INFORMATION GOVERNANCE 24
SYSTEM ACCESS AND VACCINATION DATA

1. Introduction. I overheard a discussion recently between two project managers involved in planning the Covid-19 vaccination programme where they in essence stated that "this programme is so important that Information Governance rules and stuff no longer apply". I also saw a technical plan which stated that as this programme was so important user log ins to the computers would not be required. Let me be clear and say that it is exactly because this programme is so important that Information Governance and IT Security rules will apply to it at all times.

2. Properly implemented risk-based Information Governance and Security controls will ensure that the Covid-19 vaccination programme processes patient data appropriately in a way which will maintain security and confidentiality of the data. This is vital for several reasons, not least the need to maintain public trust in the use of personal data in relation to the vaccination programme.

3. This briefing document is not intended to go into the full legal background to the use of personal data, that is covered by NHS Digital here:
   https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/coronavirus-covid-19-response-transparency-notice

4. There are however some practical points that can be made:

   4.1. Some practice staff may need to work at and access patient records from other practices, often across a PCN. This is fine, all access should continue to be made with an NHS Smartcards and all normal policies and rules apply.

   4.2. Some staff from the CCG (and potentially NHS England/Digital) may need access to practice systems in relation to the vaccination programme. All staff should ensure they have a valid working Smartcard and access rights which can be allocated at practice level. Again, all staff working in this way are covered by employment contracts and Smartcard Terms and Conditions.

   4.3. Staff not employed by an organisation working on a temporary basis may need occasional access to systems. In such a scenario we'd recommend a short-term agreement or Honary Contract needs to be in place.

5. All access to clinical record systems will continue to create audit trails which can be examined to ensure all access is appropriate. This covers access to all practice systems, Pinnacle, and the Summary Care Record where it is used. Any inappropriate access to patient data can lead to organisational fines and individuals facing disciplinary or even legal action.

6. The NHS must continue to protect its electronic systems and data stored on them by enforcing technical controls such as encryption which must be applied to all laptops and removeable media such as USB storage devices. The use of personal storage devices and personal non work email accounts is not permitted.