General Dental Council

Covert surveillance in practice: Guidance on conducting surveillance in fitness to practise and illegal practice investigations

Dated: September 2023

Version: 1

Contents

Version control

Version	Date	Author	Change
1.0	23 September 2023		

Covert surveillance in practice:

Guidance on conducting surveillance in fitness to practise and illegal practice investigations

Introduction

1. Under the Dentists Act 1984 ("the Act"), the General Dental Council's (GDC) over-arching objective is to protect the public. It achieves this by pursuing the following three objectives:

   (i) to protect, promote and maintain the health, safety and well-being of the public
   (ii) to promote and maintain public confidence in the professions it regulates, and
   (iii) to promote and maintain proper professional standards and conduct for members of those professions.

2. In accordance with this statutory objective, the GDC has responsibility for investigating allegations of impaired fitness to practise made against registered dental professionals ("registrants"). This function is performed by the Fitness to Practise Casework teams within the GDC's Regulation directorate, who, at the conclusion of each investigation, will assess whether the conduct alleged amounts to allegation(s) of impaired fitness to practise.

3. The Act also creates a number of criminal offences involving the illegal practice of dentistry or purported practice of dentistry by unregistered individuals. Investigations into reports of illegal practice are undertaken by the GDC's In-House Legal Advice Service (ILAS) and in the most serious cases, can result in a private criminal prosecution being brought against the individual concerned.

4. It will be very rare for the GDC to use covert surveillance techniques to support fitness to practise and illegal practice investigations. On each occasion, it will require a decision that balances the seriousness of the intrusion into the privacy of the subject of the investigation against the need for/value of the activity for the investigation. Authorisation requires the proposed surveillance to be legal, necessary, proportionate, and not arbitrary.

5. This document provides guidance to GDC staff on when covert surveillance techniques may be used to support investigations and where these techniques are used, the process that should be followed. ***Given the legal risks associated with covert surveillance techniques, it is recommended that this guidance is read in full before authorisation is sought.***

Purpose

6. The purpose of this guidance is to:

   (i) set out the law relevant to the use of covert surveillance by the GDC in fitness to practise and illegal practice investigations
   (ii) provide an overview of what amounts to surveillance and when authorisation is required
   (iii) set out the GDC's procedure for authorising covert surveillance methods, including the use of investigators for in-guise investigations
   (iv) promote investigatory practices that are compliant with the European Convention on Human Rights (ECHR)
   (v) avoid unlawful interference with the rights of individuals.

7. This guidance will be reviewed every two years.

The legal framework

8. The key legislation governing covert surveillance is:

   (i) the Human Rights Act 1998 (the HRA)
   (ii) the Regulation of Investigatory Powers Act 2000 (RIPA), and
   (iii) the Data Protection Act 2018 and the UK General Data Protection Regulation (the UK GDPR).

The HRA

9. The HRA incorporates the rights and freedoms established by the ECHR into national law. As the GDC is a public authority, it, and persons delivering functions on its behalf, must comply with the HRA.

10. Article 8 of the ECHR states "*everyone has the right to respect for his private and family life, his home and his correspondence*". Any investigation which involves compiling and storing information about an individual and their working practices is likely to intrude into the private sphere. Article 8 will accordingly be engaged when the GDC is seeking to obtain private information by means of covert surveillance. Article 8 is also engaged when an investigator, posing as a customer seeking treatment, forms a "relationship" with the subject of an investigation.

11. Article 8 does not confer an *absolute* right to privacy. This means that in certain circumstances interferences with that right by a public authority can be justified. However, the public authority must be able to show that the interference is lawful and necessary for one of the specified legitimate aims set out in the HRA.

12. For the purposes of the GDC's fitness to practise remit, only ***the protection of public safety*** and ***the protection of health*** may be relied on as legitimate aims.

13. In relation to illegal practice investigations, the GDC may additionally rely on ***the prevention of disorder or crime*** as a legitimate aim.

RIPA

14. RIPA provides a statutory framework under which covert investigatory techniques may be authorised at an appropriate level within designated public authorities, so that these techniques may be used in a way that is compatible with Article 8 of the ECHR. For those public authorities covered by RIPA, compliance with its authorisation provisions is not mandatory, but it provides a record of the lawful basis for using covert investigatory techniques. Compliance also provides protection from legal liability, whether under the HRA or otherwise.

15. Use of covert investigatory techniques will only be authorised if considered lawful, necessary, and proportionate. Authorisation will be considered necessary – i.e. unachievable by less invasive means – if the use of covert investigatory techniques is required for one or more of various specified purposes set out in the RIPA.

16. For the purposes of the GDC's fitness to practise remit, only ***the interests of public safety*** and ***the protection of public health*** may be relied on as legitimate aims.

17. In relation to illegal practice investigations, the GDC may additionally rely on ***the prevention or detection of crime or disorder*** as a legitimate aim.

18. RIPA is supported by two pieces of statutory guidance issued by the Home Office. These are:

    (i) The revised Code of Practice on Covert Surveillance and Property Interference. This provides guidance on authorisation of covert surveillance likely to result in obtaining ***private information*** about a person. This includes, for example, online surveillance. The Code provides guidance on when an application should be made for an authorisation and the procedures that must be followed before the activity takes place. The Code also provides guidance on the handling of any information obtained by surveillance activity; and

    (ii) The revised Code of Practice on Covert Human Intelligence Sources. This provides guidance on the authorisation of the ***use or conduct of covert human intelligence sources*** (CHIS). The Code also provides guidance on the handling of any information obtained by use or conduct of a CHIS.

Data Protection

19. The way data is gathered, held, and processed is regulated by the Data Protection Act 2018 and the UK GDPR. It is important that the GDC's investigations, covert or otherwise, are fully compliant with both pieces of legislation. This guidance does not extend to the provisions of data protection legislation, but this is directly relevant to how the GDC processes information obtained from covert surveillance.

The GDC's approach to covert surveillance and its authorisation

20. The GDC is not a designated public authority for the purposes of RIPA. However, the GDC considers any covert surveillance it undertakes should comply with the spirit of RIPA and its authorisation framework. This is to ensure that appropriate consideration is given to the ***necessity*** and ***proportionality*** of the surveillance methods it proposes to use.

21. This reduces the risk that the GDC's actions, which it takes in pursuit of its statutory aims, will be seen as incompatible with Article 8 of the ECHR and therefore liable to successful legal challenge.

22. ***Where investigations can be conducted without the use of covert surveillance, they must be. The least intrusive method of investigating should always be preferred.***

What is surveillance and when is authorisation required?

23. **Surveillance** involves monitoring, observing, recording, or listening to people, their movements, conversations or other activities and communications, with or without use of a surveillance device. Surveillance may be:

    (i) Covert: where it is carried out in a manner calculated to ensure that anyone subject to the surveillance is unaware that it is taking place. Covert surveillance can be either directed or intrusive (see below).
    (ii) Overt: where it is carried out in a manner that is not secretive, clandestine, or hidden.

24. In many cases, investigators working on behalf of the GDC will be going about the GDC's business openly. Such overt activities do not require authorisation under the process set out in this guidance and its appendices.

25. There are two main types of covert surveillance: directed and intrusive surveillance.

26. **Directed surveillance** is surveillance that is:

    (i) covert, but not intrusive, surveillance
    (ii) it is conducted for the purposes of a specific investigation or operation
    (iii) it is likely to result in the obtaining of ***private information*** about a person (whether or not such a person is specifically identified for the purposes of the investigation or operation), and
    (iv) it is not an immediate response to events or circumstances such that it would not be reasonably practicable to seek authorisation.

27. **Intrusive surveillance** is covert surveillance that is:

    (i) carried out in relation to anything taking place on any ***residential premises***, or
    (ii) in any ***private vehicle***, and

(iii) it involves the presence of an individual on the premises, or in the vehicle, or
(iv) it is carried out by means of a surveillance device.

Directed surveillance

28. In summary, therefore, directed surveillance is planned, covert, but not intrusive surveillance, and is likely to result in the obtaining of ***private information*** about a person.

What type of information is considered private information?

29. **Private information** includes any information relating to a person's private or family life. It generally includes any aspect of a person's private or personal relationship with others, such as family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and address details.

30. Individuals can have a reasonable expectation of privacy even though acting in public. While 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 includes surveillance of publicly accessible areas of the internet, such as social media websites. Where a record is being made by a public authority of an individual's activities for future consideration or analysis this is likely to amount to private information. Whether a reasonable expectation of privacy exists in a particular setting depends on all the relevant circumstances. Essentially, the more private the setting and the more personal the information which will be recorded the more likely such an expectation is to arise.

31. Where different records or pieces of information – whether or not publicly available – are analysed together, for example, to establish a pattern of behaviour, or to create a record about a person, for the purpose of fitness to practise or illegal practice investigations, the totality of information obtained may constitute private information even if the individual records or pieces of information do not. If you are in any doubt, please seek guidance from your line manager in the first instance or seek advice from a member of ILAS by email.

32. Where private information is likely to be obtained from covert surveillance of a person who has a reasonable expectation of privacy, a ***directed surveillance authorisation*** is appropriate.

Intrusive surveillance

33. The definition of surveillance as ***intrusive*** relates to the location of the surveillance – carried out in residential premises and/or private vehicles – and not to the type of information expected to be obtained. It is assumed intrusive surveillance will likely always result in obtaining private information.

Residential premises

34. **Residential premises** are premises that are being occupied or used by any person, including temporarily, for residential purposes or otherwise as living accommodation. Examples would include hotel accommodation, but not common areas. Premises also include any vehicle or moveable structure.

35. Examples of premises which would ***not*** be regarded as residential include:

    (i) Communal stairways in a block of flats
    (ii) A front garden or driveway of premises readily visible to the public
    (iii) An outbuilding to a residential property (such as a garage or shed) that has been converted for commercial reasons and can be accessed directly from the street.

36. Intrusive surveillance may only be authorised under RIPA where it is necessary:

    (i) in the interests of national security
    (ii) for the purpose of preventing or detecting ***serious*** crime, or
    (iii) in the interests of the economic well-being of the UK.

    GDC investigations will never meet any of those three tests, so ***intrusive surveillance should never be undertaken.*** See below guidance relating to 'mixed use' premises.

In-guise Investigations

37. **In-guise investigations** (for example, investigators posing as patients to gather information about practitioners) are a form of ***covert*** surveillance. As such, authorisation should be sought before any covert surveillance activity takes place.

38. In-guise investigations will require the use of a **covert human intelligence source** (CHIS). Therefore, any application for authorisation should also include approval of a CHIS.

What is a CHIS?

39. A person is a CHIS if they set up or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything which is covered by the following:

    (i) they covertly use a relationship to obtain information or to provide access to any information to another person, or
    (ii) they covertly disclose information obtained using such a relationship or as a consequence of the existence of such a relationship.

40. In-guise operations often start with an investigator, posing as a patient or interested member of the public, making an approach to the registrant through their website, by email or via social media. This initial contact is aimed at eliciting information and will

usually prompt, or at least be aimed at prompting, some form of meeting. A CHIS authorisation would therefore be required before such interaction begins.

41. Authorisations for the use of or conduct of a CHIS are required if there is to be covert manipulation of a relationship to obtain *any* information and not just private information.

42. ***Authorisation should be obtained for the use or conduct of a CHIS before they are instructed***. Authorisation should cover, in broad terms, the nature of the CHIS' task to obtain information.

43. Looser interaction – for example, open-source online research, website registration to gain access to a site, online purchasing without entering into direct correspondence or leaving feedback, electronic gestures such as friending, liking, and following – will not usually involve the establishment of a relationship and, therefore, would not trigger the need for a CHIS authorisation.

44. The CHIS authorisation procedure does not apply where members of the public volunteer information as part of their normal civic duties. Nor is it intended to apply to contact numbers set up to receive information e.g., the illegal practice or fitness to practise complaints webform or the Dental Complaints Service telephone enquiry line. Therefore, members of the public or registrants reporting concerns by these means would not generally be regarded as sources.

45. However, consideration should be given to whether a ***directed surveillance authorisation may still be required if the intention is to monitor and/or systematically collect and record online information about an individual***, as this is likely to be directed surveillance. If you are unsure whether your actions might constitute directed surveillance and therefore require authorisation in advance, please speak to your line manager in the first instance, or seek advice from a member of ILAS by email.

Mixed use premises

46. It is increasingly common for registrants to practise not from purely business premises (e.g., a traditional dental surgery) but wholly or partly from some form of residential premises. These might be premises within or adjacent to the individual's home, but adapted for clinical practice; for example, a garage, workshop, shed or even spare bedroom operating as a workshop and accessed through areas devoted to purely residential accommodation.

47. Distinct self-contained areas which are part of a property but accessed separately (for example, a ground floor workshop below a first floor flat or a garage accessed around, rather than through, a domestic dwelling) are less likely to be considered residential premises than premises where access to the adapted clinical area is via areas devoted purely to residential accommodation. Surveillance of the latter will usually be more intrusive and will accordingly require even greater justification than surveillance of the former.

48. ***If premises are used as a dental surgery or laboratory, within or alongside a home, and become subject to investigation, this should not preclude or constrain investigations that would otherwise be warranted***. It would be contrary to the GDC's statutory objectives and the public interest for the registrant's choice to practise from such premises to undermine the effective performance of the GDC's regulatory functions. However, the investigation process will need to be sensitive to any dual or parallel use of any premises, and to their likely proximity to unconnected persons (such as the registrant's family or other third parties). Therefore, special care should be taken to ensure they are not affected – something that should be considered and addressed when authorisation for covert surveillance is being sought.

49. Surveillance carried out in mixed use premises where the business "areas" of the property are within or alongside a home and where access is not distinct and separate to the residential areas will accordingly require additional care and clear justification in the authorisation request which addresses the dual or parallel use of the premises.

Online Covert Activity (Online monitoring and surveillance of websites)

50. The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation and is likely to result in the obtaining of private information, ***an authorisation request for directed surveillance should be made***.

51. **A CHIS authorisation** will be needed where the intention is to engage others online without disclosing the identity of the investigator, whether this is via publicly open websites, such as an online news and social networking service, or using more private exchanges, such as e-messaging sites or direct messaging on social media websites (Instagram direct message, Facebook Messenger etc).

52. A separate directed surveillance authorisation would not be necessary if the acquisition of the information will be covered by the terms of the CHIS authorisation.

53. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the other person(s) knowing that the surveillance is or may be taking place.

54. As stated above in paragraph 45, whilst there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, in some circumstances privacy considerations may still apply if the intention is to monitor and/or systematically collect and record online information about an individual. However, individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are less likely to hold a reasonable expectation of privacy in relation to that information.

55. Also, where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is

commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring of that information.

56. Simple reconnaissance of such sites (i.e., preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy. Therefore, it is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered.

57. In summary, to determine whether authorisation should be sought for accessing information on a website as part of a covert investigation, it is necessary to consider the intended purpose and scope of the online activity proposed. Factors that should be considered include whether:

    (i) the investigation or research is directed towards an individual or organisation
    (ii) the investigation or research is likely to result in obtaining private information about a person or group
    (iii) the investigation or research is likely to involve visiting internet sites to build up an intelligence picture or profile
    (iv) the information will be recorded and retained
    (v) the information is likely to provide the observer with a pattern of an individual's lifestyle
    (vi) the information is being combined with other sources of information or intelligence, which is information relating to a person's private life
    (vii) the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s)
    (viii) the investigation or research is likely to involve identifying and recording information about third parties, such as friends and family members of the subject, or information posted by third parties, that may include private information and therefore, constitute collateral intrusion into the privacy of these third parties.

    Depending on the circumstances, it may be that the presence of one factor, or a combination of factors, may amount to directed surveillance and require authorisation.

58. If you are unsure whether your actions might constitute directed surveillance and therefore require authorisation in advance, please speak to your line manager in the first instance, or seek advice from a member of ILAS by email.

Authorising officers and requests for authorisation

59. Through this guidance document and its appendices, the GDC is implementing an authorisation procedure for covert surveillance that accords with the spirit of RIPA and the Home Office guidance.

60. Where the GDC is proposing to use covert surveillance methods for a fitness to practise or illegal practice investigation, this authorisation procedure provides a safeguard, ensuring that any intrusion into the private lives of individuals under investigation is done only when it is deemed necessary (that is, unachievable by less invasive means), proportionate to what is sought to be achieved; and not arbitrary (that is, carried out in accordance with prescribed and proper procedures).

61. The GDC will balance the seriousness of the intrusion into the privacy of the subject of the investigation (or any other person who may be affected) against the need for/value of the activity for its investigation.

62. Any covert investigation method will receive proper prior consideration at an appropriately senior level, by someone outside the investigation team.

63. The power to grant, extend and discontinue authorisations will be restricted to an Authorising Officer, to ensure greater independence and consistency in decision-making. For this reason, Authorising Officers generally should not be responsible for authorising investigations in which they are directly involved. Contact ILAS by email for a full list of GDC Authorising Officers.

64. All requests to conduct, extend or discontinue a covert surveillance activity shall be authorised in accordance with the guidance included with the Authorisation Request Forms for illegal practice and fitness to practise. Contact ILAS by email for an Authorisation Request Form.

Working with/through other agencies

65. When another agency has been instructed on behalf of the GDC to undertake any action envisaged by this guidance, this document, and the annexed Authorisation Request Forms must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made ***explicitly*** aware of what they are and are not permitted to do.

Complaints

66. Any person who reasonably believes that they have been adversely affected by any activities carried out pursuant to this guidance by or on behalf of the GDC may complain to the Executive Director, Regulation, who will arrange for the complaint to be investigated and reviewed an Executive Director not involved in any approval process.

September 2023