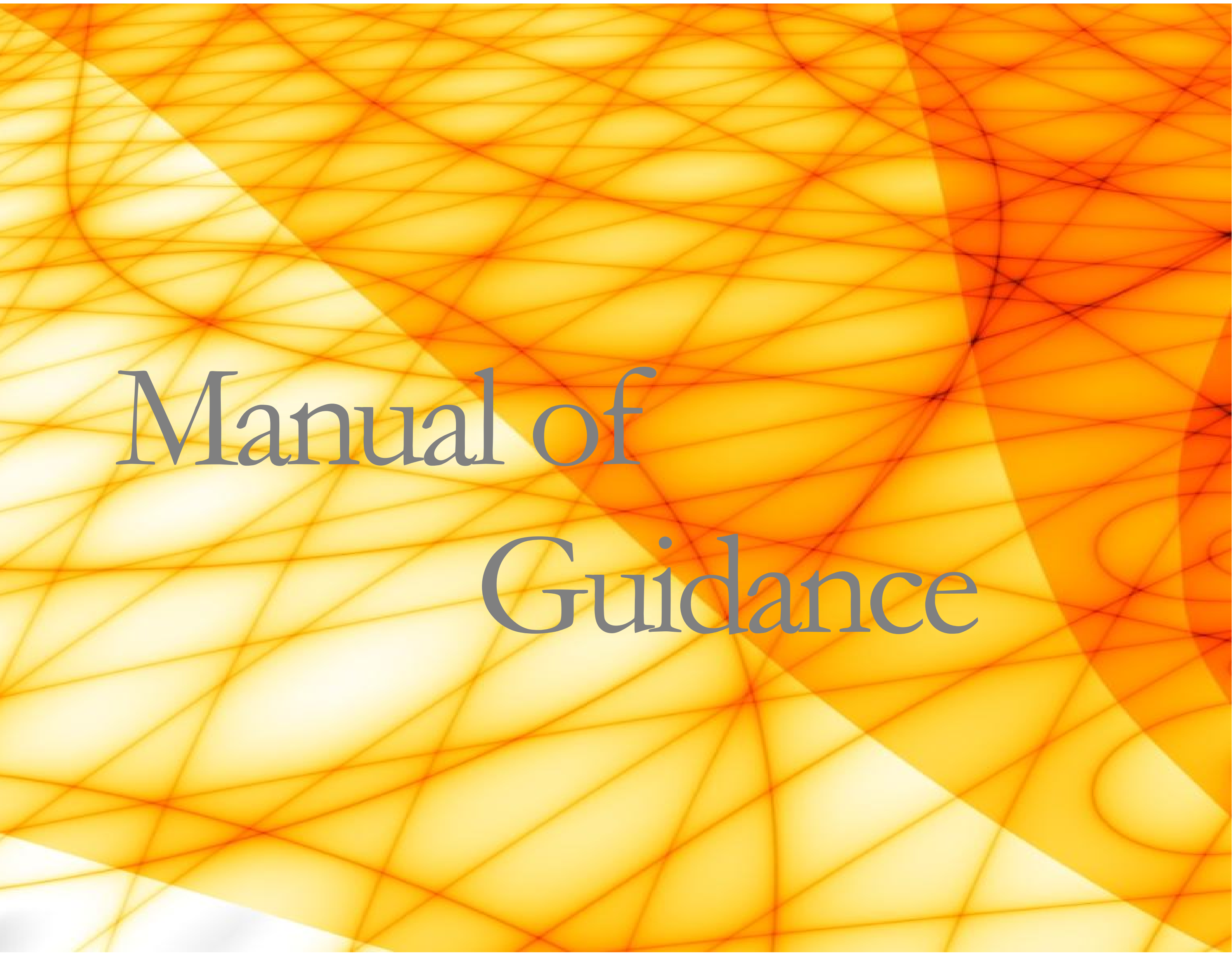
EUROPEAN HEALTHCARE

FRAUD & CORRUPTION NETWORK

Operational Sub Committee



Manual of Guidance

EUROPEAN HEALTHCARE FRAUD AND CORRUPTION NETWORK

Manual of Guidance

WITH FINANCIAL SUPPORT FROM THE AGIS PROGRAMME

AGIS 2007

EUROPEAN COMMISSION
DIRECTORATE GENERAL
FOR JUSTICE, FREEDOM AND SECURITY

© EHFCN AISBL
Avenue de Tervueren 211 Tervurenlaan
1150 Brussels
Belgium

Sole responsibility for the content of this Manual of Guidance lies with the OPSC and the European Commission is not responsible for any use that may be made of the information contained within it.

TABLE OF CONTENTS

Chapter 1 1
Introduction 1
1.1 History 1
1.2 AGIS Funding 1
1.3 Members of the OPSC 1
1.4 Aims of the OPSC 2
1.5 Holistic Approach by the EHFCN 2
Chapter 2 4
Fraud and Corruption 4
2.1 Introduction 4
2.2 Definition of Fraud and Corruption 5
2.3 Manifestation of Fraud and Corruption (An Exploration) 5
2.4 Fraud & Corruption Indicators 12
2.5 Fraud & Corruption Warnings 13
2.6 Types of Fraud and Corruption per Country 13
2.7 System Weaknesses 13
Chapter 3 14
Methods of Investigation 14
3.1 Introduction 14
3.2 The 5 Step Guidance 14
3.3 The Use of Checklists 18
3.4 Surveillance 20
3.5 Interviewing Techniques 21
3.6 Private Investigators 22
Chapter 4 24
Methods of Detection 24
4.1 Introduction 24
4.2 Accounting Systems/Internal Audits 25
4.3 Use of Technical Appliances/Resources 26
4.4 Data mining 27
4.5 Query Tools 29
4.6 Risk Measurement 31
4.7 Pre-Employment Screening 31
4.8 Whistleblowing 33
4.9 Integrity 35
4.10 Forensic Investigation Techniques 35
Chapter 5 37
Sharing Information at European Level 37
5.1 Introduction 37
5.2 Awareness Campaigns 37
5.3 Prevention 38
Chapter 6 39
Sanctions 39
Chapter 7 40
Contact Directory 40
7.1 Introduction 40
7.2 Members' Contact Details 40
7.3 Useful Contacts by Country 40
7.4 Key Contacts 40
7.5 Public Bodies per Country 40
7.6 Public Sources per Country 41
7.7 Specialist or Specialist Agencies 41
Chapter 8 42
Additional Information, Documents & Links 42
8.1 Introduction 42
8.2 Links 42
8.3 Documents 47
8.4 Healthcare Systems per Country 47
Chapter 9 48
Training 48
Chapter10 49
Biography 49

Chapter 1

Introduction

1.1 History

In September 2005 a preliminary Operational Task Force meeting was held in London. Throughout the meeting it became evident there were no mechanisms in place across Europe to exchange information and best practices. It was therefore decided that action needed to be taken and that the EHFCN was the perfect environment to begin this work. There was a wide interest to attend meetings and support the project but participation was hampered due to lack of funding.

In 2006 members of the EHFCN applied to the European Commission for AGIS funding. The application was approved and the first Operational Sub-Committee meeting was held in London on the 3rd & 4th October 2006.

1.2 AGIS Funding

AGIS was a European Commission framework programme to help police, the judiciary and professionals from the EU Member States and Candidate Countries to co-operate in criminal matters and in the fight against crime. AGIS ran from 2003 until 2006 and replaced earlier programmes.

Its purpose was to help legal practitioners, law enforcement officials and representatives of victim assistance services from the EU Member States and Candidate Countries to set up Europe-wide networks, as well as to exchange information and best practices. It also aimed at encouraging Member States to step up co-operation with applicant and third countries. AGIS supported transnational projects for a maximum duration of two years. Each year, the European Commission launched a work-programme and call for proposals.[1]

1.3 Members of the OPSC

The OPSC consists of 11 members from EHFCN member organisations.

---

[1] http://ec.europa.eu/justice_home/funding/2004_2007/agis/funding_agis_en.htm

They represent both private and public institutions from: Austria, Belgium, England and Wales, France, the Netherlands, Norway, Poland, Scotland, Slovenia, Spain and Turkey.

1.4 Aims of the OPSC

The OPSC organises regular meetings with its members to identify best practices and examine operational practices and methods in countering healthcare fraud and corruption.

The OPSC will undertake research and provide outcomes in relation to:

- Detecting and investigating healthcare fraud;
- Use of forensic investigation techniques;
- Development of high quality case management systems;
- Whistleblowing and dealing with informants;
- Proactive methods of countering healthcare fraud and corruption;
- Identifying lawful methods for sharing information;
- Creating information gateways and establishing operational contact points across Europe.

The research undertaken has led to the creation of a Manual of Guidance. This Manual is provided to members of the EHFCN. It contains examples of fraud and corruption cases for each country, methods of detection and investigation, the application of types of sanctions, case management methods, and a directory of useful contacts in each European country in relation to the investigation of healthcare fraud and corruption.

The Manual of Guidance is available in English, French, German and Spanish.

1.5 Holistic Approach

The experience of many European countries is that the potential for lost resources is too great to ignore.

Many countries have seen a vast return on their investment in countering healthcare fraud and corruption. In England alone this has amounted to over €1 billion financial benefit to the National Health Service.

There are various kinds of fraud and corruption across Europe: price fixing by suppliers, patients receiving free healthcare without being entitled to it, (i.e. health tourism) and unqualified health professionals treating patients.

Methods of detecting and preventing fraud and corruption also have many similarities, as does the important work of creating an anti-fraud culture in society.

Real, tangible benefits for healthcare systems can be gained through the implementation of effective mechanisms to reduce losses to healthcare fraud and corruption. Through promotion of opportunities, joint working, sharing of good practices and development of common working standards, European healthcare systems can be improved by reducing losses to fraud and corruption, which in turn will produce savings and social benefits through more cost effective delivery of patient care.

In particular, the following initiatives will significantly reduce healthcare fraud and corruption:

- The creation of a real anti-fraud and anti-corruption culture within healthcare systems and ultimately among all EU citizens;
- To use all possible presentational and publicity opportunities to act as a deterrent to those who intend to engage in healthcare fraud or corruption;
- The use of effective prevention systems so that when fraudulent or corrupt activities are attempted, they will fail;
- The use of detection systems that will promptly identify occurrences of healthcare fraud and corruption;
- The professional investigation of all cases of detected or alleged healthcare fraud and corruption;
- The imposition, where healthcare fraud and corruption is proven, of appropriate sanctions, namely civil, criminal and or disciplinary processes. Multiple sanctions should be used where possible;
- The seeking of redress in respect of resources lost to fraud and corruption and the return of recovered resources to the area of the patient care or services for which they were intended;
- The development of a European common standard of risk measurement (baseline figures) with annual statistically valid follow up exercises to measure progress in reducing losses to fraud and corruption throughout the EU.

It is essential that countries in Europe work together to deal with potential increases in cross-border fraud and corruption through exchanging information on current problems and solutions.

Chapter 2

Fraud and Corruption

2.1 Introduction

Fraud poses a serious risk to all financial sectors. In the insurance sector, both insurers and policyholders bear the costs. Losses caused by fraudulent activities affect insurers' profits and potentially their financial soundness. Fraud may also reduce consumer and shareholder confidence.

In cases where healthcare is provided by means of a public system, fraud may affect not only patients but also the global resources assigned to healthcare and eventually all citizens.

Resources made available for the provision of healthcare services should not be lost to fraud and corruption. Members have agreed to the EHFCN Declaration (link) and are committed to work together to reduce losses from fraud and corruption from public as well as private healthcare systems.

Real, tangible benefits for European healthcare systems can be gained through the implementation of effective mechanisms to reduce losses from healthcare fraud and corruption.

By promoting opportunities, cooperation, sharing of good practices and developing common working standards, those who agreed to the Declaration aim to improve European healthcare systems by reducing losses to fraud and corruption, which in turn will produce savings and social benefits through more cost effective delivery of patient care.

EXAMPLE CASE

A dialysis patient asked for authorisation to be treated in Pakistan as she visited there twice a year. She was entitled to claim the medical costs as well as transportation costs to and from the medical centre within Pakistan. Written authorisation was sent to the patient prior to each of her visits.

After returning to the Netherlands, the insured claimed for the treatment and the rental of a car. Soon after having submitted the claim the insured called to enquire when these costs would be reimbursed. Because the insurer was unable to tell her how long it would take, they decided to pay the costs in advance.

Suspicion of Fraud

The counter fraud department noticed the insured rented exactly the same car that she had rented in the previous year. Despite the fact that it was rented from a different car hire company it was the same make, the same number plate, same colour, etc. The receipt was written in English, but strangely enough there was a Dutch word included in the English text. The case was handed over to the counter fraud department.

2.2 Definition of Fraud and Corruption

Throughout Europe many definitions exist of fraud and corruption. A study of the literature reveals that the definition of fraud includes two important aspects, the intentional action and the resulting merits.

In 2005 the Swiss Institute of Comparative Law[2] defined fraud as follows:
Civil fraud is the use of presentation of false, incorrect or incomplete statements and/or documents, or the non-disclosure of information in violation of a legally enforceable obligation to disclose, having as its effect the misappropriation or wrongful retention of funds or property or others, or their misuse for purpose other than those specified.

See Annex A: EHFCN Overview per Country.

2.3 Manifestation of Fraud and Corruption (An Exploration)

We know that fraud and corruption occurs within the member organisations of the EHFCN. There are many types of fraud within the EHFCN and other countries of the EU. To illustrate these types of fraud, here are some examples:

Fraud Committed by Patients:

- Patients who claim exemption from prescription charges when they are not in fact exempt;

- Patients who falsely state that they have lost their prescriptions and obtained duplicates;

---

[2] http://www.isdc.ch/en/ - Swiss Institute of Comparative Law, Dorigny, CH-1015 Lausanne, Switzerland +41 (0)21 692 49 11, F +41 (0)21 692 49 49.

- Patients who have falsely registered with a number of doctors and obtain prescriptions from each;
- Patients who try to obtain refunds of medical costs they never incurred;
- Patients who obtain medication or narcotics by means of irregular procedures for their own consumption or drug trafficking;
- Patients who present false reports to obtain a disability allowance;
- Patients who trade prescriptions;
- Identity fraud: non-registered patients using the identity or E-card of registered patients in order to get benefits paid by the health insurer;
- Collusion between patients and providers in order to invoice non provided healthcare.

Fraud Committed by Pharmacists:

- Pharmacists conspiring with GPs and specialists who submit bogus prescriptions for reimbursement;
- Pharmacists who are substituting expensive drugs with a cheaper alternative, but claiming for the expensive one;
- Pharmacists adding items to prescriptions;
- Pharmacists selling medicines without prescription to wholesalers for illegal export;
- Pharmacists invoicing non-delivered drugs.

Fraud Committed by Dentists:

- Dentists submitting claims for patients who do not exist;
- Dentists who charge patients privately and also submit claims to the health insurer;
- Dentists up coding their bills with non-provided care.

Fraud Committed by Opticians:

- Opticians claiming for eye tests and the supply of glasses to patients who have died;

- Opticians claiming that 2 pairs of glasses were issued to a patient (distant and near) but only one pair was actually issued.

Fraud Committed by GPs:

- The dispensing of bogus prescriptions;
- GP who refuses to see his patients at his surgery so he can charge for night visit fees at their own homes;
- Up coding or up billing;
- GPs prescribing unnecessary or overly expensive medicine in return for benefits from pharmaceutical companies;
- GPs claiming for non-provided healthcare or for patients they never saw;
- GPs prescribing (free-of-charge) medicine for patients who are not entitled to it.

Fraud Committed by Orthopedists:

- The supply of products or services of less quality and lower price than those prescribed and eventually paid for by the national health system.

Fraud Involving the Procurement of Drugs or Services:

- A manager colluding with suppliers to produce a large amount of invoices for goods which were not delivered.
- Physiotherapists claiming for services not performed or claiming more services than actually supplied.

Fraud Committed by Carriers:

- Health transport suppliers who invoice for longer routes than those actually driven.

Fraud Committed by Staff:

- Staff claiming for duty payments and hours worked with no evidence that the work has been done;
- Staff forging signatures of authorised cheque signatories in order to submit a number of false invoices to support reimbursement requests;
- Professionals who are working without having the proper qualifications.

There are many types of corruption within the EHFCN and other countries of the EU. To illustrate these types of corruption, here are some examples from Poland:

Corruption in the Area of Health Service Provision

Informal Payments for (Patients – Service Providers):

- Health services delivered to patients who are entitled to services free of charge;

- Access to services in the public health service (e.g. faster admission to hospital; earlier procedures, avoiding waiting lists, receiving referrals, for treatment, tests, consultations, receiving hard-to-get medical products and medicines as defined by the patient, including those not connected to the patient's condition, more thorough, attentive care, etc.);

- Issuing reports of state of health (illness) incompatible with the actual state, providing a basis of the extension of unwarranted benefits (medical leave from work, receiving health benefit, exemption from military service, early release from, or the inability to serve, a prison sentence, gaining the right to residence in Poland by foreigners, extending sickness benefits or medical leave, etc.).

Others (Patients – Service Providers):

- Incitement by public health service employees of patients to a consultation in a private surgery, in order to continue further treatment in a public healthcare institution or inducing patients to be treated in the private sector;

- Ordering tests and procedures that are not medically justifiable, for financial gain;

- Non-provision of essential medical services, or lowering the level of quality to an unacceptable standard in order to gain benefits;

- Forcing a patient staying in hospital to buy medical products and medicines that should be provided by the hospital;

- A Fund operating on hospital premises, in breach of the law, which accepts payments from patients being treated within the parameters of compulsory health insurance.

Informal Payments for (Patients – Public Insurance Company):

- The payer taking a decision, beyond the accepted parameters, regarding the refund of the costs of buying orthopaedic equipment, auxiliary resources and technical medical drugs;

- Hastening a referral to a sanatorium or referral to a designated place by the payer;

- A decision by the Public Insurance Company to the benefit of an individual in matters relating to health insurance.

Informal Payments for (Service Providers –Public Insurance Company):

- Awarding a higher-than-justified Public Insurance Company contract to a service provider, receiving a specific price from the Public Insurance Company for providing a service;

- Acceptance of reimbursement fraud by the payer, for financial gain.

Others (Service Providers – Proper Authorities of Public Administration):

- Illegal payments in return for issuing authorisations and decisions by proper authorities (inspection, scrutiny and assessment services etc.)

Others (Service Providers – Public Health Service Personnel):

- Using public health service resources, including material (e.g. medical apparatus) to provide services to private patients;

- Theft by employees of public health care institutions of medical products, medicines and other items for personal use or to provide private health care.

Others (Service Providers, Public Health Service Personnel - Commercial Entities):

- Processing and illegally making patient's personal details available by a service provider.
- Corruption in the area of Health Service Supply

Illegal and Hidden Payments (Health Service Suppliers – Medical Staff):

- Lobbying in the area of health service supply (including medical products and medicines);

- Prescribing medical products and medicines of a particular brand to patients;

- Conducting surveys in the public health service during working hours on behalf of companies involved in the production or sale of medicines.

Others (Health Service Suppliers – Medical Staff):

- Advertising medical products and medicines in breach of legal regulations;

- Publication of academic papers, commissioned by pharmaceutical companies, the conclusions of which are likewise commissioned, or the authorisation by doctors of articles prepared by pharmaceutical companies;

- Benefiting from trips and training sponsored by pharmaceutical companies, or other companies operating in the health care market, accepting gifts in return for promoting or prescribing medical products or medicines of that company;

- Pharmaceutical companies supplying free-of-charge medical products (non-reimbursed, expensive, often life-saving remedies), and then withdrawing from sponsorship during the course of treatment, leaving the physician and patient dependant on the 'sponsor'.

- Pharmaceutical companies commissioning research which, under the pretext of assessing side effects, are really only designed to introduce and maintain a given drug on the market;

- Complete fitting out of doctor's surgeries by suppliers who, frequently by presenting their products or by informally committing the medical community, expect future financial benefits.

Others (Health Service Suppliers – Management Staff and Other Health Care Employees):

- Signing more expensive, error-ridden supply contracts by health care institutions in return for financial benefits from the suppliers;

- A health service institution tolerating a poor quality of supplied equipment or service in return for financial benefits from the suppliers;

- Accepting medical products in the form of a donation for a health care institution in return for the purchase of chemical reagents from the company at an inflated price;

- A health service institution issuing public procurement orders in breach of legal regulations for financial gain.

Others (Health Service Suppliers – Patients):

- False or misleading advertisements or leaflets with descriptions of the effectiveness of medical products, medicines or anti-biotic products (including prescription medicines);

- Rewarding patients by pharmacies by way of material gifts or financial benefits, in return for purchases of medicines reimbursed from public sources.

Others (Health Service Suppliers):

- Agreements between medical equipment suppliers and pharmaceutical companies that result in the necessity to use the products of a specific pharmaceutical company when using medical equipment;

- Agreements between medical product suppliers to maintain or gain high prices of medical products or medicines.

Corruption in the Area of Regulation

Illegal Payments for (Health Service Suppliers – Proper Authorities of Public Administration):

- Advantageous decisions by proper authorities enabling the sale and registration of medical products, medicines or anti-biotic products;
- Advantageous decisions by proper authorities regarding the inclusion of medicines on the list of reimbursed medicines.

Others (Health Service Suppliers – Public Insurance Company):

- Creating a demand for products offered by a health service supply company, and exerting influence (including via mass media) on persons creating procedure manuals that are contracted by the Public Insurance Company (Public Insurance Company employees, consultants);

- Health service supply company influence on medicinal programmes implemented by the Public Insurance Company and performing 'non-standard' procedures (non-standard pharmacotherapy)

Others (Health Service Suppliers – Proper Authorities of Public Administration):

- Presentation of false clinical test results for medical products, medicines etc. by health care supply companies in order to gain proper licences;

- Using forged licences to trade in medical products or anti-biotic products, and falsifying certificates, declarations of compliance or other documents.

Others (Health Service Suppliers – Proper Authorities of Public Administration):

- Failing to report undesirable effects of a medical product, by negligence or intentional action for financial gain.

Corruption in the Sphere of Management

Informal Payments (Health Care Institution Management – Health Care Institution Employees) for:

- Employment and the possibility of continued employment in a health care institution;

- Raising professional qualifications (e.g. gaining a specialisation).

Others (Health Care Institution Management – Health Care Institution Employees):

- Lack of effective and efficient control over the flow of financial resources in the unit, lack of financial control procedures, faulty internal audit.

- Others (Health Care Institution Management – Commercial Entities):
- Lack of criteria for access to public financial resources, inequality of access to information.

2.4 Fraud & Corruption Indicators

Fraud and corruption indicators are used to highlight where fraud and corruption may be present, allowing investigators to be proactive in identifying where there may be vulnerabilities in current systems.

Fraud and corruption indicators also help investigators to recognize common characteristics which may assist with detecting incidents of fraud and corruption. While one indicator may mean fraud or corruption is present, it is usually the case that two or three have alerted an investigator or a member of the public that a fraud may be occurring or that corruption exists.

The EHFCN website[3] gives an overview of the fraud and corruption indicators per country and an example of a real case.

EXAMPLE

Discovery and reporting of possible fraud:

Complainants made several claims about some pharmacies and doctors working in State Hospitals and Private Hospitals in the District Attorney of Doðubeyazýt, Turkey.

The District Attorney of Doðubeyazýt opened an investigation about these claims. During the investigation, calls made by suspects were monitored, documents were collected, searches were carried out in the relevant pharmacies, private hospitals etc., statements of complainants, witnesses and suspects were taken. During the investigation some important fraud indicators were collected.

THE FRAUD INDICATORS WERE

- **Statements of the complainants;**
- **Calls made by suspects;**
- **Health certificates and medicine clippings found in searches carried out;**
- **False documents submitted by Green Card owners;**
- **No information in patient files and hospital records about treatments and analysis carried out being in the invoices.**

---

[3] http://www.ehfcn.org

2.5 Fraud & Corruption Warnings

The secure part of the EHFCN website lists fraud and corruption warnings[4] from the members of the Network.

This area of the site allows Members to send and receive fraud and corruption warnings. Timely intervention is essential, so these warnings will allow EHFCN members to be alerted to possible cases of fraud and corruption that may be taking place in their organisations.

2.6 Types of Fraud and Corruption per Country

Fraud and corruption can permeate all areas and levels of society including healthcare provision. It does not matter whether the healthcare is administered by a public or private body. It is important for all healthcare bodies within all countries to safeguard their service delivery and administration systems against mismanagement and subsequent loss of funds to fraud and corruption.

It is also important to be aware that fraud and corruption can be carried out by either an individual or group, and can be either opportunistic or planned.

Fraud and corruption activities can take place in any area of healthcare delivery. Though many types of fraud and corruption are dependent upon the country they take place in, there are specific types of fraud and corruption in the different countries.

An overview of these types of fraud and corruption can be found in **Annex B** for Belgium, Norway, France, the Netherlands, Poland, Spain, Turkey and the United Kingdom.

2.7 System Weaknesses

The opportunity to commit fraud and corruption may depend on the way healthcare systems are organised in the different member states. The rate of success for perpetrators depends on the strength of each system.

Public as well as private healthcare systems have their own weaknesses.
An overview of the system-weaknesses in different countries can be found in **Annex C,** for Belgium, France, the Netherlands, Norway, Poland, Spain, Turkey and the United Kingdom.

---

[4] http://www.ehfcn.org/extranet/index.aspx?id=1163166

Chapter 3

Methods of Investigation

3.1 Introduction

What can you do if you suspect fraud? What is the best method of investigation? Can you do it by yourself or is it better to refer to another agency?

The aim of this chapter is to answer these questions and to clarify which methods of investigation are available.

3.2 The 5 Step Guide

Zorgverzekeraars Nederland (ZN) has developed a step by step guide on how to handle fraud cases. This has not been an easy task. Many aspects such as codes of conduct, privacy laws and the provision of information have made this difficult. As many forms of fraud exist there are various considerations to make when you embark upon an investigation.

Nevertheless ZN has drafted a step by step guide which may be of use in any investigation into healthcare fraud. Each type of fraud has its own fraud-indicators (see 2.4).

Please note that this step by step guide is exactly that – a guide. It is a living document that is constantly under review and therefore subject to change. Counter fraud specialists are invited to contribute to improve this guide.

Step 1:

Reporting a Possible Fraud Case

Departments or employees responsible for reimbursement, registration etc. need to have fraud-indicators at their disposal. These indicators may vary, depending upon the type of fraud. Being aware of these fraud indicators is essential for this first step.

After the suspicion has arisen, there will need to be an approach to the manager of the department, and also, depending upon the type of suspicion, an approach to a counter fraud specialist.

There are many ways to report a possible case of fraud. The use of a standard form could be considered. On this standard form all the known information should be filled in (for example information about the suspect, the type of fraud, circumstances etc).

We recommend handing over a possible fraud case to specialist fraud investigators as early as possible. This ensures correct handling from the start of any investigation.

It is not only necessary to have the fraud-indicators available, it is also important that employees know what the procedures are. Why is it necessary to report possible fraud cases? To whom must they pass the information? What is required on the standard form? How is the investigation to be progressed? A written fraud and whistleblowing (see 4.8) procedure should be to encourage employees to report their suspicions.

When the counter fraud specialist (or department) receives the report, they will send an acknowledgement in which they state that an investigation will be conducted and that the complainant or referral source will receive the results of this investigation.

Step 2:

First Inquiry by a Counter Fraud Specialist

The aim of the first enquiry is to determine the facts.

First the counter fraud specialist has to enter the possible fraud in a (fraud) register. All subsequent steps should be added into this file to get a complete picture of the possible fraud. It is not necessary for the head of the department to conduct these actions himself. However, it may be necessary for him to take charge of the investigation.

The questions you will need to ask will be different depending on the type of fraud. However there are steps which need to be taken in every case:

a. Who may be involved in the possible fraud?

- Do we know the suspect?
- Is the suspect known through previous fraud investigations?
- Does the suspect have an "insurance-history"? If so, how does this history look?
- If the fraud is concerning an existing health insurance contract, what is the duration of the contract, what are the terms, and what costs did the suspect claim?
- What is the line of conduct related to the payment of the premium?
- Are there any annotations in the file?
- Is there a possibility to obtain relevant information from any other sources?
- Be sure to act according to a "need to know"-principle

b. What is the actual suspicion?

- Which fraud-indicators led to the suspicion of fraud?
- Is it possible to determine fraud or is a supplementary investigation necessary?
- Specific questions related to the type of fraud?

Step 3:

Intermediate Decision: the Suspicion Drops or Rests

In the course of the investigation there will be a point where the suspicion is dropped (where no evidence of fraud can be found) or where suspicion becomes stronger or fraud is actually determined[5]. Exactly when this point is reached will vary, depending on the outcome of the investigation.

---

[5] See definition of fraud from the Swiss Institute of Comparative Law. http://www.isdc.ch/en/

a. Fraud is no longer the case

There is a need to find out what caused the misunderstanding or led to the suspicion of fraud. There may also be a need to clarify or amend existing procedures. Sometimes verification is necessary as a final step before closing the file. This might be the case for the suspected person or third parties.

It is important to inform the person who reported the suspicion of the outcome of the investigation. (See 4.8)

b. Suspicion of fraud becomes stronger or fraud is determined

At this point the investigation changes from "has fraud been committed?" to "how was fraud committed?" and one needs to consider how to collect objective evidence. How this is done will vary depending on the type of fraud.

One may also want to consider whether the investigation should be extended i.e. see if the possible fraudster had similar cases, but also if there are other persons who acted in a similar way (other members of the same group/type of healthcare-providers, people living in the same street or even family-members.

Step 4:

Take a Statement or Interview the Suspect

The supplementary investigation will probably lead to a complete picture of the actual fraud. Because it is necessary to hear both sides, you will need to take a statement from the suspect. It may be useful to ask the insured in advance for written permission to do this.

What do you do in this situation? When is it necessary to get a written statement and when do you invite the suspect to an interview? There is more than one way of approaching this. In more serious cases (i.e. where large amounts of money are involved or where there has been an abuse of power) it is preferable to conduct an interview. In less serious cases it might be enough to have a written statement.

The first interview should be neutral in character and must have the aim of collecting information. There should not be any doubts or misunderstanding about the facts during the interview. A second interview may be conducted later to confront the suspect with conflicting statements and/or suspicions. (See 3.5)

Two recommendations:

- Never conduct these interviews alone; always bring a colleague with you.
- Write down or record the statement of the suspect and ask the suspect to sign his statement.

Step 5:

Fraud is Confirmed, now Seek Sanctions.

Once fraud has been determined, a final step is necessary: take appropriate sanctions.

For example in the Netherlands the following steps are taken or are at least considered:

- Report the fraud to the appropriate authority;
- Record the fraud case in the fraud-registration of your company (and make reference to the involved parties);
- File the fraud case in the internal fraud-registration of your company (and make reference to the involved parties);
- File the fraud case in the external fraud-registration.

For further information in respect of sanctions please see **Chapter 6 – Sanctions**.

3.3 The Use of Checklists

When fraud is suspected	**Manual of Guidance**
Has the case been reported to the counter fraud specialist or inspector?	**Chapter 3.2**
Have you verified all the facts?	**Chapter 3.2**
Do you have all the original documents?	**Chapter 3.2**
What are the historical facts or records about the patient or institution?	**Chapter 3.2**
Verify with doctors, pharmacist registration, etc	**Chapter 3.2**
Search for literature concerning different types of fraud	**Chapter 8.2**

Is there a previous example of this type of fraud (EHFCN case studies)	Chapter 2.4
Analyse all the documents, clinical records and invoices	Chapter 4.10
Is there an interview plan available for patients and professionals?	Chapter 3.5
Do you know all the rules, procedures and legislations?	Chapter 6
Who is responsible for the investigation?	Chapter 3.2
Do you need help or who can help with your investigation?	Chapter 3.6
Have you made an economic assessment?	Chapter 3.2
What kind of forensic investigation methods can you use?	Chapter 4
What kind of sanctions do you propose?	Chapter 6
Is the sanction proportionate?	Chapter 6
Can you prevent this type of fraud from occurring in the future?	Chapter 3.2
Was the fraud cased by a system weakness?	Chapter 2.7
Communicate the fraud in your organisation	Chapter 5.3
Have you added this case to the EHFCN website? (case studies)	Chapter 2.4

3.4 Surveillance

Surveillance is the monitoring of behaviour.

Systems surveillance is the process of monitoring the behaviour of people, objects or processes within systems for conformity to expected or desired norms in trusted systems for security or social control.

EXAMPLE – THE BELGIAN SYSTEM

In Belgium, surveillance activities have been managed since 1963. Its approach is based on a combination of three concepts and ruled by the SMEC Service of Medical Evaluation and Monitoring (or control) - which:

- **Informs the health care providers about the right compliance with the regulations of the health care and benefit insurance in order to prevent, inter alia, the administrative mistakes or infringements.**
- **Evaluates the medical behaviours of a targeted group of providers in analysing and assessing their use and consumption of medical acts.**
- **Checks if the health care acts performed by health care providers and the prescriptions of medication are correctly carried out and compliant with the rules or regulation of the Health care compulsory insurance and benefits. This checking includes also the unfit for work and the combination of unfit for work benefit with labour activities.**

See also **Annex D**.

3.5 Interviewing Techniques

In practice this is probably the most valuable research method. Effective interviewing is an important skill.

There are various interviewing techniques. The Counter Fraud & Security Management Service (CFSMS)[6] uses an investigative interviewing model called PEACE.

It divides the interview into 5 steps.

Plan and Prepare	**Before the interview**
Engage and Explain	**Once the interview has commended** **This is where you introduce the interview**
Account	**Getting the subjects to recall the event and then go over it with them**
Challenge	**Challenge them with your evidence and do a final summary**
ClosurE	**Ask if they would like to add or clarify anything**

For further details, please consult **Annex E.**

---

[6] http://www.cfsms.nhs.uk/

3.6 Private Investigators

Introduction

A private investigator (private detective, PI or private eye) is a person who undertakes investigations, usually for a private citizen or some other entity not involved with a government or police organisation. They often work for legal agencies and many work for insurance companies to investigate suspicious claims.

Many jurisdictions require private investigators to be licensed. They are expected to keep detailed notes and to be prepared to testify in court regarding any of their observations on behalf of their clients. They will also take great care to remain within the law otherwise they risk losing their licenses as well as facing criminal charges. Many agencies specialise in particular fields of expertise. For example, some private investigators deal only in tracing. Increasingly, modern private investigators prefer to be known as “professional investigators” rather than “private investigators” or “private detectives”. This is a response to the seedy image that is sometimes attributed to the profession and an effort to establish and demonstrate the industry to be a proper and respectable profession.

History

In 1833 Eugene Francois Vidocq founded the first known private detective agency, le Bureau des renseignements (office of intelligence). Official law enforcement tried many times to shut it down. In 1842 the police arrested him under suspicion of unlawful imprisonment and taking money under false pretenses after he had solved an embezzling case. He was sentenced for five years with a 3.000 franc fine but the Court of Appeal released him.

After Vidocq, the private investigator industry was born. In the US, the Pinkerton National Detective Agency was a security guard and detective agency, established in 1850 by Allan Pinkerton. It was not until the 1920´s that the private investigator became a person accessible to the average American. Since then the private detective industry has grown with the changing needs of the public. Social issues like infidelity have impacted the industry and created new types of work, as has the need for insurance and with it, insurance fraud.

Global Focus

In some countries throughout the world private investigations are illegal. Other countries restrict the duties of private investigators. For example in South Korea, surveillance is only allowed in insurance fraud investigations. Some countries in the world require licensing of private detectives, but most do not.

Private detectives and investigators often work irregular hours because of the need to conduct surveillance and contact people who are not available during normal working hours. Many detectives and investigators spend time away from their offices conducting interviews or doing surveillance, but some work in their office most of the day conducting computer searches and making phone calls.

Some of the work involves confrontation, so the job can be stressful and dangerous, but the purpose of the work is gathering information and not law enforcement or criminal apprehension.

Training and Qualifications

There are no formal education requirements for most private detective and investigator jobs, although many private detectives have college degrees or have taken legal or criminal investigation courses. Private detectives and investigators typically have previous experience in other occupations. Some work initially for insurance companies. Many investigators enter the field after serving in law enforcement, the military, government, auditing and investigative positions.

For private detective and investigative jobs most employers look for individuals with ingenuity, persistence and assertiveness. A private investigator must not be afraid of confrontation and should communicate well. Good interviewing and interrogation skills also are important.

Pre-employment screening is necessary before employing a private investigator and should include a background check for a criminal history. Some investigators receive certification from a professional organisation to demonstrate competency in a field.

Chapter 4

Methods of Detection

4.1 Introduction

Detection

Fraud and corruption will always be present in our society; there will always be those who wish to perpetrate fraud and corruption. We must therefore have the ability to detect new fraud and corruption effectively, while still looking out for existing fraud and corruption in our healthcare systems.

The aim of this chapter is to demonstrate what methods of detection are available and how they fit in the day to day lives of investigators.

There are considerable technological risks to organisations when securing/contracting and settling the costs of health benefits:

- attempts against computer systems;
- hacking – non authorised computer system accessing;
- computer facilitated access data forgery e.g. by using records of deceased, forged contracts, etc
- misappropriation of information e.g. database with personal and sensitive data;
- modification of the database by using a logical bomb, Trojan Horse, virus or computer bug ;
- forgery of magnetic and processor cards;
- data forgery, data altering, data tracking;
- copyright infringement;

Fighting computer crime has been set out in the Council of Europe Committee of Ministers Recommendations Nr R (89)9[7] and Nr R (95)13[8].

The Recommendations among others determine:

- the rules that should be incorporated into criminal law for the efficient fighting of this kind of crime.

- the rules the Penal Proceedings Code should contain and what kind of prosecution agency structures are to be found to facilitate fighting computer crime

Due to the issues mentioned above, methods to fight computer crime have to be simple and quick. There is also the need for founding a database guarding system and perhaps also a new software guarding system that would be more efficient for the specification of the problem.

The most effective action to prevent technological crimes is "fighting fire with fire" – using technology. Nowadays systems are building in additional protection.

Independent suppliers provide many different types of protection: from biometrical identification to firewalls in order to protect systems and the Internet from cyber criminals.

Monitoring and auditing modules allow professionals to collect useful information and monitor suspicious actions. Many of them have detecting capacities to alert the administrator as soon as an attempt is made to break into the system.

4.2 Accounting System/Internal Audits

From a general point of view, prevention should be achieved by introducing quality management systems in healthcare, setting up written procedures and making a periodical monitoring and control system mandatory.
Patients should be educated concerning their rights and duties. Professionals should be informed about relevant legislation, ethics principles and quality management systems in healthcare. Where contractors and suppliers are concerned, organisations should ensure that they enter into accurate and quality assured contracts.

Whenever fraud investigations identify any weaknesses in the design of the management system any relevant procedures should be reviewed.

For further information please see Annex F.

---

[7] http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/1_standard_settings/Rec_1989_9.pdf

[8] http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

4.3 Use of Technical Appliances/Resources

Docubox/Document Analysis

The Docubox uses different types of light in combination with various filters and light perspectives to show how documents have been manipulated such as:

- Reveal different types of ink/pens (deletions, additions).
- Make underlying text visible
- Identify traces of earlier text and/or damage or scratches that show text has been deleted
- Demonstrate the presence or absence of fluorescent marks of authenticity (is it an original or a copy?)
- Demonstrate the presence or absence of other marks of authenticity - watermarks and security threads in the paper structure
- Show on the underlying document what was written on the document above it (print-through text; for example in a notebook or chequebook)
- Place ostensibly identical documents on top of each other to show (minimal) differences in shape, dimensions, etc.

The reports of investigations conducted using the Docubox are accepted as evidence by the courts.

Handwriting Analysis

In the age of digital traffic, e-mails and Internet, you could be forgiven for thinking that handwriting analysis is no longer important. In fact, the contrary is true.

Handwriting analysis is an investigative method that analyses the similarities between different handwritten or manually produced letters and characters.
It should not be confused with graphology, which focuses on analysing handwriting to deduce a person's character.

Handwriting analysis is performed by a specialist who compares the 'contested materials' with authentic materials. The focus is therefore on showing whether there are similarities/deviations in the way letters and characters are written. The more similarities, the greater the likelihood that the handwriting was produced by the supposed creator. These comparisons also take account of the nature, quality and quantity of the materials, as well as the direction of the handwriting. All of this means that this type of investigation is socially and legally valid. In practice, therefore, the results of a handwriting report are generally accepted as evidence in court.

Fingerprint Analysis

Fingerprint analysis is often conducted during scene investigations, usually in insurance investigations into burglary, arson and sabotage. Fingerprint analysis is the technique of detecting fingerprints and comparing and identifying them and is part of the forensic investigation of clues, such as traces of DNA, tyres, burglary, blood and sperm. Fingerprints are used not just as a means of investigation but also as proof of identity.

Fingerprints are made up of papillary lines, which are raised lines present on the skin in various shapes. Fingerprints have 100 % evidential value. No two people have the same fingerprints, not even twins. Fingerprints are therefore unique and unchanging. For purposes of identification, the accepted practice is that there must be several points of similarity and no differences.

The detected fingerprints are preserved at the scene and are interpreted later. In addition, the fingerprints of the suspects should also be taken in a forensically accountable way. Any clues detected can then be used to reconstruct the offence. In most cases, the combination of technical and tactical searches and a face-to-face interview with the suspected perpetrator will always uncover the truth.

4.4 Data mining

Introduction

Generally, data mining (sometimes called data or knowledge discovery) is the process of analysing data from different perspectives and summarising it into useful information – information that can be used to increase revenues, cut costs or to counter fraud. Data mining software is one of a number of analytical tools for analysing data. It allows users to analyse data from many different dimensions or angles, categorise it, and summarise the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.

Although data mining is a relatively new term, the technology is not. Companies have used powerful computers to sift through volumes of data for a long time now. However, continuous innovations in computer processing power, disk storage, and statistical software are dramatically increasing the accuracy of analysis while driving down the cost.

Data, Information and Knowledge

Data is any fact, number or text that can be processed by a computer. Today, organisations are accumulating vast and growing amounts of data in different formats and different databases:

- operational or transactional data such as premiums, healthcare costs, inventories, etc.;

- non-operational data such as forecast data and macro economic data;

- meta date i.e. data about the data itself, such as logical database design or data dictionary definitions;

The patterns, associations or relationships among all this data can provide information which can be converted into knowledge about historical patterns and future trends.

Data Warehouses

Dramatic advances in data capture, processing power, data transmission and storage capabilities are enabling organisations to integrate their various databases into data warehouses. Data warehousing is defined as a process of centralised data management and retrieval. Data warehousing, like data mining, is a relatively new term although the concept itself has been around for years. Data warehousing represents an ideal vision of maintaining a central repository of all organisational data. Centralisation of data is needed to maximise user access and analysis. Dramatic technological advances are making this vision a reality for many companies. And, equally dramatic advances in data analysis software are allowing users to access this data freely. The data analysis software is what supports data mining.

How does Data mining work?

While large-scale information technology has been evolving separate transaction and analytical systems, data mining provides the link between these two.

Data mining software analyses relationships and patterns in stored transaction data based on open-ended user queries. Several types of analytical software are available: statistical, machine learning and neural networks. Generally, any of four types of relationships are sought:

- classes: stored data is used to locate data in predetermined groups;

- clusters: data items are grouped according to logical relationships;

- associations: data can be mined to identify associations;

- sequential patterns: data is mined to anticipate behaviour patterns and trends.

Data mining consists of five major elements:

- extract, transform and load transaction data on to the data warehouse system;
- store and manage the data in a multidimensional database system;
- provide data access to business analysts and information technology professionals;
- analyse the data by application software;
- present the data in a useful format, such as a graph or table.

What Technical Infrastructure is required?

Today, data mining applications are available on all size systems for mainframe, client/server and PC-platforms.

System prices range from several thousands euros for the smallest applications up to €1 million a terabyte for the largest. Enterprise wide applications generally range in size from 10 gigabytes to over 11 terabytes.

There are two critical technological drivers:

- size of the database: the more data being processed and maintained, the more powerful the system required;
- query complexity: the more complex the queries and the greater the number of queries being processed, the more powerful the system required.

Please also see **Annex G**: A French Example of Data Mining.

4.5 Query Tools

What is a Query Tool?

A software tool that allows end users to access information stored in a database. Many modern query tools have extensive analytical and reporting capabilities. Many modern business intelligence tools have combined Query, Reporting and OLAP capabilities.

Business Intelligence

Business intelligence (BI) is a broad category of technology that allows for gathering, storing, accessing and analysing data to help business users make better decisions.

Analytic Application

A software application designed to fulfil all the analytic requirements of a particular business process e.g. financial analysis, customer analysis. These applications are often marketed as turnkey solutions by business intelligence vendors.

Balanced Scorecard

An analysis technique, developed by Robert Kaplan and David Norton, designed to translate an organisation's mission statement and overall business strategy into specific, quantifiable goals and to monitor the organisation's performance in terms of achieving these goals.

Dashboard

A user interface that organises and presents information in a way that is easy to read. The name refers to the fact that it can sometimes look like the dashboard of a car. Also known as cockpits or scorecards. (See also Balanced Scorecard)

Data Mart

An analytical data store focused on one particular business function designed to serve a particular community of knowledge workers. Often, the data mart is sourced from a sub set of data in a data warehouse and sometimes stored in a cube format for faster analysis.

Decision Support System

A now superseded term for a software application that analyses business data and presents it so that users can make business decisions more easily. (See also Business Intelligence)

OLAP

On-line Analytical Processing (OLAP) is defined as providing fast access to shared multi-dimensional data. OLAP is a term used to generically refer to software and applications that provide users with the ability to store and access data in multi-dimensional cubes. (See also Multi-Dimensional Analysis and Cubes.)

4.6 Risk Measurement

Risk Measurement

Understanding the nature and scale of fraud is an initial and critical step, fundamental to the development of any counter fraud strategy.
The Risk Measurement method can help you to assess the fraud within and against your organisation by conducting risk measurement exercises.

Based on the results, you can make sure that you are correctly prioritising your counter fraud action and targeting available resources at the areas most at risk from losses to fraud.

Risk measurement not only identifies the scale of problems but also allows you to test how effectively your anti-fraud strategies are working and, indeed, if the threat is changing.

4.7 Pre-Employment Screening

Introduction

An organisation can suffer financial and reputation damage through failure to carry out proper checks on potential employees. Vetting ensures that you are familiar with the history of the person you are employing and protecting your organisation against employing the kind of person you do not wish to have. Having an honest and appropriate workforce is an essential criterion for an organisation. There are various ways of trying to detect employee fraud, but it is better to stop fraudsters from targeting organisations for employment in the first place. An organisation must ask itself whether it wants to employ someone who is dishonest.

Views on Integrity Management

By means of pre-employment screening, a picture is created of the new employee. With this information, possible risks can be listed and estimated, and a decision can be made whether or not the employment of the new employee is justified.
It is equally important to know something about the integrity of current employees eligible for a promotion or a change in responsibilities.

Effective integrity and screening policies are not only beneficial to the employer but also to employees. The impact on colleagues of a fraud investigation is significant both in terms of time and morale.

Pre-Employment and In-Employment Screening

Standard pre-employment screening consists of several elements. These elements are compiled in such a manner that they give not only insight into the personal data, but also into the employment history, the morality and integrity of the person in question. Needless to say these investigations – which are performed only with the approval and cooperation of the candidate - are sensitive and must be carried out in accordance with laws on privacy and the protection of personal information.

It is equally important to carry out follow-up screenings of employees throughout their career. Circumstances change. Somebody might have been screened when joining the company and appeared to be honest, but can be tempted into improper behaviour at a later date.

Integrity is not an unchanging characteristic, it can be learned. An integrity audit can be very useful in this process. This involves an overall description of the integrity status of an organisation where, amongst other things, the possible risks and consequences of fraud can be described. Furthermore one can get a clear view of any measures already taken, how effective they are and how they can be further improved.

Screening of Legal Bodies

When you need more information about the status, integrity and solvency of business contacts, you can carry out an integrity check of legal bodies. These kinds of investigations cover such subjects as an identity check on managers or owners, an integrity check, a financial investigation and a reference check. Of course you may need the approval and cooperation of the person(s) in question.

Important Points to Remember:

- screening potential employees must be proportionate to the risk and the risk must be considered in light of what job the person will do, who they will come into contact with and to what information they will have access;

- not only the highest paid or most senior posts are to be vetted; there are jobs all over the organisation that require trust;

- temporary staff should be vetted as thoroughly as permanent staff, particularly in vulnerable areas;

- the applicants must be told in advance that pre-employment screening is a part of the procedure and applicants must sign an agreement before any vetting is undertaken;

- to get vetting procedures accepted within an organisation can be a long and arduous task. For some it is difficult to understand why it is important and what benefits there may be.

- vetting teams and Human Resources units must work together on this. It cannot be viewed as an extra task or a task that delays the recruitment process as an add-on, but one that is an integral part of all recruitment.

Annex H: General Information:
- Propriety Checks – EHFCN
- Medical School Index

Links:
- General Medical Council:
- Ribiz (utch Registration Healthcare Providers)
- Ministry of Education and Science for Qualifications and Foreign Qualifications
- Regional Associations
- Regional Health Authorities

Annex I: Overview per Country

4.8 Whistleblowing

Introduction

A whistleblower is an employee, former employee or member of an organisation who reports misconduct to people or entities that have the power and presumed willingness to take corrective action.

Generally the misconduct is a violation of law, rule, regulation and/or a direct threat to public interest: fraud, health and corruption are just a few examples.

The term whistleblower derives from the practice of English policemen who would blow their whistles when they noticed the commission of a crime. The blowing of the whistle would alert both other law enforcement offices and the general public of danger.

Overview

Any kind of misconduct may prompt whistleblowing.

The vast majority of cases are based on relatively minor misconduct. The most common types of whistleblowers are internal whistleblowers, who report misconduct to another employee or superior within their company or agency. In contrast, external whistleblowers report misconduct to outside persons or entities. In these cases, depending on the severity and nature of the wrong-doing, the whistleblower may report the misconduct to lawyers, the media, law enforcement, watchdog agencies, or to other local, state or federal agencies.

There are those who view whistleblowing narrowly and try to limit its impact by arguing that so-called role-prescribed whistleblowing, i.e. whistleblowing done by quality control personnel or internal auditors, does not constitute whistleblowing in the traditional sense, because the purpose of the employment is to report such things. However, the US courts have uniformly held that persons who hold quality control or auditor positions are protected from retaliation for reporting violations of law or regulations.

Common Reactions to Whistleblowing

Ideas about whistleblowing vary widely. Some see whistleblowers as selfless martyrs for public interest and organisational accountability. Others view them as "snitches", solely pursuing personal glory and fame. Because the majority of cases are very low-profile and receive little or no media attention and because whistleblowers who do report significant misconduct are usually put in some form of danger or persecution, the latter view is generally less held.

Persecution of whistleblowers has become a serious issue in many parts of the world. Although whistleblowers are often protected under law from employer retaliation, there have been many cases where punishment for whistleblowers has occurred. Many whistleblowers report that a widespread "shoot the messenger" mentality exists within organisations and in some cases whistleblowers have been subjected to criminal prosecution in reprisal for reporting wrongdoing. As a reaction to this many private organisations have formed whistleblower legal defence funds or support groups to assist whistleblowers. One such example in the UK is Public Concern at Work[9].

Legal Protection for Whistleblowers

Legal protection for whistleblowers varies from country to country. In the UK, the Public Interest Disclosure Act 1998 provides a framework of legal protection for individuals who disclose information which exposes malpractice and other matters of similar concern.

---

[9] http://www.pcaw.co.uk/

Anonymity

If you want to stay anonymous you can also contact Crime Stoppers International[10].

4.9 Integrity

Opinions are divided as to the exact meaning of integrity. Since the subject of integrity is very emotionally charged, it is important to clarify its exact meaning.
The term integrity is derived from the Latin word "in-tangere", which can be translated as "don't touch" or "untouched". Integrity refers to something or someone who is uninfected, unaffected or unviolated. Other meanings are fairness, incorrupt and intact.
Mostly integrity is defined as the absence of fraud or corruption. It is better to approach the term integrity in a more positive way, combining it with a notion of quality. In doing this, integrity means that an employee is fulfilling his job adequately and carefully in relation to his position and responsibility: "You do what you are supposed to do and you stand for it". Not committing fraud or not being corrupt is not enough. It calls for more. This means that besides the earlier mentioned requirements - there are also other values which need to be taken into account regarding integrity such as loyalty, reliability, customer orientation, objectivity, decency, and effectiveness and efficiency.
Additionally it is important to recognise that integrity is more than just complying with rules, especially when rules are lacking or rules are not clear. It is important to act in a responsible way in accordance with the employer's policies and procedures at all times.

4.10 Forensic Investigation Techniques

Computer Forensics:

- Data Recovery
- Electronic Discovery
- E-mail reviews

Document Formatting:

- Scanning of paper documents
- Searching by means of Optical Character Recognition (OCR)

Open Sources Research:

- Telephone books (Yellow Pages)
- Chamber of Commerce
- Web logs
- Advertising Sites

---

[10] http://www.c-s-i.org/

- Internet

Various:

- Figure Analysis
- Administrative research
- Benchmarks
- Procedure descriptions

Chapter

5

Sharing Information at European Level

5.1 Introduction

Along with prevention, a successful fraud and corruption awareness campaign can have an impact that lasts for many years.
It is essential that countries in Europe work together to deal with potential increases in cross-border fraud and corruption through exchanging information on current problems and solutions and building a strong network of contacts.

In this chapter we aim to demonstrate how you can set up a successful anti fraud and anti corruption campaign and provide you with the tools to do this.

5.2 Awareness Campaigns

European Healthcare Fraud and Corruption Awareness Campaign
The EHFCN coordinates a European Healthcare Fraud and Corruption Awareness Campaign (EHFCAC) across Europe on an annual basis.
In the Declaration, agreed at the first EHFCN Annual Conference in London in 2004, the EHFCN called for the creation of a real anti-fraud and anti-corruption culture within the healthcare systems among service providers, healthcare suppliers, healthcare payers, healthcare users and ultimately among all European citizens. It was agreed to designate one month every year in which each organisation in the Network could conduct activities to raise awareness of healthcare fraud and corruption. The period assigned for EHFCAC in each country may range from one day, to one week or one month. However, it is essential that there is "simultaneous activity" to raise awareness of the problem of healthcare fraud and corruption across Europe, starting on the same day and continuing over the same month.

The aims of EHFCAC are to:

- Promote awareness of healthcare fraud and corruption issues;

- Make it clear that healthcare fraud and corruption will not be tolerated;
- Demonstrate that action is being taken;
- Deter those who commit healthcare fraud and corruption by promoting an anti-fraud and anti-corruption culture;
- Develop awareness systems to counter healthcare fraud and corruption.

By creating an anti-fraud and anti-corruption culture and a deterrent effect; organisations are able to reduce losses to fraud and corruption to ensure that resources are spent on patient care.

5.3 Prevention

Preventing Fraud

Even the strongest deterrent cannot be 100% successful, so it is important to ensure that the strongest possible prevention arrangements exist. Indeed, strong fraud prevention arrangements are a key part of the desired deterrent effect.

From a general point of view, prevention should be achieved by introducing quality management systems in healthcare, setting up written procedures, and undertaking periodical monitoring and internal control checks. When setting up such systems and procedures consideration should be given to patients, healthcare professionals and suppliers.

Patients should be educated concerning their rights and duties. Healthcare professionals should be informed about any relevant legislation in force, ethical principles and quality management system in healthcare. With regard to suppliers, it is necessary to establish very accurate contracts, and quality assurance and control procedures should be part of the contract.

One of the most useful sources of information when preparing preventative systems and procedures is to refer back to previous fraud investigations.

A key part of any professional investigation is to determine what the crucial system weaknesses were which allowed the fraud to occur and to alert those who monitor systems, such as auditors, and those who can influence change to systems and regulations.

Chapter 6

Sanctions

When fraud or corruption is determined you must take appropriate sanctions. In each country there are different laws and legislation. The EHFCN[11] has produced an overview of legal arrangements per country.

---

[11] See www.ehfcn.org and consult the Legal Arrangements Database.

Chapter 7

Contact Directory

7.1 Introduction

It should be stressed that one of the aims of the EHFCN is to facilitate communication between those who are working to counter fraud across Europe.

The EHFCN website provides you with key information about different healthcare systems, personal contact details, different pieces of legislation in force and contact details of individual professionals and public bodies that are related to the investigation of fraud and corruption. Links between Members can also build and grow through working group meetings and the Annual Conference.

7.2 Members' Contact Details

It is very useful to have contact details for other members of the EHFCN. You can ask them for information or obtain the benefit of their experience to help solve any problems you may be experiencing with a particular fraud investigation.

7.3 Useful Contacts per Country

Annex J: the Netherlands

7.4 Key Contacts

Annex K lists key contacts from Austria, Belgium, France, the Netherlands, Norway, Poland, Spain (Catalonia), Scotland, Turkey and the United Kingdom.

7.5 Public Bodies per Country

Annex L lists Public Bodies contacts for Belgium, the Netherlands, Norway, Poland, Scotland, Spain (Catalonia), Turkey and the United Kingdom.

7.6 Public Sources per Country

Annex M lists Public Sources for Belgium, France, the Netherlands, Norway, Poland, Turkey, Spain (Catalonia) and the United Kingdom.

7.7 Specialists or Specialist Agencies

Annex N lists Specialists or Specialist Agencies for Belgium, the Netherlands, Norway, Turkey and the United Kingdom.

Chapter 8

Additional Information, Documents & Links

8.1 Introduction

The aim of this chapter is to help to answer any questions and clarify which documents of investigation are available.

Please note that this document is constantly under review and therefore subject to change. Counter fraud specialists are invited to contribute to improve this list.

8.2 Links

AFRIKANSERVER	http://www.africaserver.nl
Crime Stoppers International	http://www.c-s-i.org
Economic and Social Council (ECOSOC)	http://www.un.org/ecosoc
Economic and Social Development	http://www.un.org/esa
EPAC	http://www.epac.at
EVD	http://www.evd.nl
Foundation for International Studies on Social Security (FISS)	http://www.fiss-socialsecurity.org.uk
Global Campaign on Social Security and Coverage for All	http://www.ilo.org

HEALTHFINDER	http://www.healthfinder.gov
HelpAge International	http://www.helpage.org
Institute of International Social Cooperation (ICOSI)	http://www.icosi.org
International Actuarial Association (IAA)	http://www.actuaries.org
International Commission on Occupational Health (ICOH)	http://www.icohweb.org
International Construction Institute (ICI)	http://www.internationalbuilders.org
International Council on Social Welfare (ICSW)	http://www.icsw.org
International Federation of Health Plans (IFHP)	http://www.ifhp.com
International Federation on Ageing (IFA)	http://www.ifa-fiv.org
International Institute of Administrative Sciences (IIAS)	http://www.iiasiisa.be
International Institute on Ageing (INIA)	http://www.inia.org.mt
International Labour Organization (ILO)	http://www.ilo.org
International Monetary Fund (IMF)	http://www.imf.org
International Organization for Standardization (ISO)	http://www.iso.org
International Social Science Council: Comparative Research Programme on Poverty (CROP)	http://www.crop.org
International Society for Labour Law and Social Security	http://www.asociacion.org.ar
International Statistical Institute (ISI)	http://isi.cbs.nl
International Training Centre	http://www.itcilo.org/en

ISSA	http://www.issa.int
Organisation for Economic Co-operation and Development (OECD)	http://www.oecd.org
Organización Iberoamericana de la Seguridad Social (OISS)	http://www.oiss.org
PAKISTANHOSPITALS	http://www.pakistanimagebuildingforum.org
Rehabilitation International (RI)	http://www.rehab-international.org
SELAMPTA	http://www.selamta.net
Social Protection	http://www.ilo.org
Social Protection and Labor	http://www1.worldbank.org/sp
Social Security Policy and Development Branch	http://www.ilo.org
SOCIALSECURITY	http://www.socialsecurity.fgov.be
Strategies and Tools against Social Exclusion and Poverty (STEP)	http://www.ilo.org
Union of International Associations (UIA)	http://www.uia.be
United Nations	http://www.un.org
United Nations Research Institute for Social Development (UNRISD)	http://www.unrisd.org
USEMBASSY	http://thehague.usembassy.gov
World Bank	http://www.worldbank.org
World Health Organization (WHO)	http://www.who.int
World Medical Association	http://www.wma.net
World Safety Organization (WSO)	http://www.worldsafety.org

Europe

Council of Europe	http://www.coe.int
European Association of Paritarian Institutions of Social Protection	http://www.aeip.net
European Association of Public Sector Pension Institutions (EAPSPI)	http://www.versorgungskammer.de
European Centre for Social Welfare Policy and Research	http://www.euro.centre.org
European Health Forum Gastein (EHFG)	http://www.ehfg.org
European Institute of Social Security (EISS)	http://www.eiss.be
European Social Insurance Platform (ESIP)	http://www.esip.org
European Union	http://europa.eu
Information Society	http://ec.europa.eu/information_society
Economic and Social Committee	http://www.epsu.org
Employment and Social Affairs	http://ec.europa.eu/employment_social
European Agency for Safety and Health at Work	http://osha.europa.eu
European Employment Observatory	http://www.eu-employment-observatory.net
European Foundation for the Improvement of Living and Working Conditions	http://www.eurofound.europa.eu
Mutual Information System on Social Protection in the Member States of the European Union (MISSOC)	http://ec.europa.eu
Statistical Office of the European Communities (EUROSTAT)	http://epp.eurostat.ec.europa.eu
US-EU Cooperation on Workplace Safety and Health	http://osha.europa.eu/eu-us
Institut de la protection sociale européenne (IPSE)	http://www.euroipse.org
Observatoire social européen	http://www.ose.be

Organización Iberoamericana de Seguridad Social (OISS)	http://www.oiss.org
United Nations Economic Commission for Europe (EC)	http://www.unece.org

Africa

Organization of African Unity (OAU) - African Union (AU)	http://www.africa-union.org
United Nations Economic Commission for Africa (ECA)	http://www.uneca.org

Americas

Caribbean Actuarial Association	http://www.caa.com.bb
Caribbean Community (CARICOM)	http://www.caricom.org
Centro Interamericano de Estudios de Seguridad Social (CIESS)	http://www.ciess.org.mx
Consejo Centroamericano de Instituciones de Seguridad Social (COCISS)	http://www.sica.int
Inter-American Conference on Social Security (CISS)	http://www.ciss.org.mx
Organización Iberoamericana de Seguridad Social (OISS)	http://www.oiss.org
Pan American Health Organization (PAHO)	http://www.paho.org
United Nations Economic Commission for Latin America and the Caribbean (ECLAC)	http://www.eclac.cl

Asia and the Pacific

Asean Social Security Association (ASSA)	http://www.asean-ssa.org
Asian Development Bank (ADB)	http://www.adb.org

Social Protection	http://www.adb.org/socialprotection
United Nations Economic and Social Commission for Asia and the Pacific (ESCAP)	http://www.unescap.org
United Nations Economic and Social Commission for Western Asia (ESCWA)	http://www.escwa.un.org

8.3 Documents

Annex O:

- Tackling External Fraud
- Medical School Index
- IAIS Fraud Report
- Cross Border Presentation
- Global Corruption Report 2006 TI

8.4 Healthcare Systems per Country

Annex P: Healthcare Systems per Country

Chapter 9

Training

9.1 Introduction

From the very onset, the EHFCN has taken a keen interest in providing training to (improve) counter fraud and corruption across Europe.

Its initial objective was to conduct research into the currently available training programs in respect of countering fraud and corruption in healthcare.

The ultimate goal is to use the training syllabus as a standard for all healthcare organisations in Europe. For more information please consult the EHFCN website[12].

Several countries offer special training programs for counter fraud specialists.

---

[12] www.ehfcn.org

Chapter 10

Biography

The following people/organisations/ literature sources have been consulted, to establish this manual.

Association of Certified Fraud Examiners	http://www.acfe.com
CAPER	http://www.caper.ca
CFSMS	http://www.cfsms.nhs.uk
CNAMTS	http://www.ameli.fr
Commission for the Prevention of Corruption	http://www.kpk-rs.si
EHFCN	http://www.ehfcn.org
Ernst & Young	http://www.ey.com
Federal Ministry of the Interior (BIA)	http://www.bia-bmi.at
General Medical Council	http://www.gmc-uk.org/
General Subdivision of Healthcare Evaluation and Inspection, Health Resources Head Office, Catalan M	http://www.gencat.net
Hoffmann	http://www.hoffmannbv.nl
International Association of Insurance Supervisors IAIS	http://www.iaisweb.org
KPMG	http://www.kpmg.com
Ministry of Education and Science for Qualifications and Foreign Qualifications	http://www.mec.es
Ministry of Health Turkey	http://www.saglik.gov.tr
Ministry of Health. Poland	http://www.mzios.gov.pl

National Audit Office NAO	http://www.nao.org.uk
National Institute for Health and Disability Insurance (INAM I- Institut National d'Assurance Maladie)	http://www.inami.fgov.be
Nav - Norwegian Labour and Welfare Service	http://www.nav.no
NFZ POLAND	http://www.nfz.gov.pl/new
NHS Scotland Counter Fraud Service	http://www.cfs.scot.nhs.uk
NHS UK	http://www.nhs.uk
Regional Associations	http://www.comb.es
Regional Health Authorities	http://www.gencat.net
Ribiz Dutch Registration Healthcare Provider	http://www.ribiz.nl
SPSS	http://www.spss.com
Transparency International	http://www.transparency.org
Unive (IZA, TRIAS, VGZ)	http://www.unive.nl
VERBOND van VERZEKERAARS	http://www.verbondvanverzekeraars.nl
Zorg en Zekerheid	http://www.zorgenzekerheid.nl
Zorgverzekeraars Nederland	http://www.zn.nl

EHFCN
EUROPEAN HEALTHCARE
FRAUD & CORRUPTION NETWORK

© EHFCN AISBL
Avenue de Tervueren 211 Tervurenlaan
1150 Brussels
Belgium