contain information about individuals who are now deceased;
    c. that an outbound central call centre will be calling those individuals who are on the DMS List but who have not yet contacted the Service, to offer them information about the Service and support;
    d. that the Dataset can only be used and shared by local authorities as outlined above in paragraphs (f) and (g) of the Agreed Purposes; and
    e. that each local authority processing the Dataset will comply with the relevant aspects of paragraphs 7, 8, 9, 11, 12 and 13 below.

6. The Disclosed Data is confidential patient information and is provided by DMS in confidence to the Cabinet Office, any other Controllers with whom it is permitted to share the Disclosed Data, including local authorities (**Approved Controllers**) and to its Processors. The Disclosed Data must be maintained by the Cabinet Office, Approved Controllers, and its Processors as confidential in accordance with the common law duty of confidence (**Duty of Confidence**). The NHS number is a highly sensitive data item as it is used across the health and social care system as evidence of entitlement to health and social care and is used by patients to access health and social care services. As such the NHS number should not be used or shared by the Cabinet Office for any purposes other than the initial purpose for which it was proved, namely to verify that a person seeking support from the Service is on the DMS List and as part of the process of verifying the individual's identity. It may also be shared with local authorities if this is

necessary for the local authorities to verify the identity of the individual and/or their entitlement to social care services, given that local authorities have a legal basis to process this information under the COPI Notice referred to above and to provide social care.

7. The Disclosed Data can be processed under this letter only for the Agreed Purposes and until 30th September 2020 (the **End Date**). The End Date will be reviewed by DMS and the Cabinet Office and if the Cabinet Office, its Processors and any Approved Controllers continue to need any of the Disclosed Data for the Agreed Purpose beyond the End Date, DMS and the Cabinet Office will agree in writing an extension to the End Date and any necessary changes to the terms of this letter, including the legal basis for continued processing by the Cabinet Office, its Processors and the Approved Controllers of the Disclosed Data.

8. The Cabinet Office will and will procure that all Approved Controllers either obtain the express consent of every patient who contacts the Cabinet Office or Approved Controller or ensure it or the Approved Controller has another legal basis under GDPR to any processing by the Cabinet Office or Approved Controller of the Disclosed Data beyond the Agreed Purposes. If the Cabinet Office or Approved Controller does not have another legal basis under the GDPR for continued processing, the Cabinet Office will and will procure the Approved Controller will cease processing the Disclosed Data if a patient subsequently withdraws their consent to processing by the Cabinet Office or Approved Controller. The Cabinet Office will and will procure that the Approved Controllers will also cease contacting a patient if that patient opts-out of receiving contact from the Service or the Approved Controller or declines the offer of support from the Service or Approved Controller.

9. The Cabinet Office will share such information with DMS as the parties agree is necessary for DMS to maintain the DMS List.

10. The Cabinet Office will publish a Privacy Notice on the Service website providing details of how personal data is processed by the Cabinet Office as part of the Service, including reference to the data it has obtained from DMS and the personal data that it may share back with DMS (as the parties may agree above) to enable DMS to maintain the DMS List and shall procure that Approved Controllers also publish details of the Disclosed Data they are processing.

11. The Cabinet Office and DMS will agree a process for the Disclosed Data to be updated with changes to the DMS List reflected in new releases of the DMS List made available by DMS. Changes to the DMS List will include new patients who are added to the DMS List, patients who are removed from the DMS List (including patients who have died), changes to the contact details of patients on the DMS List and may include changes to contact preferences expressed by patients on the DMS List. The Cabinet Office will ensure it puts in place processes to update the Disclosed Data with any changes in updated versions of the DMS List released by DMS and will ensure that these changes are also reflected in any data from the Disclosed Data which is shared by the Cabinet Office with its Processors and any Approved Controllers.

12. The Cabinet Office will ensure that it and any of its Processors and the Approved Controllers:

    a. comply with the GDPR, the Data Protection Act 2018 and all applicable law concerning privacy or the processing of personal data (**Data Protection Law**) and the Duty of Confidence in relation to the processing of the Disclosed Data;

    b. take all reasonable steps to ensure the reliability and integrity of the individual personnel who have access to the Disclosed Data and ensure that they:

        i. are informed of the confidential nature of the Disclosed Data and the Agreed Purposes for which it may be processed;

ii. do not publish, disclose, or divulge any of the Disclosed Data to any third party unless to another Processor, Approved Controller or personnel authorised by the Cabinet Office and for the Agreed Purposes;

iii. are subject to appropriate confidentiality undertakings that are in writing and are legally enforceable;

iv. have undergone adequate training in the use, care, protection, and handling of personal data that enables them and the Cabinet Office, Approved Controller or Processor to comply with their responsibilities under Data Protection Law;

c. shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risks associated with processing the Disclosed Data;

d. shall notify DMS without undue delay if it:

i. becomes aware of any Personal Data Breach (as defined in GDPR) in relation to the processing by the Cabinet Office or its Processors or Approved Controllers of the Disclosed Data;

ii. receives any request, complaint or communication relating to either party's obligations under Data Protection Law or the Duty of Confidence connected with Disclosed Data;

iii. receives any communication from the Information Commissioner' Office or any other regulatory or supervisory body connected with the Disclosed Data;

e. will on the End Date, securely delete or securely return to DMS, any Disclosed Data (and any copies of it) and require the Approved Controllers and its Processors (and any approved sub-Processors) to do the same, unless the Cabinet Office or Approved Controller has a lawful basis under the common law duty of confidence or GDPR to continue to process this Data beyond the End Date. The Cabinet Office will at the request of DMS provide and shall require Approved Controllers and its Processors (and their sub-Processors) to provide, certificates of destruction signed by its Data Protection Officer to confirm such secure destruction.

13. DMS and the Cabinet Office will work together to agree any necessary changes to the terms of this letter to reflect any necessary changes to the processing of the Disclosed Data and to agree:

a. Any other Processors or Controllers to whom the Disclosed Data may need to be disclosed and for what purposes in order to deliver the Services. Any other Controller will be required to agree to relevant terms the same as or similar to, those set out in this letter in order to process the Disclosed Data;

b. Any other purposes for which the Disclosed Data may be processed to support the provision of the Services;

c. The process and legal basis for the Cabinet Office sharing back to DMS any updates to the Disclosed Data, which are obtained by the Cabinet Office from patients who use the Service, in order to ensure that DMS can maintain the accuracy of the DMS List; and

d. The process for DMS sharing any updates to the Disclosed Data with the Cabinet Office when a new release of the DMS List is made available.

14. Any dispute in respect of these terms or their subject matter will be escalated to appropriately senior officers of GDS and DMS for resolution.

15. The contact details for the parties respective Data Protection Officers are:

    a. MoD: Mr Ian Henderson, cio-dpa@mod.gov.uk

    b. Cabinet Office: Steve Jones, DPO@cabinetoffice.gov.uk

Your sincerely