



Association of British Insurers

GUIDELINES

on the instruction and use of
PRIVATE INVESTIGATORS

September 2014

CONTENTS

FOREWORD	2
-----------------	----------

SCOPE	3
--------------	----------

BACKGROUND	4
Investigation of insurance claims	4
The views of the Government and the Regulators	4

PRIVATE INVESTIGATORS (PIs)	5
Considering the use of a PI	5
Due diligence checks	6
Entering into a relationship with a PI	7
Fair processing wording	11
Instruction to the PI	12
Access to data collected by a PI	12
Retention of data collected by the PI	13

AUDITING	14
-----------------	-----------

MANAGEMENT INFORMATION	14
-------------------------------	-----------

FCA REGULATORY REQUIREMENTS	15
------------------------------------	-----------

FOREWORD



OTTO THORESEN
Director-General,
Association of British Insurers (ABI)

People rightly want to ensure that their privacy is protected. At the same time they do not want to pay more for their insurance because others are getting away with fraud and theft. Insurers have to strike the right balance, respecting privacy whilst doing all they can to prevent fraud which adds around £50 to the average household's annual insurance premiums.

To protect the interests of policyholders, it is sometimes necessary for an insurer to use a private investigator (PI) in appropriate circumstances to check whether or not a claim is genuine or for other purposes including other liability investigation matters. When this step is taken, it must be taken with care. It is simply not enough to employ a PI just because it 'gets results' - any organisation that fails to check the credentials and working practices of a PI runs the risk of falling foul of the law, not meeting their regulatory requirements, facing prosecution and dealing with the associated reputational damage.

It isn't just about finding the cheats or determining liability. Insurers will also use tracing agents to find beneficiaries who are due windfalls from long-forgotten policies. Insurers will expect the same high standards to apply to tracing agents, as they do to PIs.

Insurers should also remember that they too can be the victims of deception perpetrated by individuals operating illegally to obtain personal information for financial gain. So staff, particularly those in call centres and claims departments, should be suitably trained and robust controls should be in place to safeguard personal and sensitive data. The ABI has consulted with the Financial Conduct Authority in developing this guidance, as well as with the Information Commissioner and the Association of British Investigators with whom we worked in developing the original version published in July 2007.

The guidance should provide further reassurance about how insurers use the services of reputable PIs in a proportionate way, while respecting the right to privacy.

SCOPE

These guidelines apply to the instruction of PIs by insurers or their appointed lawyers or other authorised agents in the United Kingdom. They are intended to provide a framework for insurers to devise their own procedures for investigating claims from policyholders and third parties. The guidelines are designed to deliver a framework where insurers appoint with confidence only PIs who operate within the confines of the law and to high ethical standards.

For claims which are handled on behalf of an insurer by an appointed law firm or authorised agent, any investigations which include the appointment of a PI must be approved by the instructing insurer before such appointment is made. This applies equally for claims at the pre or post litigation stage. We would ordinarily expect law firms and authorised agents to only appoint PIs who are already contracted with the insurer and use the same instruction process for a claim where a PI is appointed directly by the insurer.

This guidance is not confirmed by the Financial Conduct Authority (FCA). However, the FCA, the Information Commissioner's Office (ICO) and the Association of British Investigators have been consulted in the development of the guidance. Adoption of the guidelines is voluntary and entirely at the discretion of each individual insurer.

BACKGROUND

Investigation of insurance claims

The vast majority of insurance claims are not subject to investigation for fraud purposes. Of those that are, most are conducted by in-house insurer counter-fraud specialists covered by FCA regulation (see Annex – FCA Regulatory Requirements), or chartered loss adjusters who are subject to their own professional standards. Most investigations are carried out with the knowledge of the claimant and will often involve standard checks against fraud indicators, open source data (e.g. social media) and industry databases, which the customer has usually been told about at inception of the policy and the third party claimant at the point of making the claim. Fraud indicators and database searches may lead to a personal interview of the customer and/or claimant which can allow the interviewer to obtain comprehensive information directly from the person making the claim which, when required, is an invaluable line of enquiry. Face-to-face interviews also allow insurers to evaluate behavioural traits displayed by the interviewee.

In 2013, insurers uncovered dishonest insurance claims worth £1.3bn. Despite the insurance industry investing around £200m every year to counter fraudulent activity, it is estimated that more than £2bn of insurance fraud goes undetected each year, adding around £50 to every household's annual insurance premiums. It is incumbent upon insurers to do all that they can to protect honest customers against the actions of fraudsters and thieves. It is therefore sometimes necessary to conduct covert investigations.

The views of the Government and the Regulators

WHAT PRICE PRIVACY?

This ABI guidance was first published in July 2007, in response to concerns raised by the Information Commissioner. In May 2006, the Information Commissioner published 'What price privacy?' This report highlighted the existence of a widespread trade devoted to illegally buying and selling personal information causing significant distress, intrusion and harm to individuals. The report identified the insurance industry as one of the sectors with an apparent incentive to acquire confidential personal data, particularly in respect of suspect claims. While these activities already constitute offences under Section 55 of the Data Protection Act (DPA), the report proposed a substantial increase in penalties, including custodial sanctions.

In December 2006 the Information Commissioner published a further report, 'What price privacy now?' that set out the reactions from the media, the security industry, financial bodies and the Government to the initial report. Many organisations have taken positive steps to raise awareness and tighten security. The report explicitly acknowledged the work that the Association of British Insurers (ABI) undertook, which culminated in the publication of the 2007 ABI guidance. The FSA stated that compliance with all relevant legislation is necessary in order to meet the authorisation threshold criteria for firms to act in a fit and proper way. The ICO advised that it would make the FSA aware of any regulated firms that are convicted of Section 55 offences. The Information Commissioner has subsequently campaigned for heightened enforcement powers in relation to Section 55 offences, including custodial sanctions.

LEVESON INQUIRY

The use of private investigators attracted much media attention throughout 2013, fuelled by the Leveson Inquiry and the Home Affairs Select Committee's investigation into the 'SOCA list' (subsequently taken forward by the Information Commissioner).

REGULATION OF PRIVATE INVESTIGATORS

On 31 July 2013, the Home Secretary announced proposals to introduce the regulation of private investigators with effect from autumn 2014. This will require private investigators to obtain a licence, which will only be granted by the Security Industry Authority (SIA) when an applicant has successfully completed due diligence checks¹, training and achieved a Government recognised qualification. Operating as an unlicensed PI or supplying unlicensed PIs will become criminal offences punishable by a fine of up to £5000 or up to six months in prison. While the timetable for introducing regulation has slipped, the Home Office still expects it to become a criminal offence for a private investigator to operate without a licence sometime during 2015.

FCA THEMATIC REVIEW

During 2013, the FCA undertook thematic work looking into how the insurance sector uses PIs. While the FCA recognises that PIs are valuable to insurers (and their customers) in identifying fraudulent claims, they wish to ensure that insurers meet regulatory requirements (see Annex – FCA Regulatory Requirements) when outsourcing work to PIs. The findings of the FCA review were published in a factsheet on 1 October 2013 and have been taken into account in revising this guidance.

¹ The proposed individual licensing will only check criminality at Standard Disclosure level. It is not a zero tolerance policy. Recency and relevance of criminality will also be considered. The SIA is understood to be committed to follow individual licensing with a business licensing regime. It is expected that for the PI sector this will be based on the BSi Code of Practice for the provision of investigative services [BS102000/2013] which includes due diligence checks and good practice following the Association of British Investigators model.

PRIVATE INVESTIGATORS (PIs)

Considering the use of a PI

There are many different reasons why an insurer might employ the services of a PI. These include undertaking surveillance in relation to a fraud investigation; credit hire enquiry services; tracing services to support motor recovery claims or to find beneficiaries under life policies; motor theft and accident enquiries; vehicle enquiries; claims screening and training.

The use of PIs for surveillance purposes will occur in two main instances: first, where an insurer has good grounds to suspect that a customer or third party claimant is inventing or grossly exaggerating a one-off claim and cannot reasonably accept the evidence presented; and second, where organised fraud is suspected and alerting the suspected fraudster might prejudice other investigations, including those conducted by the police. Such investigations are most often used where there is scope to fabricate or exaggerate bodily injury, or in some cases of organised property damage (e.g. motor 'crash for cash').

The use of PIs for surveillance, by its very nature, is likely to be an intrusion into that individual's privacy. So a PI should only be employed where there is reasonable suspicion that the claim might be fraudulent or there are reasonable grounds for requiring validation of a claim and the information they can obtain using surveillance is deemed appropriate and necessary under the circumstances. When an insurer is considering whether or not to instruct a PI to investigate an individual, it should consider all other options first, such as using other sources of information available to the insurer and assess whether information gathering by the PI is strictly necessary. Only after this evaluation should an insurer consider instructing a PI. Certainly the use of surveillance should not be considered as the first and only response. The purpose of surveillance, as recognised by the courts, is to obtain independent, objective evidence in order to prove, disprove or validate a claim. Properly authorised surveillance is often the only effective method of securing the evidence necessary for a fair trial.

There might be circumstances where the use of a PI might not be an appropriate or the best way of confirming the validity of a claim, for example, because an individual is alleging an illness that could not be verified through surveillance of that individual. So the insurer should consider what alternative courses of action might be appropriate in the particular circumstances of the case. For example, there are a number of research tools available to the insurer that can play an important role in the claims validation process. These include underwriting and anti-fraud databases including, but not limited to, the Insurance Fraud Register, the Claims and Underwriting Exchange (CUE), CIFAS (the UK's financial fraud prevention service), and credit reference agency databases. In relation to bodily injury claims, insurers can also obtain much useful information from independent medical reports.

In some cases the information that may impact upon a claim cannot be obtained by surveillance of the individual, but is held securely by another organisation for its own purposes. Obtaining personal information knowingly and recklessly without the consent of the claimant or the organisation that holds it, either by deception or bribery, is a criminal offence under Section 55 of the DPA. An insurer instructing a PI to gather information that could only reasonably be obtained by these means may be committing a criminal offence, as will the PI.

Where another organisation holds information that is necessary for the insurer to investigate a fraud, and is not available from other legitimate sources, it should be approached directly by the insurer or its agent. It will then be for that organisation to decide whether or not to disclose the relevant information to the insurer or their agent. The organisation approached would have to be satisfied that they had a legitimate basis for the disclosure.

In respect of cases of suspected fraud, the insurer should apply a bespoke strategy to manage each claim (to be signed-off at senior level). This can help to ensure that PIs are only appointed in appropriate circumstances.

Due diligence checks prior to the appointment of a PI

Before a PI is employed the insurer should undertake appropriate due diligence, taking account of relevant FCA regulatory requirements (see Annex – FCA Regulatory Requirements). This should include performing an impact assessment; and it is recommended that a ‘reason for instruction’ note should be completed, documented and retained. Areas to be assessed and included are:

WHAT ARE THE INSURER’S GROUNDS FOR SUSPICION?

The insurer should state why it believes that the claim might not be genuine.

WHAT MEANS HAVE BEEN EXPLORED, OTHER THAN THE USE OF A PI, TO VERIFY THE INSURER’S SUSPICIONS?

A PI should only be used to undertake surveillance where there is reasonable suspicion that the claim is not genuine. The insurer should always consider what information it already has at its disposal, or may gain access to, before instructing a PI.

WHAT INFORMATION NEEDS TO BE DISCLOSED TO THE PI SO THAT HE CAN FULFIL HIS INSTRUCTIONS?

Only the minimum information necessary to allow the PI to perform their task should be provided to them. Each case should be assessed on its individual merits. The PI will require sufficient background in order to provide context for their investigation. It might be acceptable ordinarily to provide a brief summary of the injury and any alleged disability or inability to perform basic tasks. But it will ordinarily be inappropriate, for example, to inform the PI of the ailment that the claimant is suffering, particularly where this would involve disclosing sensitive data such as an actual illness. The insurer should instead generalise. For example, the PI may be asked to assess the way in which the claimant acts and may

ask for evidence of particular activity (e.g. the claimant may have difficulty lifting objects or should not be driving). If the insurer is aware that the individual under investigation could potentially endanger the PI, then the PI should be forewarned.

Whilst the disclosure of sensitive personal data to a PI should be carefully considered², and a risk assessment should be completed before doing so, in some circumstances it may be necessary to inform the PI of the illness, for example in cases of depression, panic attacks, chronic fatigue, incontinence or agoraphobia.

With personal injury cases, it is often necessary to disclose the location on the human body of the injury so that video footage is properly focused on the areas and activity relevant to the claim.

WHAT INFORMATION WOULD BE REQUIRED FROM THE PI TO VERIFY SUSPICION?

The insurer should only request the PI to obtain information that is reasonably necessary to establish the status of the claim and should not request information that could only be obtained by deception or bribery. As part of its assessment the insurer should consider what information is required and why it is justified.

This might include:

- 1. Pre-surveillance enquiries** – the insurer might ask the PI to undertake pre-surveillance enquiries to verify the identity of the claimant under investigation, to establish whether it is likely that the claimant travels to a place of employment, their general demeanour and physical capabilities and such other pertinent information as may be appropriate. Such enquiries should only be used in very carefully controlled exceptional circumstances – they should never be a routine activity. If relevant, justified and proportionate, the PI might visit the locality of the claimant’s place of residence to make enquiries

² Medical reports, pay slips and salary details are deemed to be sensitive personal data and should never be disclosed to PIs.

of neighbours or at the property directly. The First Data Protection Principle requires personal data to be obtained fairly and lawfully. Such enquiries carry an element of risk and should be considered very carefully before they are undertaken. Overt enquiries e.g. “Does Mr S live here?” are likely to put the claimant on notice that he is under investigation. Covert enquiries carry the risk of reputational damage or even the enactment of a criminal offence if they are deemed to breach Section 55 of the DPA. The ICO would expect a detailed audit trail to be kept of the authorisation and investigation so that the insurer can fully demonstrate its reasons for using a PI and authorising pre-surveillance enquiries.

2. **Desk-based profiling of claimant** - the PI will usually need to verify where the individual lives, and that the person lives at the address supplied. This might, for example, be obtained by cross checking against the electoral roll. Not knowing the individual's address might lead to the privacy of an innocent person being breached if the wrong information is supplied. The PI might also be instructed to carry out County Court Judgment (CCJ) screening; Directorship/Company Secretary searches; other anonymised internet searches of databases; business websites; user derived content websites and social networking sites; and police telephone enquiries³.
3. **Photographic evidence** – the insurer should consider whether photographic evidence is required for positive verification
4. **Film evidence** - this might, for example, demonstrate the claimant's level of mobility or that the claimant is working. The original DVD/CD/memory stick should be from virgin stock (i.e. new and unused). The original media should never be edited under any circumstances, but copied to provide working copies. The original media should be labelled, sealed and numbered as an exhibit

and retained securely for production in court or forensic examination as necessary. Individual agents employed by insurers should never be permitted to copy or edit their own footage as this militates against an integrity audit trail. It may be necessary to edit the evidence (e.g. to preserve the anonymity of a minor). If working copies are to be edited and the insurer has a specific preference as to how it wants the evidence edited, the insurer should stipulate this at the time of instruction.

5. **PI Report** – this might be required, for example, to register the claimant's movements and may include the PI's surveillance activity log.
6. **Other physical evidence** – such as advertisements offering services, invoices or receipts.

Entering into a relationship with a PI

The insurer, appointed law firm or third party claims administrator acting on behalf of the insurer should ensure that it chooses a PI that will act in an appropriate manner, both in compliance with the law and with standards of ethics, and explicitly require the PI to do so. Prior to entering into a formal business relationship, the insurer might consider sending the PI a due diligence questionnaire. This might cover background issues such as past and present personal and business financial standing; evidence of compliance with relevant laws and a consumer-centric approach; security; training and skills; quality assurance; disaster recovery⁴ and membership of a reputable trade association, as well as any other factors that are normally reviewed and considered as part of any outsourcing procurement review. If the response to the questionnaire is satisfactory, then the insurer should also conduct a site visit to the trading offices of the PI. Where the insurer has an ongoing business relationship with the PI, it is recommended that the insurer requires the PI to complete an annual due diligence questionnaire.

³ Enquiries of the police are legitimate where, for example, the interest of the police in the person who is the subject of the investigation is known and related to the claim. Police officers can also be formally interviewed for the likes of motor vehicle accidents.

⁴ These are characteristics of the Association of British Investigators Code of Practice, now also covered in BS102000/2013.

Whether a PI is a data processor or a joint data controller will depend upon the exact terms of engagement. However, most PIs act as data processors and will obtain information under clear instruction from the insurer. It is strongly recommended that there is an appropriate written agreement or contract between the insurer and the PI, so as to comply with the requirements of the DPA. Without such a formal arrangement being in place, it is difficult to see how an insurer could limit any additional use of the information, confine its disclosure, ensure its secure destruction at an appropriate time and confirm that appropriate security arrangements are in place. The advantages of a formal agreement or contract include that it:

1. Ensures that the insurer complies with the requirements of the DPA.
2. Protects the insurer from financial liability in the event of the insurer being sued and risk to reputation.
3. Provides certainty as to the extent of the PI's remit.
4. Provides guidelines for the security of documents and information.
5. Forms a basis for recovering damages against the PI in the event of improper conduct by the PI.

It should be noted that if a PI, when acting on behalf of an insurer, knowingly and recklessly obtains personal information without the consent of the organisation that holds it, this may be an offence under Section 55 of the DPA. In these circumstances, the Information Commissioner may investigate both the PI and the insurer with a view to prosecution. For this reason, and to ensure compliance with "Treating Customers Fairly", it is important that the insurer leaves the PI in no doubt that they are to obtain information by legal means and in accordance with high ethical standards only. It should do this in its instructions and any ongoing contact around the investigation of the case.

In deciding on the terms of the written agreement, the insurer should be mindful of the requirements laid down by FCA regulation (see Annex - FCA Regulatory Requirements – in particular, SYSC 13.9.5G).

The insurer, or appointed law firm or authorised agent, should consider including the following provisions⁵ in any agreement entered into with the PI:

1. The PI company's employees engaged in the provision of the services should be suitably qualified, skilled, experienced, and trained. Many PIs may be involved in activities that are unconnected to insurance claims investigations. So the insurer should ensure that the PI fully understands what is required of him in the particular case. The insurer might wish to establish what checks the PI company undertakes of staff prior to recruitment and should consider seeking references and specimen reports.
2. The PI company and its employees should hold any licences required by legislation.
3. The PI company and its employees should act in accordance with all applicable laws, rules, regulations and codes of practice, including in relation to health and safety, (hereinafter referred to generically as 'The Act') relevant to the services provided.
4. The PI company should maintain adequate systems and controls to ensure that all of its personnel receive adequate training and are properly supervised in relation to requirements of the contract, the Act and health and safety. Records should be kept of all training and insurers should seek evidence of regular testing of PI companies' staff on their knowledge of relevant legislation, regulation and policies.
5. The PI company should perform all services to the same standards as if they were all regulated activities, notwithstanding that some services will not be regulated activities.
6. The contract should clearly set out the basis on which the PI company is being remunerated and how matters relating to breaches of contractual terms and conditions are to be remedied.
7. The PI company should hold adequate professional indemnity insurance. This reduces the risk borne by the insurer and provides a degree of comfort that the PI company has demonstrated a level of professionalism. It should also hold other relevant

⁵ The provisions contained in sub-paragraphs 1-15 are characteristics of the Association of British Investigator's Code of Ethics and Professional Standards, now also covered in BSI 102000/2013.

insurances as appropriate, such as employers' liability and public liability.

8. The PI should complete only the provision of services requested and retain the personal information involved for no other purpose.
9. The PI company should obtain prior agreement from the insurer before sub-contracting to an agent in fulfilling the provision of the service. The insurer should reserve the right to carry out due diligence on any sub-contractors and ensure that a suitable agreement is in place between the PI company and the sub-contractor.
10. The PI company should take appropriate steps to ensure that if it sub-contracts to other agents in the provision of services to the insurer, those agents are bound by the same requirements as the PI. This should include full awareness training, and periodic testing, about the Act and the legal obligations that arise from it.
11. The PI company should take appropriate steps to ensure that its employees comply with the DPA when obtaining, using and disclosing the data.
12. The PI company should take appropriate steps to ensure that neither it or any of its employees or agents shall use any data other than in connection with the provision of services as instructed by the insurer and should not process the data for any other purpose.
13. The PI company should have an entry on the register of data controllers maintained by the Information Commissioner.
14. The PI company should hold all data in strict confidence and take all actions, and put in place appropriate security measures, necessary to protect that data from:
 - Any unauthorised or unlawful access;
 - Any accidental loss, destruction or damage; and onward use and disclosure not associated with the investigation.

The PI company should also return or ensure the secure destruction of the data when it is no longer required for the investigation, defence of the claim, potential further legal action, or accounting purpose. The PI company should notify the insurer of those measures on request. These might include steps that the PI company takes to maintain a clear chain of evidence, to store securely all original evidence and to safely dispose of evidence at the appropriate time.

15. The PI company should keep complete and accurate records of the services it carries out under its control and store all documents, information and data (in whatever form) in an intelligible format for an appropriate period (e.g. 6 years) from the termination of the contract or, on request by the insurer, return the records to the insurer in an intelligible format.
16. The PI company should allow the insurer, on request, to carry out an audit of its procedures in respect of the data gathered under this agreement. This might be conducted at the premises of the PI company, as well as at the insurer's own premises. The PI should cooperate fully, and supply promptly, relevant information, data and records of whatsoever nature as may be reasonably requested by the insurer. The PI company should grant to relevant regulators the same rights as those granted to the insurer in relation to auditing rights.
17. The insurer may wish to regularly assess the performance of the PI company, by reference to service levels and key performance indicators.
18. The PI company should submit management information to the insurer on a regular, agreed basis and in an agreed format. The management information requirements will be subject to review from time to time and any amendments will be agreed between the insurer and the PI.

19. The insurer has the right to remove from the investigation employees of the PI company or sub-contractors, if they are found to be acting inappropriately or if there are reasonable grounds for suspecting that they may be acting inappropriately. Without prejudice to the insurer's right to pursue damages against the PI company in the event of improper conduct by the PI company, the insurer might also seek recovery of any interim fee payments made.
20. If the PI company receives any complaint, notice or communication which relates directly/indirectly to the processing of personal data (or to either party's compliance with the DPA), it should immediately notify the insurer and provide full cooperation and assistance in relation to the matter.
21. The PI company should inform the insurer, as soon as reasonably practicable, following receipt of a subject access request from a claimant and should assist the insurer in satisfying that subject access request. The PI company should not disclose personal data to any data subject or to a third party only other than at the request of the insurer or as provided for in the contract.
22. On completion of the provision of services or on the renewal of the Service Agreement or after a set and agreed period, the PI should return all case material that is not active to the insurer.
23. The PI company should not transfer the data, or any part of it, to a country or territory outside the European Economic Area except with the explicit consent of the insurer.
24. The PI company should inform the insurer as soon as it becomes aware of any breach of the terms of the Act and advise the insurer of the steps that it intends to take to remedy that breach. The PI company should agree to keep the insurer informed as to the progress and completion of those steps. The parties should agree that if the insurer considers the breach to be a material breach of the Act, the insurer is entitled to terminate any agreement that it has with the PI company by notice in writing. Any outstanding instructions at the time of receipt of that notice should be regarded as cancelled.
25. There should be a time limit to the Service Agreement or contract.

OTHER CONSIDERATIONS

Reinsurance

Where there is reinsurance in place, the insurer should also consider whether the agreement should also reflect any conditions imposed by the reinsurer.

Giving evidence in court

The insurer should consider whether the PI has ever given evidence in court or at a tribunal hearing in connection with an investigated claim. It is worth remembering that evidence might not be heard for several years. So the PI should be asked what measures are taken to ensure that the evidence can be supported several years after the investigation e.g. maintaining a surveillance log. All events that occur during the surveillance operation must be recorded in longhand in the surveillance log. The evidence should be recorded contemporaneously or as soon as reasonably practicable after the event (and, in any case, while the events are still fresh in the PI's memory).

Evidence contained within signed contemporaneous surveillance logs is usually acceptable in court in circumstances where the original media has been lost or damaged or where there is no independent film evidence, for example, if a DVD/CD/memory stick is defective or where an evidential incident may have occurred which could not be documented by footage. To avoid any suggestion of malpractice, a copy of the original handwritten surveillance log should always be attached to the surveillance report as an appendix.

INSURER CODE OF PRACTICE

Individual insurers might also adopt their own code of practice, that can also often be incorporated into the agreement or contract with the PI company. The aim of the code is to ensure that the insurer is at all times represented in a professional and proper manner by the PI company, thereby minimising the risk of reputational damage to the insurer. The code might cover issues such as:

- **Ethics** - the PI company should ensure that its employees, consultants, agents and sub-contractors are of good character and free from criminal convictions, unsatisfied County Court Judgements and bankruptcies.
- This section should also cover matters such as the use of pre-surveillance enquiries and vehicle trackers.
- **Interviews and surveillance** – the PI company and its agents must only conduct interviews/surveillance in accordance with the insurer's specific instructions and the law (for example, covert surveillance must not be conducted in a manner that would involve trespass on private property).
- **Surveillance and minors** – The PI company and its agents must take all reasonable steps to avoid filming children. In locations where it is likely that children will be present (e.g. schools; leisure centres; swimming pools; public playgrounds) no video filming or still photographs should be taken under any circumstances. Where capture of images of children cannot be avoided (e.g. a child inadvertently appears on any surveillance footage) then the child's identity should be protected⁶ and the PI should advise the insurer on submission of evidence.
- **Filming at other sensitive locations** – these include hospitals, surgeries and cemeteries.
- **Representations to insurer customers/third parties** – unless acting under the explicit instruction of the insurer, the PI company and its agents must not make a direct approach to the claimant's legal representatives, negotiate a claims settlement or make an allegation of fraud to the claimant or their representative or to law enforcement, or seek to recover monies on behalf of the insurer.

Fair processing wording

The First Data Protection Principle requires data to be fairly and lawfully processed. This would ordinarily require the insurer to disclose to the customer all sources, uses and disclosures of personal data.

A PI will be instructed in order to verify an insurer's reasonable suspicions of fraud and to assist in the processing of genuine insurance claims. Where PIs are not routinely instructed, a generic reference to the processing of data, including disclosures to third parties, for the prevention, detection and investigation of crime (including fraud/attempted fraud) might be sufficient. This information should be included in the notification given to customers. The customer would have the right to be informed of the identity of the third parties should they make an enquiry of the insurer.

Where PIs are instructed routinely, the insurer should make that clear to customers in its fair processing notice. The insurer should inform the applicant / policyholder at the earliest stage that a PI might be used.

This might be in the:

1. Application form
2. Renewal form
3. Claim form e.g. a group contract where the insurer would not receive any personal data until the claims stage
4. Supporting documentation at the proposal stage

A third party claimant, for example, an employee claiming under a group policy or a third party motor accident claimant, or a solicitor representing them, should be notified in the initial letter from the insurer following receipt of the claim.

⁶ Anonymity can be preserved by using software to pixelate the child's face. Pixelation is not, however, a legal requirement.

Instruction to the PI

The insurer should decide on the most appropriate medium for issuing instructions. The insurer might choose to use a mandatory standard form template which might, for example, include the rationale for appointment of the PI and the outcome being sought.

The insurer should ensure that instructions are provided to the PI company by secure medium. Telephone instructions could, for example, be open to interpretation and lack any form of documentation. So it might be prudent for any instructions to a PI to be given in writing and sent securely (e.g. sent by recorded delivery). Alternatively, the insurer might provide instructions via a secure portal or could send an email, with the instructions contained in an attachment that is suitably protected against unauthorised access (e.g. by encryption or, at the very least, password protected).

The instructions to the PI must be explicit and transparent, with the subject matter clearly documented. The insurer should only request the necessary and appropriate amount of information needed to gather evidence to support the insurer's suspicions or to assist in the processing of a genuine claim.

The insurer should provide the PI with sufficient information as is necessary to ensure that the investigation focuses on the correct individual. The information provided to the PI should only be that which is necessary and relevant to identify the subject of their investigation and inform them of what type of investigation is required. This might include:

1. The claimant's name (and any known aliases or previous identities)
2. The claimant's sex

3. The claimant's address (and any known previous addresses) (on file) [which the PI may be asked to verify]
4. The claimant's date and place of birth
5. The claimant's occupation (if employed) and occupation history
6. Details of the claimant's known hobbies or interests
7. The description of the claimant (this might be obtained, for example, from the nurse's report or other medical report)
8. Family circumstances
9. Brief explanation of illness or disability
10. Details of claimant's vehicle
11. A description of the type of data required⁷:
 - Photographs
 - Video footage
 - PI report
 - Original signed surveillance logs
 - Any other information that is reasonably required (and justified) in order to help the insurer resolve the case. If the insurer is in any doubt as to whether further information is required or is justifiable, the insurer's data protection officer should be consulted.
12. Any other relevant information obtained through open source research.

If appropriate, the insurer and the PI might hold regular review meetings. This would help to ensure consistent standards of work, a mutual understanding of what is required from each investigation and provides a forum for providing feedback on the PI's work.

Access to data collected by a PI

The insurer should establish appropriate procedures to ensure that access to the information collected is restricted to relevant employees.

⁷ See "what information will be required from the PI to verify suspicion" [page 6].

But there might also be a number of organisations that the insurer needs to consult in connection with the claim (e.g. to gather evidence) and this might involve disclosure of some of the information obtained by the PI. These include:

1. The **reinsurer** who underwrites a proportion of the risk, and may be consulted on the appointment of a PI and as to whether the claim should continue following receipt of the PI's evidence.
2. The **employer** who, as the policyholder on a group policy, might have the right to ascertain whether a claim should continue.
3. The **legal advisers** who might be involved in advising on whether the claim should be repudiated, involved in subsequent legal action or in advising on legislative requirements.
4. The **medical advisers** who might need, for example, to give an expert opinion as to whether certain behaviour or activity might be possible if the claimant is suffering from the condition claimed.
5. The **police and insurance fraud agencies** such as the Insurance Fraud Enforcement Department (IFED) and the Insurance Fraud Bureau (IFB).

Individuals who are the subject of investigation by a PI will be entitled to claim their right to see the data obtained about them from the insurer who has instructed the PI. All disclosures made under the data subject access request right will be subject to lawful exemptions, where appropriate. The confidentiality of other individuals about whom the PI may have inadvertently collected additional information should be redacted from any disclosure.

Retention of data collected by the PI

The insurer should consider the length of time that it might need to hold the data provided by the PI. The Fifth Data Protection Principle states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. FCA guidance on systems and controls similarly provides that the general principle is that records should be retained for as long as is relevant for the purposes for which they are made.

For evidential purposes, in line with the Limitation Act 1980, it might be prudent to hold data for six years following the cancellation of the policy or repudiation of a claim. The insurer should also allow sufficient time for an appeal to be lodged or disposed of. It is important that the insurer notifies the PI when a claim has been settled/closed so that the PI can then archive the file, taking account of the need to ensure security of the information. When sufficient time has elapsed, the PI should take steps to dispose of the data securely.

AUDITING

It is important that due diligence is carried out on an ongoing basis where there is an ongoing relationship with a PI. Measures include undertaking regular audits, including file reviews at the insurer's own offices and regular (e.g. annual) site visits to the PI's offices.

Given that PIs will ordinarily be appointed in a small proportion of cases only, it is important that firms develop Quality Assurance processes in respect of internal claims handling procedures.

MANAGEMENT INFORMATION

Management Information (MI) should be prepared and reviewed, for example, to record the number of claims where a PI had been appointed and how frequently PIs appointed had actually identified any evidence of claim exaggeration or fraud. Such information could help monitor whether the insurer's fraud indicators are appropriate and ensure that claimants had been treated fairly.

The insurer should ensure that the written agreement or contract with the PI includes appropriate obligations to compile and submit MI of the type, and in the form, agreed.

FCA REGULATORY REQUIREMENTS

It is vital that insurers are aware of how the FCA Handbook applies to work outsourced to PIs when handling claims as part of their regulated activities and are able to demonstrate how they monitor and mitigate any potential risks to customers arising from outsourcing claims functions and/or activities to PIs.

When using a PI, insurers are outsourcing part of the regulated activities they perform as the work falls within the FCA Handbook Glossary definition of outsourcing, which is '.....the use of a person to provide customised services to a firm.....'

The FCA expects insurers to ensure that the work performed by PIs, which impacts upon their claims handling practices, is consistent with their regulatory obligations under SYSC, PRIN and ICOBS, and they are able to evidence this. So it is particularly important that insurers are aware of the following sections of the FCA Handbook and understand the impact they have on their practices in this area:

ICOBS 8.1.1R

- An insurer must handle claims promptly and fairly.

PRIN 2.1.1R

Principle 2 – Skill, care and diligence – A firm must conduct its business with due skill, care and diligence.

Principle 3 – Management and control – A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

Principle 6 – A firm must pay due regard to the interests of its customers and treat them fairly.

SYSC 3.2.3G

- A firm's governing body is likely to delegate many functions and tasks for the purpose of carrying out its business. When functions or tasks are delegated, either to employees or to appointed representatives or, where applicable, its tied agents, appropriate safeguards should be put in place;
- Where there is delegation, a firm should assess whether the recipient is suitable to carry out the delegated function or task, taking into account the degree of responsibility involved;
- The extent and limits of any delegation should be made clear to those concerned.
- There should be arrangements to supervise delegation and to monitor the discharge of delegates functions or tasks; and
- If cause for concern arises through supervision and monitoring or otherwise, there should be appropriate follow-up action at an appropriate level of seniority within the firm.

SYSC 3.2.4G

- The guidance relevant to delegation within the firm is also relevant to external delegation ('outsourcing'). A firm cannot contract out of its regulatory obligations. So, for example, under Principle 3 a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor.
- A firm should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls.

SYSC 13.9.1G

- As SYSC 3.2.4G explains, a firm cannot contract out of its regulatory obligations and should take reasonable care to supervise the discharge of outsourced functions. This section provides additional guidance on managing outsourcing arrangements (and will be relevant, to some extent, to other forms of third party dependency) in relation to operational risk. Outsourcing may affect a firm's exposure to operational risk. Outsourcing may affect a firm's exposure to operational risk through significant changes to and reduced control over, people, processes, and systems used in outsourced activities.

SYSC 13.9.4G

Before entering into, or significantly changing, an outsourcing arrangement, a firm should:

- Analyse how the arrangement will fit with its organisation and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
- Consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure relating to the outsourcing;
- Conduct appropriate due diligence of the service provider's financial stability and expertise;
- Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and
- Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms.

SYSC 13.9.5.G

In negotiating a contract with the service provider, a firm should have regard to:

- Reporting or notification requirements it may wish to impose on the service provider;
- Whether sufficient access will be available to its internal auditors, external auditors or actuaries (see section 341 of the Financial Services and Markets Act 2000) and to the appropriate regulator (see SUP 2.3.5R [Access to premises] and SUP 2.3.7R [Suppliers under material outsourcing arrangements]);
- Information ownership rights, confidentiality agreements and Chinese walls to protect client and other information (including arrangements at the termination of the contract);
- The adequacy of any guarantees and indemnities;
- The extent to which the service provider must comply with the firm's policies and procedures (covering, for example, information security);
- The extent to which a service provider will provide business continuity for outsourced operations, and whether exclusive access to its resources is agreed;
- The need for continued availability of software following difficulty at a third party supplier; and
- The process for making changes to the outsourcing arrangement (for example, changes in processing volumes, activities and other contractual terms) and the conditions under which the firm or service provider can choose to change or terminate the outsourcing arrangement, such as where there is:
 - A change of ownership or control (including insolvency or receivership) of the service provider or firm; or
 - Significant change in the business operations (including sub-contracting of the service provider or firm); or
 - Inadequate provision of services that may lead to the firm being unable to meet its regulatory obligations.



Association of British Insurers

For more information

Association of British Insurers
51 Gresham Street,
London EC2V 7HQ

ABI.ORG.UK