INFORMATION GOVERNANCE
PERSONAL DATA BREACHES

1. Introduction. A frequent question we get is “do we have to inform all persons affected by a data breach”. This factsheet sets out to answer that question as well as advising on which circumstances would require you to inform a person about a data breach.

2. UK GDPR does not require you to inform every person affected by a data breach. It does however require that you inform a person where “there is a high risk to an individual’s rights and freedoms”.

3. Note that the Duty of Candour does not apply where the data breach does not affect patient care.

4. Unless the ICO compels it, you do not need to inform patients or service users of a breach if:

   4.1. Appropriate organisational or technical measures were in place at the time the breach occurred, which made the data unusable or inaccessible. For example if a lost device was encrypted or if NHS Mail secure service was used..

   4.2. You have taken measures to ensure that any high risk impacts on the patient or service user are now unlikely to happen. For example, you have corrected the data you hold that was maliciously altered during a cyber attack.

   4.3. Disproportionate effort would be needed to inform the patient or service users of the breach. In which case, a public message on the website or in local newspapers alerting patients or service users to the incident would suffice.

   4.4. Personal data is recovered (returned or securely destroyed) from a "trusted partner organisation." A trusted partner organisation could be another GP Practice or your local NHS hospital. This could provide you with assurance that they will not read or access the data sent in error.

   4.5. There is a risk the affected individual may not fully understand the nature of the incident and may become unduly concerned about it.

5. When informing an individual of a breach, you should describe, in clear and plain English, the nature of the personal data breach and at least:

   5.1. The name and contact details of any DPOs you have, or other contact point where more information can be obtained.
   5.2. A description of the likely consequences of the personal data breach
   5.3. A description of the measures taken or proposed, to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
   5.4. If possible, you should advise individuals on the steps they can take to protect themselves, and what you are willing to do to help them.