How to hold adequate data

Sarah Cook

Head of NHS, Business and General Practice

How can you be sure that the records you hold about your employees are Data Protection compliant? In particular, that they are 'adequate, relevant and limited to what is necessary'. In this article we are going to think about the 'data minimisation' principle and how to ensure your HR records meet these requirements.

So what is data minimisation? This is identifying the minimum amount of information needed to fulfil your particular purpose. That is the data you should hold, and no more.

All dental practices collect, hold and maintain an abundance of information relating to the business including employee information. It is important to ensure that practices identify at the outset what information must be kept. Once this is established, they must then have effective and well-organised systems in place to ensure that the data kept meets the data protection principles.

You also need to be able demonstrate that you have suitable processes in place to ensure that you only hold and collect the personal data you need.

With this in mind, GDPR also says that individuals have the right to ask you to delete any unnecessary data you hold, this is called the right to erasure or to complete any incomplete data which is inadequate for your purpose, the right to rectification.

So what is considered adequate, relevant and limited?

These terms are not defined in the regulations. However, essentially it means collecting and holding only the minimum amount of personal data needed to fulfil your purpose. It will be dependent on your reasons for collecting and using the personal data. In order to assess this you should carry out a data audit to determine what data you have and why you need it. This

will give you a clear picture of what data you have, where it is stored, who has access to it, what it is used for and accordingly why you have it and why you need it. Employers are not able to collect personal data because it might be useful, or if you have not identified a specific purpose for it.

It must be relevant; this means there must be a rational link to the stated purpose for collecting it. It must be limited to what is necessary, you must not hold more than you need for that purpose. This is even more important for special category data, such as health information, where it is vital you keep only the minimum information required. If you hold more data than is necessary then it increases the inherent risks in a personal data breach and also increases the burden on you of collecting, storing, securing and keeping up to date unnecessary data.

In addition, you should regularly review your processing to check that the personal data you hold is still relevant and adequate for your requirements and delete anything you no longer need. This is closely linked with the storage limitation principle. The Data Protection Regulations do not set out specific retention periods although there will be information within certain records that is subject to a statutory retention period. Where this is not specified there will usually be a recommended retention period which you should follow.

Let's think about specific HR situations, for example when you could be holding too much data.

As an employer, you hold details of your staff's vaccination records for those working with patients. You need these details from your dental nurses in case of an accident such as a needle stick injury. If you hold the vaccination record for your receptionist on the other hand, this information is likely to be irrelevant and excessive as they do not engage in the same clinical work.

Conversely, there are some situations where you could be deemed to processing inadequate personal data. If the data you hold are not giving you the information you need to achieve what you need to do then the personal data you have may be inadequate.

For example, the quality of CCTV images is so poor that identification is impossible. You should not be processing personal data if it is insufficient for its intended purpose.

What about collecting information in relation to the current COVID-19 situation? For example, you might want to ask your staff if they have specific health conditions such as severe asthma or pregnancy that would make them more vulnerable. This is health data and therefore special category data. The ICO guidance is that collecting health data may be necessary in current circumstances for employers trying to ensure the health and safety of their employees. Keep the principle of data minimisation in mind. Do not collect more data than you need, i.e. limit the collection of health data to information that is relevant to COVID-19. Make sure you keep the data safe and secure and only share if absolutely necessary and there is a legal basis for doing so.

You will also need to consider if you need to carry out a data protection impact assessment which is required for any processing that is high risk and special category data is more likely to be deemed high risk. You may also want to consider updating your privacy notice so that you are as transparent as possible to your staff about the data you are collecting, what it will be used for and who it may be shared with.

BDA members can access further advice about Data Protection compliance at: <https://www.bda.org/gdpr> ♦

<https://doi.org/10.1038/s41404-020-0419-3>

© Westend61/Getty Images Plus