The Right Protection

Pharmaceutical businesses are very familiar with the requirement to protect patient information and clinical data, but how many are as careful with their staff data? Nicola Walker at Hogan and Hartson, London, investigates

Nicola Walker is a Partner at Hogan and Hartson, specialising in English employment law and privacy. Her employment practice encompasses employment advice for both employers and senior executives. Nicola has considerable experience advising clients and litigating business protection issues, including restrictive covenants and confidentiality provisions. As a litigator, she has experience in Employment Tribunals, the Employment Appeal Tribunal, and the High Court. She has acted in many complex cases involving dismissals, transfer of undertakings and discrimination. Nicola also counsels companies on the employment aspects of large corporate transactions. She advises clients on consultation strategies and the reorganisation of businesses, including motivating and retaining key employees and making large-scale workforce reductions.

Key requirements of the Data Protection Act 1988 are that employers must comply with eight principles and most employers must register as a data controller. Individuals have the right to access their data and the right to correct, and sometimes block, the data from being processed. There are two types of data – ordinary and sensitive data. In the employment context, any information which relates to somebody's sex, health or whether they have committed any previous offences is sensitive data.

The eight key principles include an obligation to process data fairly, to limit the amount of information that can be collected and the uses to which it can be put, a requirement to destroy information which is no longer required and to ensure the security of retained information. One of the most difficult hurdles for many multinational businesses is the obligation that precludes the transfer of information outside the UK and Europe unless it is to another country that has adequate data protection laws in place.

WHAT DOES THIS MEAN IN PRACTICE FOR AN HR TEAM?

In the UK, the data protection regime is supervised by the Information Commissioner. They have produced a four-part code for employers which addresses employment issues and is essential reading for any HR practitioner.

The first practical step is for management to assess and understand what personal information is collected. This will include offers of employment, contracts, salary and payment details, benefit administration, sickness and holiday records, appraisals and disciplinary records.

The second step is to understand what the requirements are for the processing of information, and to make sure there are proper records in place to deal with the fair processing.

An issue which causes much difficulty in larger multinational companies is the transfer of data. Information cannot be transferred outside the European Economic Area without adequate safeguards being in place. Multinationals with head offices in the US commonly want to know a significant amount about their subsidiaries' operations, wherever they are situated in the world. For them, as for other multinationals, the transfer of data can be a headache; however, there are various options as to how this can be dealt with.

Personnel information may not be collected or processed unless there are permissible grounds. The person to whom the information relates should be told of the purposes for which it has been collected and the way in which it will be handled and used. The best way to do this is to include specific clauses in the contract of employment or employee handbook which explain these steps. Some employers rely on consent as the basis for the collection and processing of personnel information. However, it is often preferable to assume that the employer has a legitimate interest in any staff information being processed, and that this interest is not overridden by the risk of prejudice to the individual. Employers should avoid reliance on consent. Most European countries adopt the view that consent is only effective if it is freely given and can be withdrawn at any time; they regard employees as unable to genuinely give consent freely. In relation to the processing of sensitive data, it is essential that explicit consent is granted. Moreover, employers should avoid collecting sensitive data wherever possible. In practice, systems such as health insurance can be set up so that the claim is dealt with directly by a health insurer so that the employer has little or no contact with that information.

The third key issue is to train management so that they do not collect unnecessary information and understand the limits pertaining to the use of information that they have collected. It is also worth considering retention periods for certain types of data. Files should be routinely weeded and checked so that out of date information is destroyed.

Fourthly, employers should ensure the security of employee information. Employee files should be securely protected and made available only to those who really need access. Staff need to be trained to ensure that security measures are enforced and personal details are not given out without permission.

TRANSFER OF DATA

An issue which causes much difficulty in larger multinational companies is the transfer of data. Information cannot be transferred outside the European Economic Area without adequate safeguards being in place. Multinationals with head offices in the US commonly want to know a significant amount about their subsidiaries' operations, wherever they are situated in the world. For them, as for other multinationals, the transfer of data can be a headache; however, there are various options as to how this can be dealt with. One option that seems easy, but is less useful in practice, is to ask employees to consent. As before, consent should be freely given and can be withdrawn, so this is often not a reliable option. Another option is to enter into a Model Contract or, where the transfer is to the US, to use Safe Harbor, a system in which companies choose to opt into a regime that requires adherence to a similar standard set by the European regime, and is administered by the Federal Trade Commission. The Model Contract is a regime under which companies who opt for this route must use a mandatory form of contract. These contracts have been approved by the European Commissioners as providing adequate security for data.

A more recent option which some larger companies are considering is binding corporate rules. These have to be approved by the European Union. This process is gradually being simplified and the various European Supervising Authorities, such as the European bodies responsible for data protection, have agreed that approval can be obtained through one lead authority. The UK's Information Commissioner has a firm commitment to making this process a workable option for business. However, getting approval is still a lengthy process and an expensive option for smaller businesses.

CONCLUSION

Since HR departments expect to handle employee data carefully and securely, the practical arrangements necessary for compliance with the European standards are often already in place. Nevertheless, choosing the best option for transfer of staff data takes time and careful consideration. For those companies who do not have this assessment in hand, a review and a decision as to how best to deal with the matter is essential. Pharmaceutical companies are often the target of public scrutiny and even those who are not involved in day-to-day pharmaceutical operations should adopt a high standard of care in their work. To do this, they should ensure that they are familiar with the key requirements for proper protection of employee data and that they are installing and maintaining the procedures needed to comply with the relevant legislation. ◆

The author can be contacted at nwalker@hhlaw.com