Accessing employee's private information online

NHS National Services Scotland

This briefing takes into account relevant guidance contained in the 'Draft' Statutory Code of Practice in respect of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S) A). This Code of Practice includes new sections on accessing the internet, social media and private social networking sites to obtain private information was published in February 2018.

What is 'private information'?

'Private information' is defined in RIP(S) A as "....private information includes any information relating to a person's private or family life.... As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships....."
'Family' should be treated as extending beyond the formal relationships created by marriage or civil partnership.

'Private information' will in most cases, also mean personal data, such as names, addresses and telephone numbers.

It is likely that any 'private information' obtained, will fall within the definition of 'personal data' as currently contained in the Data Protection Act 1998, and the forthcoming General Data Protection Regulations 2018.

What is 'surveillance'?

Some types of surveillance, as of itself, are not unlawful. It neither breaches a person's Human Rights, as incorporated in legislation nor requires a specific authorisation to conduct any such activity. (E.g. general observations by the Police carried out in the course of their patrols or duties)

Surveillance, for the purpose of RIP(S) A, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is
or may be taking place.

'Directed surveillance' is covert surveillance, if carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person.

What about accessing information online, can it be classified as 'private information' or 'personal data'?

Yes. Public use of the internet has expanded rapidly so that far more activity and interaction now occurs online than ever before. There may be a reduced expectation of privacy for material accessible on the internet, but privacy considerations may still apply, e.g. information posted on private social networking sites or social media, where the information may include or constitute private information and/or personal data.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is being made by a public authority of that person's activities for future consideration or analysis.

Surveillance of publicly accessible areas of the internet should be treated in a similar way, it is important to recognise that there may be an expectation of privacy over information which is on the internet, particularly when accessing information on social media websites or private social networking sites. (Facebook, LinkedIn, etc)

Expectations of privacy are important considerations when deciding to access the internet to obtain private information. There may be less of an expectation as regards private information held on public directories or by public record-keeping such as Companies House or the public facing telephone directory. Also expectations might be less when posting private information on social media, where the intention is to communicate or publish material to a wide audience. (E.g. Twitter).

Expectations about privacy may increase however, when posting private information to private social networking sites, (E.g. Facebook, Linked In). This is regardless of whether or not the account holder has applied any available privacy settings to the online account.
In deciding whether carrying out activity to obtain private information online amounts to covert surveillance, consideration should also be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity.

Accessing employee's private information online

NHS National Services Scotland

What type of surveillance is CFS authorised to carry out?

CFS is the only part of the NHS in Scotland, being a relevant public authority, regulated under RIP(S) A to carry out authorised, directed, covert surveillance for the purpose of preventing or detecting crime. By complying with RIP(S) A, CFS can rely on a statutory framework under which, authorised, directed, covert surveillance can be conducted compatibly with the Human Rights Act 1998.

In what circumstances should accessing 'private information' or 'personal data' online only be carried out by CFS or the Police?

It should only be CFS or the Police if the activity constitutes authorised, directed, covert surveillance as defined above, and is for the purpose of the prevention or detection of crime. This is because CFS are the only part of the NHSS, being a relevant public authority, regulated and authorised to carry out this activity in these circumstances, and remain compatible with the Human Rights Act 1998.

When HR colleagues or line manager's access 'private information' or 'personal data' online, for a legitimate business purpose; is this legal, if carried out in line with local policy?

It is unlawful for a public authority to act in a way which is incompatible with a Convention Right (Human Rights Act 1998 section 6.1).

If HR colleagues or line managers suspect criminal activity such as fraud, forgery & uttering, embezzlement, bribery & corruption, certain kinds of theft, please refer to the answer to Q.5
If this is for some other legitimate business purpose, then reference should be made to the relevant national NHSS, and local Health Board and public sector policies. Case specific guidance may also be sought from CLO as required, or your information governance and data protection officer. It may also be necessary to contact the Police for advice about accessing private information online, in relation to reports or suspicions about other types of criminal conduct, not dealt with by CFS.

Where else can colleagues get reliable sources of advice regards accessing private information online in the course of their duties?

Specific advice can be provided by Central Legal Office; the ICO Employment Practices Code November 2011, Chartered Institute of Personnel & Development (www.cipd.co.uk) or your local information governance/data protection adviser/officer.

What should public sector organisations do with any private information/personal data obtained by managers or HR colleagues from these kinds of online sites?

If possible you should ask your local information governance or data protection adviser/officer what should be done with any private information obtained in these circumstances, before any action is taken to further process or destroy it.

Should we contact CFS if we are unsure in particular circumstances?

Yes, we would recommend you contact your Fraud Liaison Officer in the first instance or CFS for an informal discussion.

Contact: cfscommunications@nhs.net

Visit our website for more information on all of our services www.cfs.scot.nhs.uk

Follow us @NHSSCFS

Fraud.
Together we can stamp it out.

Fraud Hotline
08000 15 16 28
Powered by Crimestoppers
cfs.scot.nhs.uk