# Healthcare fraud

Understanding and measuring fraud

Best practices for proven technology to reduce Healthcare fraud

# Background of this white paper

The issue of healthcare fraud is proving to be a major concern as more and more enquiries are made to Eurosmart and its members how to  tackle this problem.

Eurosmart selected five countries for its study on Healthcare fraud: France, Germany, the UK, the USA and Slovenia as very detailed information have been made available in the past months (see the EHFCN's and NHCAA 's reports page 13 and 22). The differences in share of public and private funding, size of population, type of culture (Mediterranean, Anglo-Saxon and others) were also key criteria for the short-list.

## About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work in dedicated working groups (communication, marketing, security, electronic identity, new form factors and prospective emerging markets).

Eurosmart is acknowledged as representing "The Voice of the Smart Security Industry" and is heavily involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit **www.eurosmart.com**

# Summary

# Introduction

This white paper presents a compendium of observations on trends in healthcare fraud, as well as a selection of best practices and specific recommendations to reduce fraud by implementing better-coordinated IT processes and by putting technology to better use.

In our report, the term “healthcare system” encompasses healthcare funding, the provision of healthcare and healthcare administration. Although fraud affects funding for healthcare, it is committed at the time services are provided, hence the need to analyze both healthcare funding and the provision of healthcare itself.

It therefore seemed beneficial for Eurosmart to share the accounts given by our members and their clients — as well as their best practices—and recommend a select number of practical, targeted measures to better combat this serious and growing threat to healthcare systems.

Over and above the debates, implementing improved systems is an entirely realistic goal. These systems can be extremely effective in fighting fraud, as well as in eliminating administrative errors.

This study provides a summary of the commentary gathered by Eurosmart during the period of 2009-2012. Given the great diversity of respondents, our study does not aim to provide a statistically representative survey of opinion.

Views presented here are not necessarily shared by the majority of stakeholders. It is important to note that this brief publication is simply an attempt to provide a fair summary of all contributions, as they were presented to Eurosmart. Our study does not take a position with respect to respondent commentary.

Given the broad scope of healthcare fraud, the study does not purport to provide an exhaustive assessment. It gives a solid basis for understanding the issue of fraud in healthcare systems and solutions that can be considered.

December 2012

# Abstract

On average, around **6% to 10%** of spending in the healthcare sector is lost to fraud, according to the European Healthcare Fraud and Corruption Network (EHFCN). In Europe, which spent €1,100 billion on healthcare in 2010, this means nearly €110 billion was lost in that year alone. Feedback from interviewees for this study indicates that the higher EHFCN figure is closer to the true cost of this problem.

Fraud, abuse and errors are not just an issue for one specific healthcare system. They occur **everywhere**, regardless of the share of public and private funding, levels of technology, the type of culture (Mediterranean, Anglo-Saxon, European and others), or the amounts of money involved.

Usually, fraud involves the payment of unauthorized benefits, or access to services through intentional deception or misrepresentation. Three trends are currently gaining ground: a **shift from fraud committed by isolated individuals to that committed by organized groups, the intentional endangerment of people's lives** for financial gain, and an **increase in identity theft**.

**All processes seem to be affected,** and **anyone can be involved.** This means fraud mechanisms are becoming more complex, and that detecting fraud requires forms of collaboration that can be difficult to establish (fraud investigators, law enforcement officers and lawmakers).

Even if healthcare professionals are sometimes involved, administrative procedures relating to healthcare claims processing are inadequate, in terms of **data integrity, patient identity and claiming entitlements.**

The best practices for the fight against fraud can be found in a systemic approach, all components of which (legal, technical, administrative, etc.) must be improved.

Although we must accept that progress will be made in each area at a different pace, the legal framework does not have to be finalized before technical and organizational solutions can be implemented, especially since fraud has to be tackled dynamically, on a continual basis, as the healthcare sector is in constant flux.

Even if this comprehensive approach takes time, and is difficult and costly initially, it provides a considerable return on investment. **The United States** began to fight fraud and improve data quality 10 years before European initiatives started to take shape, and their experiences must be used as a guide, along with the successful strategies implemented by **the banking sector**, which now has a fraud rate of less than 1%.

**Information technologies** must be regarded as essential and indispensable for improving healthcare information systems. They are powerful tools to achieve potentially considerable **results in the fight against fraud and abuse, as well as to eliminate errors**.

The quality of data entered automatically at the source, the protection of data confidentiality and the issue of claimant identification (as well as the protection of entitlements) are issues in all healthcare systems. It is therefore not surprising that microchip card technology has been included in most universal healthcare and healthcare programs deployed over the last 20 years.

Government agencies and health insurance organizations should liaise with global technology partners able to integrate the power of IT and smart card technologies to fight fraud.

They can better anticipate enrolment, card issuance identity and right verification issues. These suppliers will ensure higher efficiency in fighting fraud characterized by best practice sharing.

**Smart card technology is often under-used** at present, in areas where it can achieve excellent results.

> **Strong identification and authentication** for patients and healthcare professionals are key features of microchip cards, and should be implemented in the healthcare sector. Yet this is not the case in many countries.

> Implementing healthcare smart cards with an identification number and PIN or biometric authentication would enable the creation of personalized **online services,** a quintessentially «patient-centric» approach, but these initiatives are still in the development stages.

> The ability to **verify benefits**, expiration dates, repeated and multiple uses is on the whole under-used.

> Thus far, the benefits of paperless, electronic medical data exchanges have not been fully tapped. Yet cards have a role to play in **creating consistent databases,** with the automatic reading of data, and the temporary or permanent **confidential local storage** of additional data such as blood groups, allergies, chronic diseases and associated treatments.

**This robust technology can strike at the heart of fraud mechanisms,** often with little investment in infrastructures, and without major changes for patients and healthcare professionals. Smart card technology is an invaluable asset to combat fraud in healthcare in the interest of all.

# Nine recommendations from Eurosmart

>> These nine recommendations are detailed in chapter 5.

1. Take stock of feedback from existing systems and stakeholders
2. Set up a central body to manage the system as a whole
3. Adopt paperless procedures that enable more structured administrative and medical data for consistent data quality through smart card usage
4. Implement microchip card technology to make a priori checks simple and efficient
5. Rather than make healthcare professionals enforce regulations, delegate this task to card technology
6. Implement back-up procedures (hard copies), ensuring that they are highly secure
7. Ensure that the entire system is highly secure
8. Validate the identities of patients and professionals using a secure face-to-face registration process
9. Leverage the experience of key industry players

# Chapter 1: Mixed-model plans and the shared challenges of healthcare systems

## Four basic models

>> The idea of universal healthcare is not new. To fully understand the variety of healthcare and health insurance systems, we need to understand their origins. Indeed, government programs for healthcare, retirement benefits and family allocations, and in particular health insurance, are the legacies of national traditions. They have developed according to four different models

### The Bismarck model

This model of universal healthcare was created in Germany by Bismarck, who enacted social legislation between 1881 and 1889. Health insurance and access to healthcare are therefore linked to the notion of employment in this system. It is financed through social contributions, rather than taxes.

This model relies on health insurance funded through social contributions (by employers and employees), managed by the representatives of companies and employees. The state must decide on the scope of intervention of health insurance funds, and take the appropriate measures if a financial imbalance arises. The German example was used as a blueprint in Austria and Belgium, in France with the decrees of October 1945, in Luxemburg and the Netherlands.

In all countries that have adopted the Bismarck model, protection has been extended to include population categories that were not protected initially (students, independent workers, etc.), and “risks” not taken into account to begin with.

### The Beveridge model

Implemented in 1942 in the United Kingdom following Lord Beveridge’s report, this social protection system is based on the principle of universal access to healthcare, non-dependent on employment. This access to healthcare is not considered as contingent on employment, but rather as an intrinsic part of citizenship. Public authorities fund this system through taxes, rather than through social contributions. A centralized system is in place in the United Kingdom and Ireland, while a decentralized system has been adopted by Mediterranean countries (Greece, Spain and Portugal).

### The Semashko model

This model, which was developed during the 1920s in the Soviet Union, then spread to the USSR’s satellite states after 1945. It is named after Nicolai Semashko, the USSR’s health minister from 1918 to 1930. It was, of course, the product of a specific political ideology. Healthcare services belonged to the state, and healthcare professionals were paid by the state. Services were usually free, but patients had to pay out-of-pocket fees for medication, for example.

>> The system provided universal access to healthcare. It was broadly a benefits in kind system. Coverage levels and the amounts set aside for healthcare spending (share of GDP) were defined centrally.

Healthcare and health insurance systems from this era are currently undergoing radical change in the Central and Eastern European countries.

### The out-of-pocket model

The fundamental principle of the American healthcare system is that health is a matter of individual responsibility and private insurance.

In practice then, there is no compulsory national system, and a preponderance of private organizations (two-thirds of Americans under the age of 65 are covered by employment-related insurance).

Public healthcare is only provided for the elderly (Medicare) and disadvantage (Medicaid), not unlike the Beveridge model. These two programs were established in 1965 under the administration of Democrat L.B. Johnson.

Medicare is a federally funded and managed healthcare system for citizens over 65 and Medicaid is a jointly funded system between the federal and state governments for families with low incomes and resources. Both Medicare and Medicaid are the responsibility of the federal agency, Centers for Medicare & Medicaid Services (CMS). CMS directly manages Medicare and oversees Medicaid. The states manage their individual Medicaid programs for their citizens.

## Mixed-model plans

### European mixed-model plans aimed at ensuring healthcare for all

The Bismarck and Beveridge models have had a lasting influence on most European countries.  During the second half of the 20th century, all European countries progressively extended universal healthcare to cover nearly all citizens.

Since the implementation of the CMU (universal healthcare coverage), the French system has ensured that everyone has access to healthcare. Employment no longer determines access to healthcare, as is theoretically the case.

### The universal challenges of system efficiency and funding

For the last 20 years, faced with the sharp rise in healthcare costs, all European countries have tried to rein in spending, while improving the efficiency of systems in place. Funding methods have not been called into question. In all countries influenced by the English model, funding mainly comes from taxes, while in other countries it is mainly drawn from social contributions. In countries influenced by the Bismarck model, such as France or the Netherlands, social protection is mainly funded through contributions. These differences in funding are linked to how the system is organized: in general, funding through taxes corresponds to a state-run organization, while funding through social contributions usually means that trade unions and employers' organizations are involved.

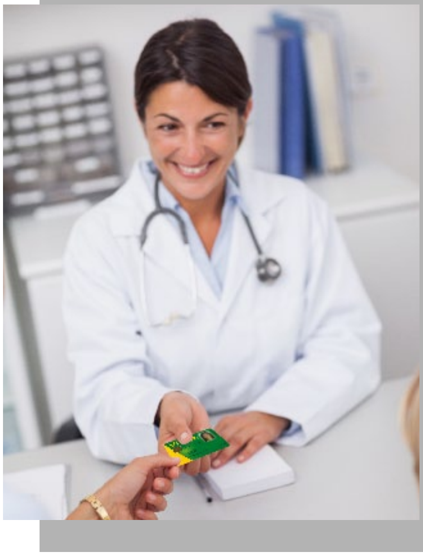
### Justifiable efforts to improve efficiency and fight fraud

The healthcare sector is an important part of our societies, due to the resources which are allocated to it, the role played in healthcare by the state or regional authorities, and because of the large number of stakeholders which it links, either directly or more indirectly. More than €1,100 billion is spent in the European Union on healthcare.

Social protection does not fall under the jurisdiction of the European Commission, but is an example of the principle of subsidiarity, and therefore under the jurisdiction of national governments. That being said, Europe-wide cooperation does exist on the matter, in particular concerning the cross-border mobility of patients (with measures such as the E111 form). Cooperation also facilitates the exchange of knowledge and best practices. The existence of cross-border organized fraud is a particular problem for small European countries.

Three major challenges arise when considering healthcare system management.

**National healthcare spending represents 17% of the United States' GDP, 12% of France and Germany's, and 10% of the UK's in 2010 (source: OECD, 2011).**



## The three chief challenges to providing healthcare

### Providing long-term healthcare while ensuring a steady source of funding

The first challenge is of course to maintain or improve the health of citizens by providing healthcare that meets the legitimate expectations (medical or otherwise) of the general public. Issues surrounding the funding of the system, continuity and proper management are, of course, fundamental.

We will mainly focus on the best ways to manage the resources available. There are several priorities, such as optimizing the system by rendering procedures paperless, freeing patients up from the many administrative procedures linked to the management of healthcare.

If the aim is to implement lasting improvements, the fight against fraud, abuse and error must, of course, be included.

As one of our French contacts explains, fraud is a serious and growing problem in particular in terms of social injustice and its consequences.

> **"Every euro we lose to fraud and abuse is a euro that is not available to treat AIDS, to immunize children, or to discover new treatments for cancer and other diseases. Some fraud schemes even pose a direct threat to the health and safety of patients. The information I have gathered during my research has shown me that existing verification systems do not work the way we imagine they should. Often the manner in which fraud schemes are revealed suggests that detection is more down to luck than method.**
>
> **That's why we need to create a reference system and set up indicators for security needs related to risks of fraud and errors. This framework will allow us to define the scope of what we want to assess, nationally and of course for international exchanges. Setting up an organization in this way would allow us to move from fraud detection to fraud prevention."**

A less controversial subject, and more essential for implementing and monitoring healthcare systems, is the management of errors, an even greater part of the drive for efficiency, in other words meeting targets with the optimal use of resources.

Take, for example, the inadvertent effects or complications resulting from medical treatment or advice, known as iatrogenesis. This is an issue of some magnitude. In the United States, the total number of deaths due to iatrogenesis in 2001 reached 738,936. The number of deaths caused by cardiac disease was 699,697, and 553,251 deaths were caused by cancer (source: American Iatrogenic Association 2002). In France, in 2004 the number of deaths resulting from iatrogenesis was higher than 10,000, and 3.19% of hospital stays were due to medical errors and medication errors.
A financial assessment of this issue is particularly difficult to carry out. No realistic study relating to the amounts involved was to be found. But the causes of the phenomenon are known.

Iatrogenesis can be linked to many factors, such as doctors lacking information or training, patients lacking information or education, prescription errors (inappropriate medication: dose, protocol, treatment), over-prescription or incomplete prescription, a lack of information on the patient (allergies, symptoms not all taken into account, multiple pathologies), an under-estimation of drug interactions and self-medication.

Between 30% and 50%+ of iatrogenesis could be avoided (French Ministry of Health, July 2010). Better information systems could play a part in cutting this figure. This is one of the goals of the Personal Medical File.

## Focusing the work of healthcare professionals on patient health

Most programs in this area are aimed at facilitating information exchanges and helping healthcare professionals to concentrate on care and treatment rather than management. This attempt to reorganize the relationships between patients, healthcare professionals and administration is greatly helped by the introduction of new digital technology for exchanges between healthcare or insurance organizations, and the creation of health cards.

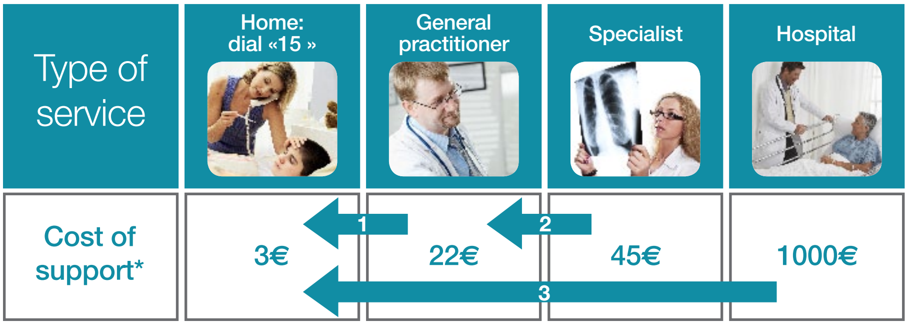
These factors can often lead to drastic improvements. In France, for example, patients are now reimbursed after five days, rather than after two or three weeks (due to paperwork). More than 1.1 billion electronic claim forms were used in 2010—representing 85% of all claim forms—resulting in increased administrative productivity and treatment costs divided by six for the claims in question. The introduction of electronic claim forms and the cut in the number of statement sheets means that 3 billion A4 sheets of paper are saved. They are no longer produced, printed, distributed, stored or destroyed.

## Coordinating and optimizing information-sharing

The aim is to optimize the use of medical data. A patient's "Personal Medical File" ensures that all their medical information can be accessed by healthcare professionals, whenever and wherever. This record therefore cuts errors and hesitancy in emergency situations, and improves the quality of services provided. It also improves cooperation between all healthcare workers, pooling all available information on patients into a centralized file.

Personal Medical Files streamline healthcare systems. They limit the number of medical interventions, and ensure that care provided for patients is consistent. There are also advantages for government health policy: a well-treated patient does not have to keep coming back.

Telemedicine also presents fantastic opportunities. This refers to any situation where information is passed between healthcare professionals electronically (general practitioners or specialists, care workers, pharmacists, etc.). This information could be messages, letters, signals, results, images, administrative data, complete files, etc., for diagnosis, therapy or monitoring.



| Type of service | Home: dial «15 » | General practitioner | Specialist | Hospital |
|---|---|---|---|---|
| Cost of support* | 3€ | 22€ | 45€ | 1000€ |

* : Cost of support for patient - France

Best practice :

1 • Dial «15» to get free medical support instead of calling a general practitioner
2 • Follow the healtcare process
3 • Favor home card and telemedecine

Telemedicine is a growing necessity due to the following:

> Centers of excellence are increasingly rare, while demand for them is increasing.
> There is a growing equality issue in terms of regional development.
> The exodus of certain services or specialties from entire regions, especially in emerging countries.
> The development of “Citizenship 2.0” in the modern world, and the sense that healthcare services should be accessible from anywhere.

The ideal model for telemedicine, pooling rare resources, ensuring that information comes to individuals rather than vice-versa, offers tangible progress in terms of personal health and social well-being. With the help of technical resources, secure, confidential, high-quality exchanges of information can be put in place, with face-to-face contact available when necessary.

Facts and figures relating to fraud, abuse and errors in healthcare claims processing systems in a few selected countries are detailed in the following chapter.

# Chapter 2: Measuring healthcare fraud

## Definitions

>> First of all, it is necessary to define exactly which types of “loss of income” are discussed: errors, waste, abuse and fraud.

### Error

This refers to the act of making a mistake. This can be both administrative and medical. Sound management of a system strives to correct errors, and to modify procedures which cause them, so that they are no longer made. Legally, errors are either examined with a view to correcting them, or to determine the validity of the act that produced the error.

### Waste

The intentional or unintentional, thoughtless or careless expenditure, consumption, mismanagement, use, or squandering of healthcare resources. Waste also includes incurring unnecessary costs because of inefficient or ineffective practices, systems, or controls.

### Abuse

Abuses are defined as the misuse, inordinate or unjust use of something. An abuse is also an act outside the norm, the rules, established through habit or usual practices. Abuses are of interest to the law, since the inordinate use of a right can often infringe upon the rights of others. In political discourse, abuses refer to people or organizations unjustly benefiting from a legal procedure.

### Fraud

Act in bad faith, detrimental to others. Dishonest act, made in order to cheat the law or regulations and obtain consent, undeserved moral or material gains or in order to shirk one’s responsibilities.

> The definitions given by the Swiss Institute of Comparative Law provides a definition that, overall, is relatively general and applicable in many countries. “Fraud is the use or 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 of others, or their misuse for purposes other than those specified.’”

The economic and financial consequences of fraud are certainly some of the worst aspects of the problem. Fraud is unethical, immoral and illegal. Those guilty of fraud should be prosecuted, and money gained through fraud should be recovered. But these measures only intervene after the act of fraud. The definition of an action plan, with an assessment of fraud levels as the first step, must integrate plans to combat fraud as well as systematic prevention plans.

## Assessment

The assessment of losses linked to fraud (abuses and errors), is of course the first indicator and driver for action. There are a number of disclaimers to be made.

First of all, it is an assessment rather than a statement of fact: the aim is to estimate the total amount of fraud, if the extent of fraud could ever be fully known, which is not possible. Furthermore, detected or measured fraud is only a partial indicator of total fraud, and varies considerably depending on the resources put into action. Finally, recovered amounts of money, lower still, mainly reflect the efficiency of anti-fraud systems in place.

Then it is necessary to precisely define what is included (or excluded) in the assessment: errors, abuses, organized groups, etc. Depending on the effectiveness of anti-fraud resources, fraud detected after five years of anti-fraud measures corresponds to 10% of actual fraud, and 1% of the “loss of income” due to fraud, abuses and errors. Furthermore, the distinction between the different terms can be hazy. The question is, how can the difference between opportunistic and premeditated fraud or abuse be defined?

It is also a political issue, since it includes economic and technical aspects, but also legal, ethical, and moral aspects. Declarations abound on the subject, but are often tactical. It is also a delicate issue, since it can uncover organized practices, and compromise a considerable amount of vested interests.

Finally, since it is a recent topic, legal tools (laws, decrees, etc.) and technical tools (paperless procedures, statistical tools) are still nascent, and cannot yet provide authoritative information on the subject.

## The eye-opening report by the EHFCN: €56 billion lost in the EU

The first major official publication in November 2009 on the topic, “The financial cost of Healthcare fraud”, provided us with an estimate of the financial impact of fraud, confirming that this is an issue of some magnitude. It provided results from analyses carried out in six countries: the United Kingdom, the United States, France, Belgium, the Netherlands and New Zealand. It studied 69 projects by 33 organizations in these 6 countries, and analyzed nearly €340 billion in spending. It did not take studies on detected fraud in these countries or opinion polls into account.

The work undertaken by the European Healthcare Fraud and Corruption Network (EHFCN) since 2004 groups together data from the following member states: Belgium, France, Germany, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Slovenia and the United Kingdom.

It established that out of the €1,000 billion allocated to healthcare spending in the European Union in 2008, nearly €56 billion was lost to fraud. In fact, between 3% and 10% of funds were misused. The average sits at about 5.59% of spending budgets, and this figure opened people’s eyes to the considerable amounts of money involved.

The different types of fraud which were analyzed were:

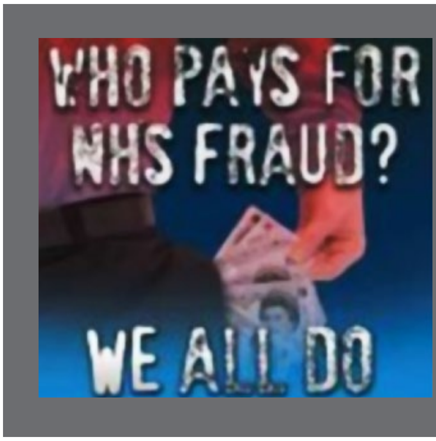
> The fraudulent provision of medical certificates
> Prescription fraud by pharmacists
> Prescription fraud by patients
> Fraud and errors relating to claims processing for general practitioners
> Fraud and errors relating to doctors’ payments for patient care
> Dental fee fraud
> Fraud and errors by opticians
> Fraud and errors relating to healthcare organization personnel
> Fraud and errors relating to costs for hospital services
> Fraud and errors relating to long-term care
> Fraud and errors relating to home care
> Fraud and errors relating to services and supplies
> Fraud and errors relating to child health insurance

The study concludes that, based on evidence gathered, healthcare systems fraud accounts for at least 3% of expenditures—a figure likely to be closer to 5% which may even be as high as 10%.

## United Kingdom: a rate greater than 3%, very likely to be as high as 10%

According to a May 2011 report by the EHFCN, the National Health Service (NHS) lost more than £3.4 billion out of a budget of £110 billion in 2010. Fraud is estimated at around 3% to 10% of overall spending. It should be noted that Paul Vinckle is the President of the EHFCN and Director-General of the NHS.

Nevertheless, NHS Protect, the "anti-corruption, violence and fraud" branch of the NHS, is a relatively recent creation, and the difficulties arising during its implementation probably account for the lack of experience and hindsight on the issue of fraud, in terms of audits and statistics.



**Pictured above, a message from the NHS. The following message from the EHFCN is just as clear:**

**"It is in the interest of all to eradicate fraud! Nearly 80 million Europeans live in poverty, and are denied access to healthcare. Every cent that is lost is a step away from a high-quality, universal healthcare system. Say no to medical fraud and corruption!**

**"Some people benefit from fraud, but it deprives us all of healthcare. Each year, for example, with the money lost to fraud we could build 3,500 new clinics or create 2.5 million nursing jobs."**

The NHS estimates that it lost £263 million in 2009 to fraud, or less than 0.3% of spending. The difference between this figure and the EHFCN estimate is 13 times higher. In France there is a similar learning curve in terms of estimating the extent of fraud in healthcare systems.

According to a press release in March 2011 by the British company PKF Accountants and Business Advisers, fraud in the public sector in the United Kingdom—and in particular in healthcare—represents around 4.57% of spending on average. This is around 30 times the measured amount.

## United States: between 3% and 10% of total expenditures

The United States began working to fight healthcare fraud relatively early on compared with European countries, in particular with the creation of the National Healthcare Anti-fraud Association (NHCAA). Furthermore, the American Health Information Management Association (AHIMA), which has a research branch, published in 2005 its first studies on two topics of interest to us: fraud assessment and the help provided by information technology in the fight against fraud.

In its September 2005 report on the use of technology in the fight against healthcare fraud, the American Ministry of Health, through The Foundation of Research and Education (or FORE, of the American Health Information Management Association) estimated that around 3 to 10% of expenditures was lost to fraud.

> "Fraud has a significant impact on the US health economy. The Nation Health Care Anti-Fraud association (NHCAA) estimates that of the nation's annual healthcare outlay at least 3%—or $51 billion in calendar year 2003—was lost to outright fraud. Other estimates by government and law enforcement agencies place the loss as high as 10% of our annual expenditure, or $170 billion."

For the Healthcare sector, technology from the banking sector could be very useful in the fight against healthcare fraud.

> "Much of the technology used in the financial and banking sector can be directly applied to the healthcare sector. Credit card fraud, currently estimated at less than 7 cents for every $100, so 0.07%, is widely seen as a major issue. Healthcare fraud is 100 times more costly!"

It should be noted that in 2010 the NCHAA confirmed its estimate. In its report, it also mentioned the work carried out by the EHFCN, and the consistency of the conclusions they came to.

> "Financial losses due to healthcare fraud are estimated at between $70 billion and the astronomical figure of $234 billion per year... The FBI estimates that between 3% and 10% of expenditures was lost to healthcare fraud."

## Slovenia: between 3% and 7%

Slovenia is very advanced in terms of managing and using new technology in its healthcare system, and is considered the breeding ground for the best practices in Europe.

Fraud is defined as an activity which aims to obtain an undeserved financial gain. I differentiate it from abuse, which has the goal of obtaining more services, but both need to be taken into account, since they damage public services.

It is estimated (ZZZS) that 3% to 7% of overall spending is lost to fraud. The official estimate is 3%, so €60 million per year.
This figure represents more than the total amount of funding for hospitals—€40 million in 2006.

## Germany: more than €15 billion in 2009

Germany spends more on healthcare than any other country in Europe: €278 billion in 2009. The healthcare system is regionalized, with more than 200 health insurance funds in competition since 2004, which remain relatively compartmentalized. Faced with demographic changes, and increasingly acute social gaps, in 2010 the government began a reform of the healthcare system, aiming to make spending in the sector fairer, more balanced and more sustainable.

The financial cost of fraud is estimated at between €8 billion and €24 billion by Transparency International Deutschland (2006). According to statistics on criminal activity, fraud is even more widespread in healthcare than in the construction industry, which is infamous for its poor practices in the country (source: KKH-Allianz). The EHFCN's 2009-2010 annual report gave an average rate of 5.60%, so more than €15.5 billion lost to fraud in 2009.

## France: an estimate at 1%, but the reality is different

The global fight against fraud in France really began in 2005. Social Security authorities estimate that in 2008, 1% of expenditures—or €1.5 billion—was lost to fraud, while 0.1% (€160 million) was detected. Let us recall the EHFCN's estimates of 5.6% on average —and up to 10%—or between €8 billion and €15 billion in France.

Indeed, although the study is focusing on health insurance, other national procedures should be examined, since they are just as affected by fraud problems. Comparative figures can be used to make estimates and reasoning more reliable.

In particular for France, we will therefore refer to other areas of the French Social Security system (CNAV, State Pensions Fund; CNAF, National Family Benefits Fund) and the French Treasury (DGFIP, taxes).

The following are the figures for detected fraud in 2008 for the three main offices relating to public spending:

- 0.11% for the CNAMTS (French National Health Insurance Fund)
- 0.001% pour la CNAV (State Pensions Fund)
- 0.14% for the CNAF (National Family Benefits Fund)

Source: Cours des comptes (French Court of Audit), Report on Sécurité Sociale, September 2010

1% of healthcare spending is currently estimated to be lost to fraud.

For taxes (DGFIP), nearly €14.7 billion in fraud was detected in 2009, out of a total budget of €360 billion, so around 4%. The effectiveness of the French anti-fraud system for taxes can be seen in the consistency of the amounts recovered, and the total estimated amount (detected + lost) could be around 7% to 8%.

This figure gives real credibility to the EHFCN's annual report, since the estimate of 10% could even be conservative, given that the health insurance sector, in its current state, is rife with opportunities for fraud, when compared with the tax sector.

Between 2009 and 2011, the press noted the "low estimates" of fraud rates by the authorities. In April 2011, newspaper Le Figaro in particular noted that:

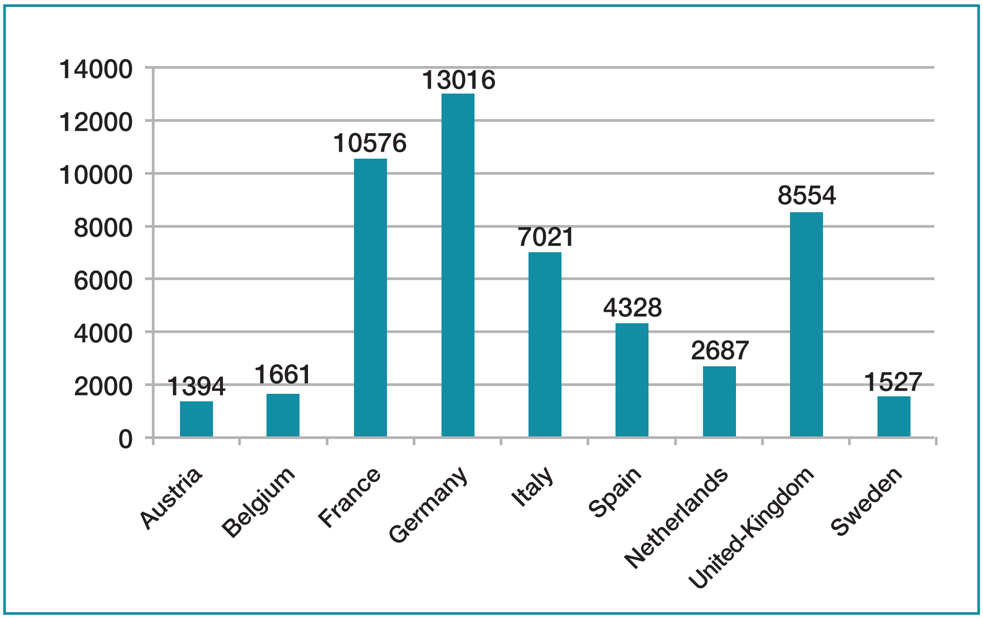
> "The Audit Court is currently assessing the level of benefit fraud. The 1% benefit fraud figure currently suggested by the directors of social governmental organizations is increasingly being questioned. …If we take into account "errors"—"overpayments" in Social Security jargon—the amounts of money lost by the authorities are much higher. For example, the CAF (Family Benefits Fund) detects €2 billion in overpayments each year."

It should be noted that the estimate based on a sample does indeed give us a figure close to 1% (between €540 million and €800 million). But this only covers fraud in the strict sense of the word, and €2 billion in detected "errors" (overpayments) should be added on. In short, the CNAF extrapolates 1% of fraud from a sample, and detects 3.6% of overpayments—which suggests that there must be more instances that haven't been detected. The total amount of "loss of income" should therefore logically be estimated as at least 6% to 7%, which corroborates the EHFCN's estimates.

## Summary: the EHFCN reveals the extent of fraud

During the investigations, and after several representatives of European countries pointed us towards the work carried out by the EHFCN, it is apparent that the 2009 and 2010 reports are fully capable of bringing debates to a close, in any case with regards to the amounts of money in play.

The amounts estimated in the graph below (EHFCN 2009-2010 annual report) show that in France in 2006 around €10 billion was lost to fraud and errors, so around 6% of healthcare spending. The estimate for Slovenia was €137 million, also 6%, which is in line with the statements made in the interview. The average rate announced 2 years previously by the EHFCN is still relevant.



**Estimated cost of healthcare fraud, in millions of euros**

**Source: 2009-2010 EHFCN report (2008 figures), at an average rate of 5.6%**

| Country | Population in millions | Healtcare spending in billions of € - EHFCN study | Estimated fraud for the country by % | Average rate of fraud by % - EHFCN 2009 study |
|---|---|---|---|---|
| France | 63 | 189 | 1 | 5,6 |
| Slovenia | 2 | 2,4 | 3 | 5,6 |
| UK | 68 | 153 | 0,3 | 5,6 |
| US | 308 | 1700 | 3 | Not included in EHFCN study |
| Germany | 82 | 232 | NA | 5,6 |

## Conclusion

Due to increasing budget cutbacks brought about by current economic circumstances, a real drive has been underway for several years to fight fraud. The work carried out by the EHFCN—in particular the 2009 study—has demonstrated the magnitude of healthcare fraud. Feedback from contacts interviewed, in particular on errors caused by information systems, has pushed the estimates towards the upper end of EHFCN figures.

Statisticians, given enough data, could probably draw up graphs based on the comments by our interviewees:

> **There is an average fraud rate of 6% to 10% in public contribution systems. The rate in the healthcare sector is similar.**

> **When audit and penalty systems are fully operational, behaviors change and average fraud rates drop below 6%.**

> **There are two rates which would seem nearly impossible to exceed:**
**- The recovery rate would appear never to exceed 70% of actual amounts lost fraud.**
**- The fraud rate would appear to never drop below 2%.**

# Chapter 3: What fraud is committed and who is involved?

## France: The types of fraud and those involved

>> Why are there so many differences in estimates? What explains these deviations? In practice, what kind of fraud are we talking about? The semantic debate, essential for measuring fraud, has raged in France, and shows the complexity of the issue.

### Definition, types and actors in France

Here is a case in France, reported in the newspaper Le Figaro (April 2011):

> "A hospital invoices a whole day of hospital treatment for a simple eye examination or an operation which wasn't carried out?" For the health insurance authorities, this is not fraud, but a mistake. Dr. Pierre Fender, from the DRF (Social Security Anti-Fraud Department), explains that this is because of the wording of the legal definition of fraud. According to the Civil Code, fraud is a deliberate, repeated act."

Let us take a look back at the work carried out by the DRF, in order to better understand the progress made by the Social Security authorities in France on the issue.

The DRF managed to recover around €132 million in 2008. Out of this amount, €13 million was recovered for fraud or abuse related to sick leave, nearly €33 million related to hospital institutions (25%), €11 million for cosmetic surgery fraudulently declared as medical treatment to claim reimbursements, many hospital treatment invoices for procedures which did not require a hospital stay (wart removal, cast removal), abuses linked to drug prescriptions, physiotherapy, nurses or midwives.

> Concrete examples of fraud:
>
> - After receiving a sick note from a doctor, a patient fraudulently alters the end date (more than 10,000 errors of this kind are detected every year)
> - Doctors writing up a very large number of sick notes (13% of sick notes are unjustified)
> - Patient misuses medical transport or taxis
> - Transport companies invoicing fictitious services, or invoicing too much

During a French National Assembly session in 2011, the different types of fraud were broached, including fraud relating to the alteration of prescriptions without the consent of the prescribing physician, changes to dosage, added medication, renewals without the consent of the prescribing physician or even falsified prescriptions presented by patients (and confirmed by an accomplice if the pharmacist makes a phone call).

The case of organized groups (a pharmacist with a prescribing physician or a patient) obtaining reimbursements for prescriptions that aren't filled is mentioned. The existence of "enabling" software at pharmacies supplied by certain software companies is also mentioned, though no reliable sources apart from the press are given. This software carries out false accounting, with the particular goal of cutting the amount of taxable income. This software is well known in the catering industry.

There is also the case of fraud by doctors who keep patients' e-healthcare cards and invoice fictitious visits.
This occurs even more often when patients receive French State Medical Assistance (AME- Aide Médicale d'Etat), since they do not have the "Vitale" e-healthcare cards.

There has been a sharp rise in the amounts recovered from university hospitals (CHU-Centre Hospitalo-Universitaire) between 2009 and 2010, increasing from €33 million to more than €127 million. Initiated in 2005, activity-based costing has also proved to be effective for monitoring spending.

## French administrative procedures are still rife with opportunities to commit fraud

In order to better understand fraud, we should not just focus on why people commit it, but also on the administrative procedures or roles that, due to their design, could be rife with opportunities for relatively opportunistic people.

As an example, an article published in newspaper France Soir on benefit fraud relating to earned income supplements (Revenu de Solidarité Active, or RSA) points out that one procedure requiring the verification of a number of conditions every three months (income, age, children, address, etc.) is rife with opportunities for fraud. Indeed, the volume of information to process on a regular basis, as well as the variety of information—and therefore how it is inspected—makes it nearly impossible to collect validated information. This increases the number of errors and intentional omissions.

## For French doctors, combating fraud is the responsibility of the police or Sécurité Sociale

After focusing on ill-intentioned people, in particular patients, transport companies and fraud or errors in CHUs, the role of healthcare professionals in the mechanisms of fraud was broached during a French National Assembly session in January 2011.

> **Vitale card theft**
Prescriptions are sometimes used up to 100 times before the French eHealthcare Vitale card is refused (as was the case in a large-scale fraud scheme trafficking drugs to the Congo). It is therefore essential that the process to declare stolen Vitale cards be expedited.

> **Vitale card picture ID**
Pharmacists do not have to check the identity of cardholders, since they do not have the legal right to do so (this is the case for all healthcare professionals). Furthermore, the photo sent for the card may not even be a picture of the beneficiary; there is no face-to-face meeting during the application process. Finally, someone can pick up medication for someone else who cannot make the trip. All things considered, it would seem that the photo serves no real purpose.

**French Vitale 2: What is the exact purpose of the patient's picture?**

### > Non-mandatory pharmaceutical records

At the time of writing, 12 million French citizens—25% of whom were over the age of 60—had established pharmaceutical records. For the Ordre des Pharmaciens (French pharmacists association), pharmaceutical records do not stop fraud since they are not compulsory. They can have an indirect effect, however. If a Vitale card is stolen, knowing that the cancellation procedure is not efficient, pharmaceutical records could be used to refuse the card. These records would not stop fraud perpetrated by patients, however. The association is not in favor of making pharmaceutical records or Personal Medical Files compulsory; 17% of French citizens currently refuse to establish pharmaceutical records.

### > Issues with reporting fraud to anti-fraud organizations

Pharmacists cannot report fraud, since they are bound by confidentiality obligations. A collaborative partnership has been agreed with Dr. Pierre Fender from the Anti-Fraud Department, but these exchanges are still informal, and information is shared only from the top down so far. An information-sharing procedure was nevertheless set up in 2010.

There is also the issue of **excessive sick notes.** It is difficult to estimate the figures involved, although the Social Security authorities have set the target of inspecting patients who have received notes from doctors who prescribed more than 20,000 statutory sick pay days in a year, the equivalent of 65 years of sick leave.

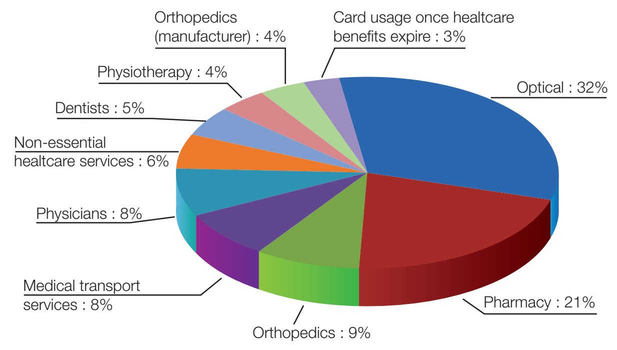
### > France: Conclusions on the types of fraud and those involved

- University hospitals are responsible for a considerable part of healthcare fraud detected by the Social Security authorities; detection has probably improved thanks to the new activity-based costing system introduced in 2005.
- The amounts recovered cannot be used as reliable representative samples of actual fraud.
- All healthcare professions are involved in detected fraud mechanisms.
- It is not up to healthcare professionals to fight fraud or to check the identity of patients.
- Prescriptions for medication are used in fraud, those guilty of fraud vary: patients, pharmacists, doctors, etc.
- The Vitale card is not an effective means of proof of identity.
- Medical records can only be effective in fighting fraud if they are compulsory.

# Germany: A rise in measured fraud in 2010

>> Germany also experiences a high level of health fraud. The KKH-Allianz group provides a breakdown of measured fraud in 2004-2005 by area in the chart below.

The following case is quoted. A German company that imports from China supplies 600 dentists with dentures. The supplier pays the dentists a commission and they implant the dentures in patients. The insurance company reimburses the company at the German national healthcare system's standard rate of €900, when in fact the actual cost of the dentures is only €120.



Fraud domains - Top 10

A typical fraud scheme in the country: the doctor orders medication from pharmacists, who record the order yet deliver nothing to the patient. The insurance organization "reimburses" the pharmacy and the pharmacist shares the proceeds with the doctor.

In March 2011, the German Doctors' Journal (Deutsches Ärzteblatt) explained that KKH-Allianz analyzed 949 cases of fraud in 2010. Investigators confirmed that the overall amount lost to fraud is the highest recorded in 10 years. They have asked that a specific "healthcare fraud offense" be defined. Given results in 2010, KKH-Allianz explained that the coordinated work of two investigative and legal bodies is necessary. Only then will it be possible to competently tackle accounting fraud. More than one in three cases of fraud relate to pharmacies. 25% of cases relate to physiotherapists, 6% to doctors.

At the start of 2011, AOK, the biggest health insurance organization in Germany with 25 million people and also the largest in Free States of Thuringia and Saxony announced that compared with 2009, the amount of detected fraud has doubled in these two regions alone.

> **"Even in cases where no one is prosecuted (20%), suspicion runs high for invoices with mistakes due to ignorance or accidental omissions. Criminal networks are often at work, involving pharmacists, psychologists, physiotherapists and midwives. There is a long list of suspicious prescribing doctors, based on sham agreements and very real fraudulent arrangements."**
> says Olaf Schrodi, AOK lawyer.

Source: Freie Presse, Sachsens Grösste Zeitung of March 4, 2011.

AOK
Die Gesundheitskasse.

## United States: The shape of fraud trends to come

>> According to an article in the Wall Street Journal published October 28, 2009, the United States loses at least $60 billion to healthcare fraud, waste and abuse a year. Up to 10% of total healthcare expenditures in the country could be lost in this manner, a considerable amount given that 2009 expenditures reached $2,340 billion (source: HHS, Centers for Medicare and Medicaid Services).

Under intense focus: the Medicare and Medicaid federal public healthcare systems. The Medicare program distributes more than $400 billion per year and audits just 3% of its spending. In 2008, Medicare announced that it paid out nearly $10 billion in overpayments (2.5% of total expenditures). $3.2 billion (32%) was recovered in 2008, and $4 billion in 2009.

Anti-fraud agencies focused on South Florida, greater Los Angeles, and other areas notorious for fraud.

The FBI noted two new trends in fraud in 2010 (October 2010 NHCAA white paper): the deliberate decision by some healthcare professionals to risk their patients' lives if a profit could be made, as well as identity theft.

In June 2010, a doctor in Kansas and his wife were arrested. They were making "miracle" pills. The doctor's clinic, specializing in pain relief, prescribed these pills. They received more than $4 million in unauthorized reimbursements from private insurance companies and federal healthcare programs. As a result, over a six-year period, 100 people overdosed and 68 died. This is of course not representative of the medical system in the country.

**Kansas: the Schneider couple (56 and 52 years old) : 68 deaths in six years**

In January 2010, the members of an "organized group" of clinics were arrested for large-scale fraud against the Medicare and Medicaid systems. This fraud involved the embezzlement of $110 million. The clinics in question, spread out over five states, were creating false reports for the treatment of AIDS, cancer and other diseases. To commit this fraud, the identity of patients eligible for Medicare benefits was stolen.

Identity theft in healthcare is a particularly heinous crime. The medical insurance and finances of victims are affected for years. As the Los Angeles Times noted, winning back one's identity is a full-time job.

The Foundation of Research and Education (or FORE, of the American Health Information Management Association) also classifies fraud by type:

- Suppliers submitting claims for fictitious procedures
- Invoices for visits that never took place
- Fictitious companies that have obtained a supplier number and file claims for people who never receive the healthcare
- Company invoicing equipment that was never received
- Paying citizens in good health to make unjustified visits
- Carrying out unnecessary surgical procedures
- Payment for medical certificate falsification, which require medical visits, in order to receive kickbacks
- Generation of false claims from fictitious clinics
- People posing as healthcare professionals
- Obtaining information on patients and clinics to submit claims (reimbursement or payment) for healthcare that was never provided
- Invoicing supplied services for more than what was paid
- Patients who visit several doctors in order to obtain several prescriptions for controlled substances
- Patients alleging that non-medical procedures were medically justified, and attempting to be reimbursed for them.

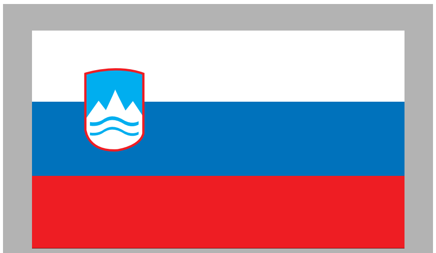
## Slovenia: The best practices in Europe

Slovenia has centralized administration and particularly effective citizenship and identity check procedures. It is currently the most advanced country in Europe in terms of modernizing its healthcare system. In 2009, Slovenia implemented an advanced electronic signature and identity system, which included the healthcare system in its scope, using next-generation cards (2010 Slovenian e-healthcare plan).

Our contact at the Slovenian health insurance authority (ZZZS), explained that healthcare fraud in Slovenia is mainly linked to the payment of employment-related taxes, prescriptions and medical equipment and services.

He provided us with a few examples of fraud detected through audits or brought to their attention:

- Salary increases with non-declarable income: luncheon vouchers, trips, per diem, etc.
- Borrowing health cards, due to the different ways of proving one's identity; second-generation cards have now restricted this phenomenon
- Request for unauthorized benefits
- Prescriptions for non-medical procedures: spas, medical relaxation devices
- Completely fictitious healthcare services
- Multiple invoices for the same services
- Fabricated waiting list
- Non-compliance with working hours paid for by taxpayer money (absenteeism)



Cross-border healthcare fraud is a concern for all countries. In 2007, 22,570 Slovenian insured parties applied for care out of the country, including 221 treatments with prior arrangement, for a total of €11.9 million. 70% of services were provided in Croatia, and concerned elderly people and tourists.
22,497 European Union citizens asked for emergency care in Slovenia, for a total amount of €9.7 million.

Until now, there has been no identity fraud, probably because the European health card has a shortened 3-month validity period. The risk seems higher for special cross-border care, which aims for all costs to be covered by public funds.

Our contact quoted the case of Slovenian women traveling to a private clinic in Austria in 2006 and 2007 in order to give birth. They then filed claims, using their European health insurance card. The Slovenian health insurance authorities rejected these claims, arguing that these services could not be classified as emergency services. Treatment that is planned out cannot be taken into account by this system.

## Supranational classification of the types of fraud

A more thorough analysis of global fraud mechanisms in the healthcare sector was carried out in Transparency International's 2006 study.

A number of factors make the healthcare sector more vulnerable to fraud:

- The difficulty of implementing rules that can be applied to everyone
- The fact that healthcare is delegated to private organizations, which are often tempted to put financial interests above patient health
- The astronomical amounts of money involved, estimated at more than $3,100 billion in 2006 (globally)

The types of fraud or abuse detected are classified, and full definitions are provided in the study.
Here is a summary of the list:

Procurement

- Over-payment for goods or services

Theft and embezzlement

- Theft of medications, equipment, and other supplies for personal use or re-sale
- Embezzlement of funds for personal use

Personnal

- Absenteeism
- Informal payments: under-the-table payments in exchange for special privileges or treatment
- Abuse of hospital resources (cars, telephones, etc.)
- Favoritism when choosing suppliers
- Use of a position or title to sell accreditation, certification, etc.

Payment system

- Insurance fraud, by over-charging, submitting invoices several times or false invoices
- Invoicing for "ghost" patients
- Paid referral arrangements between doctors and hospitals (commissions or kickbacks)
- Performing unnecessary medical interventions in order to maximize fees charged

The categories are particularly well defined and relatively universal, so in this sense will be easy to use. However the difficulty lies in creating regulations that can be complied with and implemented by the healthcare sector as a whole.

## Conclusion

>> Fraud, abuse and errors are not just an issue for one specific healthcare system.

They occur **everywhere and regardless of:**

- the share of public and private funding
- the levels of technology
- the type of culture (Mediterranean, Anglo-Saxon, European and others)
- the amounts of money involved

Fraud levels are similar from one country to another, and typically relate to:

- Unauthorized payments (for services, equipment, medication), in order to embezzle money
- Unjustified access to services (treatments, medical transport or taxis, medication, etc.), which also affects the financial balance of the system

**All areas seem to be affected,** from general practitioners to hospitals, prescription filling to spa treatments, to dental care and more.

**Anyone can be involved** (industrial organizations, patients, healthcare professionals, criminal organizations, etc.), and sometimes several parties collude. This means fraud mechanisms are becoming more complex, and that detecting fraud requires forms of collaboration that can be difficult to establish (fraud investigators, law enforcement officers and lawmakers).

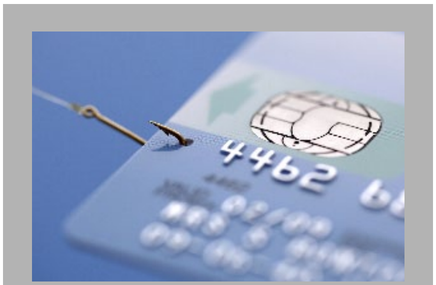
Even if healthcare professionals are sometimes involved, administrative procedures relating to healthcare claims processing are inadequate, in terms of **data integrity, patient identity, entitlement authorizations and more.**

Furthermore, in the banking sector, which the smart card industry has worked with for 30 years, the transition to paperless, digital administrative procedures has led to a **shift in fraud by isolated individuals to organized groups.**

Finally, trends highlighted by the FBI in 2010 in the United States—**deliberately endangering patients** for financial gain, and an **increase in identity theft**—should be tackled with all necessary and appropriate measures.

# Chapter 4:
# Best practices in the fight against fraud

## A very effective banking sector



Among the best practices identified, the banking sector is particularly effective in fighting fraud.

In the 1970s, banking was one of the very first sectors to make the big leap in adopting paperless transactions, starting with Diners Club then Bank of America cards, ultimately leading to an impact on the use of checks. At the time, magnetic stripe card technology enabled speedy deployment, but also led to an increase in fraud. Since the 1990s, banks have implemented technology based on microchip cards, incorporating anti-fraud features such as PINs or encryption.

Fraud was tackled with some force and success in this sector. Banking fraud and healthcare fraud share some comparable characteristics (computerization, financial amounts, etc.). For example, GIE CB estimated (the figure is close to the actual amount of fraud) that the fraud rate in the banking sector in France was 0.072%, for financial amounts around 3.5 times higher than those involved in healthcare claims processing. If we compare this with the estimated 5.6% for fraud and abuse alone in the healthcare sector (EHFCN estimate), a rate 70 times higher, then we get an idea of the progress that still needs to be made.

It should be noted that in France, banking fraud (cards) was 20 times higher before the mass adoption of microchip cards with anti-fraud features and electronic transactions. Even if the validity of comparing the two sectors is open to discussion, in France (banking system with GIE CB and healthcare system with SESAM-Vitale), there are a certain number of similarities.

| 2009 Figures | GIE CB | SESAM-Vitale | Comments |
|---|---|---|---|
| Cardholders | 58 million | 50 million + | |
| Total value of transactions | 597 billion | 175 billion* | *Consumption of medical care and materials in 2009 (INSEE-French National Institute of Statistics and Economic Studies) |
| Number of electronic transactions | 3,5 billion electronic authorizations | 1 billion electronic claim forms | 1 billion paperless electronic claim forms, or 80% of the total in 2009 (85% in 2010) |
| Number of transactions by card/year | 113 | 20 | |
| Fraud percentage of total amount | 0,072%* | 5,6%** | *Source: GIE CB<br>** EHFCN average |
| Number of professionals with equipment | 1.134.000 retailers | 240.000 healthcare professionals | |
| Geographic source of fraud | 40% outside France<br>60% in France | Not available | |
| Internet fraud | 75% of all fraud* | Not applicable | * Using only a CVV2 code – so no Chip and PIN |
| Card-present fraud | 25% of fraud is in face-to-face payments* | Not available (no PIN) | *Presence of the payer, use of the PIN |

>> It would be reasonable to wonder why two systems using microchip card technology have such different fraud rates. The answer lies in the different uses assigned to cards.

Banking cards need to offer as much security as possible for customers, retailers and banking institutions. They therefore include anti-fraud features such as the verification of data stored in the chip by the issuing bank, card authentication by the payment terminal, card authentication by the authorization server, credit limit management, risk management or even authentication of the cardholder with a PIN.

The health insurance card was not designed with these features. It only stores the information that can be read on the front of the card, and is not protected by a security mechanism. This is due to the goals of the SESAM-Vitale program: making claim form processing paperless, by implementing electronic links between healthcare professionals and organizations providing mandatory or additional health insurance.

In the United Kingdom, €410 million in 2010 was lost to banking card fraud (The UKCARDS Association), while an estimated €8.5 billion was lost to fraud in the healthcare sector, according to an EHFCN estimate—a figure 21 times higher.

In the United States, on average, fraud was handled within 21 hours in 2009, and half of all victims report it. The number of arrests has therefore doubled, and the number of cases prosecuted has tripled (Source: Javelin Strategy & Research, «Identity Fraud Survey Report», February 2010).

## Six lessons from the banking sector

Six lessons can be learnt from the banking sector to establish general guidelines:

> Specialist fraud personnel need to be provided with a considerable amount of training to master IT tools and become analysis experts.
> Fraud is not a problem linked to competition. All entities can collaborate and standardize data structures.
> Stricter identity controls and a more aggressive stance with regard to identity theft have markedly reduced banking fraud.
> The involvement of consumers is a key factor for success.
> Credit card authentication is a model for personal medical files.
> 95% of data loss is unintentional, so errors are actually of more importance than fraud.

Accenture carried out a study in 2011 on the parallels between the banking and healthcare sectors
http://www.ehfcn.org/media/documents/Heather-Adams.pdf

# The United States has been fighting healthcare fraud for 15 years

>> The United States began to combat healthcare fraud long before Europe. They have achieved concrete results.

The five main reasons are due to:

- the large amounts of money involved in healthcare (currently $2,340 billion, so 17% of GDP)
- the large amounts lost to fraud (between $75 billion and $250 billion according to the FBI)
- a great deal of action-focused pragmatism
- the presence of a powerful IT industry (availability of equipment, software, systems, skills)
- a privacy protection system which allows for a certain amount of leeway where national interests are concerned (to establish databases, for instance)

To illustrate this, here are some examples of the measures taken and the end results.

In 2010, the Obama administration increased its budget to fight healthcare fraud by 50% to $320 million. The results achieved are impressive (information from the 2010 report on healthcare fraud by the Department of Health and Human Services and the Department of Justice, released on January 24, 2011). More than $4 billion was recovered in 2010—a record amount.

The annual report outlines the number of cases brought to court, and also highlights the collaboration between the Department of Health and Human Services, the Department of Justice and the FBI to create the Medicare Fraud Strike Force, in particular in Baton Rouge, Brooklyn, Chicago, Dallas, Detroit, Houston, Los Angeles and Tampa. The communications plan to promote the fight against healthcare fraud also includes a number of conferences organized by the Department of Health and Human Services and the Department of Justice on the challenges and measures taken to eradicate fraud, in particular with the new legal tools provided by the Affordable Care Act. The "Patient Protection and Affordable Care Act", voted in by Congress and promulgated by Barack Obama on March 30, 2010, marks the first stage of reform of healthcare in the United States.

In 2011, the 14th year of anti-fraud measures, the program requested a budget of $266 million and was awarded an additional amount of $311 million by Congress. The return on investment of the program since 1997 is $4.90 recovered for every dollar spent. The average from 2008 to 2010 even increased to $6.80 for every dollar spent.

The August 31, 2011 edition of USA Today ("Feds go after health fraud") announced that 2011 would almost certainly be a record year. 903 cases have already been brought to court, compared with 731 for the whole of 2010. More than $4.9 billion will have been recovered (compared to $4 billion in 2010). In February, the government set up two new healthcare anti-fraud units. This biggest ever case of mass healthcare fraud was uncovered this year. No fewer than 111 people (hospital managers, doctors and nurses) have been charged with embezzling $225 million—an unprecedented amount. Anti-fraud specialists rely on data from the country's Medicare and Medicaid service center databases.

But this is not down to chance. With nearly 15 years' experience, the maturity of methods and teams is boosting the performance of this organization. The country's federal system of government has also generated strong overall support for the initiative.

The report dated 29 July 2011 on actions taken to protect the Medicare Program against payment errors, fraud and abuse (Medicare Program Integrity: Activities to Protect Medicare from Payment Errors, Fraud and Abuse) summarizes the programs implemented, sources of funding and the interest of the U.S. Congress in effectively protecting this system. The program is in itself impressive representing $ 523 billion in 2011 for a total 47.5 million beneficiaries. The estimated rate of fraud is again discussed. A range of 3 to 10% of total spending is put forward.

Two issues in particular stand out in the report:

- Medicare reimburse within thirty days of receipt of claim forms, which is faster than private health insurance. With such a short processing time, it is difficult to verify abusive or fraudulent payments.

- Recovery officers or «Recovery Audit Contractors» working for private companies, have the task of identifying undue payments and recovering improperly paid out funds without being required to identify the nature of the fraud. Feared by doctors and hospital staff alike, they are considered aggressive in their investigations. They are paid a percentage of amounts recovered. The appointment of these officers is one of the actions instigated under the Tax Relief and Health Care Act of 2006 and is mandatory in all states since the end of 2010.

Finally the report describes progress made to date in anti-fraud and anti-waste activities. Note that in twelve months, there have been thirteen presentations to congress on fraud in the Medicare system.

In this context it is interesting to note that a bill was introduced in Congress on September 14, 2011 by representatives of the Democratic and Republican parties to propose the use of smart ID cards for Medicare patients and providers.

Finally, continuing to ramp up enforcement efforts—which federal authorities must above all ensure are efficient—at a time when national spending is being called into question gives added clout to anti-fraud teams and increases their chance of success.

## New legal frameworks in Europe

### France

>> In France, as for most European countries with large budgets for reimbursing healthcare, the fight against fraud began in practice in 2005, specifically with the social security finance act (Programmation de la Loi de Financement de la sécurité sociale, or PLFSS).
This act was to be ratified in 2008 with the Lisbon Treaty, which defines the main principles for the European-level anti-fraud framework. In France, the creation of the center for European and international social security coordination (Centre des Liaisons Européennes et Internationales de Sécurité Sociale, or CLEISS) is a result of this. The center was set up to collaborate with other European countries and cross-reference data, in particular to target fraud.

> “Only halfway through the years 2000 did politicians, governments and top-level administration start to realize the significance of healthcare fraud» (Le Figaro, April 2011).

As of 2005, the legislature began to require the French Court of Audit (Cour des Comptes) to validate the reports from social organizations, which manage more than €300 billion, and whose accounts should be “accurate and in good faith”. In 2008, a national anti-fraud delegation (Délégation National de Lutte Contre la Fraude, or DLNF) was set up at the Ministry of Finance. At the same time, the Court of Audit started to assess the rate of benefit fraud.

But the legal arsenal has received considerable reinforcements over the last five years. The CNAF has cross-referenced its files with central income tax records for the last 10 years, and can now ask other social organizations, utility companies (EDF, GDF-Suez, etc.) and especially banks for the personal data of beneficiaries.

The Court of Audit has drawn up a report on the measures taken from 2005 to 2010 to fight benefit fraud in general.

**France now has heavier sanctions for persistent abuse and attempted fraud, as well as rights of access to information and simpler procedures. But, as the Court of Audit report highlighted, much progress must be made to establish a more perfect legal system.**

The health insurance law of August 13, 2004, had already increased the ability of the Primary Health Insurance Fund (Caisse Primaire d’Assurance Maladie, or CPAM) to detect fraud and impose sanctions. But the legal means available to local funds have above all been increased thanks to subsequent universal healthcare funding laws.

The conventional sanction for fraud is still a fine. But various other measures have been taken. For healthcare, the 2004 law set out a range of sanctions (notifications, warnings, prior agreements, financial penalties) to punish fraudsters, but also to sanction persistent abuse (the two concepts had thus far not been distinguished for repeated punishable offenses). The 2009 funding law made prior procedures more flexible, and increased the range of sanctions that could be imposed.

Information access rights were extended by the law of August 6, 2004, amending the law of January 6, 1978, on data processing, data files and individual liberties.

But, as highlighted in the Court of Audit report, much progress must be made. One need only peruse the 2010 PLFSS to realize this (Section 7, Articles 50 to 54 – Measures relating to fighting and controlling fraud).

For an outside observer, sanctioning attempts would seem an obvious measure and the maximum sanctions could seem paltry and assessing levels of activity an obvious way to calculate sanctions.

An outside observer could also consider this to be yet another issue to allow the problem to be put on the backburner indefinitely. It shows the difficulty inherent in implementing a catchall legal system for fraud in the healthcare and social protection sector.

For the additional measures put forward in 2010 to strengthen inspections in amendment of the law of 2006, since each proposal has to be covered by a decree, it will take around six to ten years before any of the measures are actually implemented.

In short, France is lagging behind in terms of implementing legal and judicial systems, although these will need around a decade to bed in and become fully operational. In the United Kingdom, progress in the fight against fraud is also recent, as we have already seen. But France, the United Kingdom and Germany have tremendous healthcare budgets.

In France, the use of Vitale cards has in particular made it possible to create homogenous databases, since there are no input errors with automatically recorded and exchanged electronic data. The Vitale program—with its standardized processes and procedure classification system—has also played a major part in improving the overall quality of the system. A posteriori targeting of fraud and abuse is made much easier by this consistency across France as a whole.

### Slovenia

Let us now look at Slovenia, where the amounts involved reflect its population of 2 million inhabitants.

Our contact explained that in Slovenia the fight against fraud is based on a relatively recent system, and a true reflection of its performance will only be seen in five years at the earliest. Slovenians have nevertheless understood that legal systems need to be adapted and improved on a continual basis.

The fight against fraud is part of more widespread reform and changes to the healthcare system in the country. Budgetary constraints are particularly important, due to the cumulative effect of an aging population, unemployment (8.4% in 2011 according to Eurostat), budgetary constraints linked to the management of public debt, heavy costs for chronic diseases, next-generation medical equipment needs and demand for better services for patients and insured parties («patient-centric»). Social protection laws (health and health insurance) mainly define people's rights to healthcare coverage.

> "I realize how difficult it currently is for large countries to implement an appropriate legal framework, and the best approach to systematically fight fraud. Slovenia has an advantage since it is a small country. But our capacity to quickly get to grips with this problem does not exempt us from an obligatory learning period. The sheer scale of the task means there can be no overnight revolution in Slovenia. Nevertheless, the successes in the fight against fraud should be widely communicated. The amounts recovered and saved provide an obvious, considerable «political return on investment», at a time when Slovenia's solidarity-based social model is under pressure. I think the components are present to create a virtuous anti-fraud circle." says our contact.

### Europe

Best legal practices in European countries range between two extremes.

> "Old" countries in terms of a legal framework, such as France, which has proved its effectiveness by recovering considerable amounts (EHFCN 2009/2010 Annual Report) but has taken 10 years to start to provide considerable returns, in particular because of the process of laws and decrees.

> "New" and more flexible countries such as Slovenia and the Baltic countries, which should perform admirably in five years' time.

Finally, laws must continually be updated, to improve and adapt to the new challenges in the fight against fraud.
For the 27 EU Member States, this process must be based on European legal foundations.

The legal system is a mandatory requirement, but not sufficient in itself for the technical solutions implemented to produce good results. Each nascent program or measure must therefore advance at its own rate. Fortunately, these foundations do not have to be fully completed before implementing technical and organizational solutions. Furthermore, we can learn a lot from the United States in terms of the best technical practices, thanks to its past measures in these areas.

## A recent and difficult start for all

>> The 2011-2013 National Anti-Fraud Plan in France clearly shows that this approach and its progressive organization are still relatively recent.

**Learning and organizing:** there is a need for regional, national and international multidisciplinary coordination and exchanges.

**Assessing and being assessed:** international benchmarks such as the one carried out in 2010 on fraud in OECD countries (Canada, United States, Spain, Belgium, United Kingdom, Italy, the Netherlands) show that frames of reference are being sought, and highlight the need to share experience.

**Raising awareness, training:** initial and continuous training, to educate and set targets for everyone.

**Exploiting data:** Finally, the “data mining experiment» and the “increased” access to digital data and communications reveal the low use of IT tools at present.

Another manifestation of the recent priority assigned to the fight against fraud can be seen in its inclusion in management and objective agreements between the state and universal healthcare authorities. But the Court of Audit believes they are “insufficient» and “not catalysts for change”.

According to the Court of Audit, tools to provide guidance in choosing the most efficient internal organization or procedures are often lacking. Best practices are not identified, and cannot therefore be systematically disseminated in the network.

For example, nearly 300,000 home inspections are carried out in France every year by CAF inspectors, without a written procedure covering the preparation, completion and write-up of these inspections.

Furthermore, organizations have no information relating to prior acts of fraud committed. Someone could have been found guilty of fraud, even given a criminal sentence by a regional organization, and still commit this same fraud in a region under the jurisdiction of a different body, without current information systems picking it up.

The fight against fraud therefore needs to be a systemic approach, and not just focused on the deployment of tools. This means that personnel need to be given precise goals, provided with the proper documentation and properly trained, and in particular must report their experiences in order to improve procedures.

Slovenia took the opportunity of the recent modernization of its healthcare system (2010 Healthcare Plan) to implement tools and an organization well suited to the fight against fraud.

According to our contact:
«First of all, fraud inspections are standard procedures in our healthcare IT system. This system is very new, and needs more time to produce results. We estimate that it will take two to five years for it to reach a satisfactory level. Partnership contracts are the second tool. They define performance, measurement tools and auditing rules. Audits themselves are first of all internal, then external (Medical Chamber of Slovenia) and administrative (Department of Health), if healthcare system rules are violated.

“Finally, the microchip healthcare card—which all Slovenians possess—is a very effective way of identifying and checking validations. It is the key to confirming a patient’s eligibility, and answers the question of who is paying, for whom and for what. That is why we pay particular attention to issuing procedures for the card, and regularly check entitlements linked to it.

“There remains a lot of work to be done in terms of taking administrative data and medical data into account, and we still need to invest in this area, to the delight of hospital personnel, against strong resistance from doctors.»

Slovenia has integrated EHFCN’s working groups, in particular to address the issue of cross-border fraud.

The example of Slovenia shows that the fight against fraud is fully integrated into an approach that is systemic (national contracts with healthcare professionals, university hospitals and manufacturers, integration of anti-fraud tools in the design of a global system, etc.), collaborative (EHFCN membership, collaboration with crime-fighting services, involvement of specialists in decision-making bodies, etc.). In two to four years’ time Slovenia will be a breeding ground for good practices in the fight against fraud.

## Tools

>> Apart from the quality of source data and detection performance, a comprehensive approach allows changes to be anticipated in advance, for fraud to be tackled before it even arises. The comparison with the banking industry is especially relevant here. A bank can cancel a credit card following an «attempt» at fraud, and warn its customer before the fraud even takes place. Just as in the banking sector, this would mean that a new card would have to be available in under a week.

The SAS Institute group, one of the first suppliers of data analysis tools, helps us to understand the power or the new tools available.

The benefits of fighting fraud only became apparent in the 1980s, when contributions in the United States increased markedly. The creation of the National Health Care Anti-Fraud Association was initially created because of the need to share information and raise awareness of this risk.

The 1990s, with the automation of procedures and healthcare claim forms, paved the way for considerable opportunities for fraud, with little chance of being caught. The initial response was to implement a raft of anti-fraud and technical measures, with the tentative arrival of analysis and information systems after 2000.

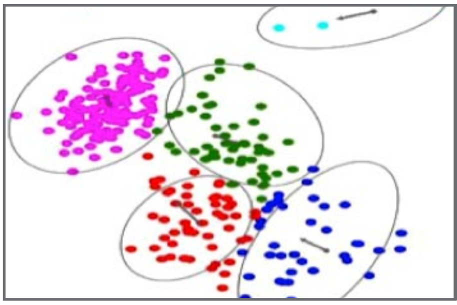
At present, the new systems enable fraud to be detected, but also prevented.

To detect fraud, systems capable of consolidating a very large amount of data (organized or not) are required.
The quality of input data is therefore essential for detections.

Predictive models compare claims with baselines or limits to draw up statistical limits, above which fraud is likely. Social models enable the links between suspect claims to be visualized, as well as expose the networks of organized groups. These tools can also flag suspicious behavior.

Finally, a key element for solving these issues, investigation uses technical systems that can manage the entire lifecycle of an investigation, prepare the case in the event of criminal procedures, and follow up investigations after cases are closed, while ensuring that each step can be traced back. Another key player in data analysis, the European software developer SAP has implemented these types of tools for AOK in Germany (National health insurance for private sector employees, with 25 million members), Centrelink in Australia (governmental universal healthcare agency), the AEAT in Spain (Spanish national tax administration), and the renowned American NCIS (Naval Criminal Investigation Service).

But SAS Institute and SAP both agree that the fight against fraud will continue on a permanent basis. Fraud is particularly adaptable and mobile, and fraudsters are inventive.

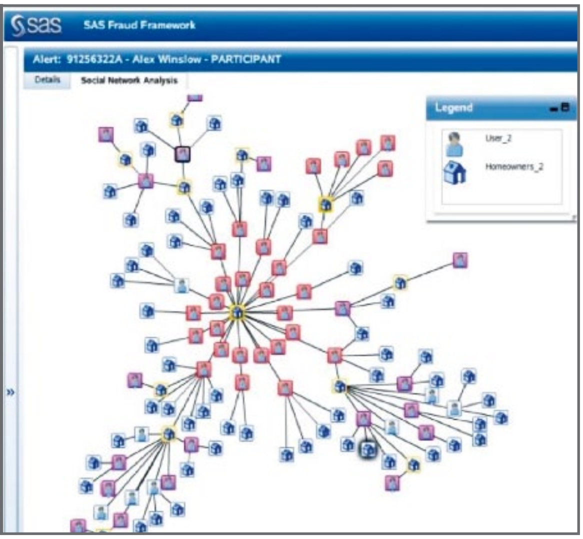


**Example of anomaly detection through graphical representation of data thresholds, pictured here at the center of the ellipses. Data theft, suspicious healthcare record activity for individual patients, prescription fraud, suspicious claims, unusually high numbers of specific treatments and more can be plotted. Source: SAS Institute**

## Data

These monitoring tools will only produce the best results when fully qualified, comprehensive data is used, with sufficient statistical data, with the knowledge that all this would depend on the effective application of collaborative procedures. Nevertheless, these tools will hopefully prove to be effective in the very near future.

**This model plots claims processing anomaly and neighborhood data (source: SAS Institute) in the aim of at identifying potential fraud organized with the help of neighbors or family members.**



## What can be expected from a systemic approach?

>> Even if the approach is systemic, and therefore slow to implement, and recent, especially in Europe, there are concrete results published by the EHFCN, and a report by FORE in the United States from 2005 showing the expected results in four stages, over a 20-year period.

The approach developed by FORE, which has the advantage of being a real research center, with a sizeable database, is to put forward an economic model using high-quality patient data, and providing a return on investment, from the start year through to the establishment of a system performing well in the fight against fraud, through four main cycles which are sufficiently explicit for each country to be able to ascertain their current situation and the steps they need to take (Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities, FORE, September 2005).

The second point of interest is that the FORE report is based on 2001 data. It is interesting to note that in 2011, healthcare spending in the United States was around $1,400 billion, and it was estimated that $1.7 billion of this was lost to fraud, so a rate of 0.12%. This is remarkably similar to French figures for 2010, with the same rate of fraud (0.11%). Furthermore, from 1995-1996 in the United States, and towards 2005 for Europe, the fight against fraud has been organized.These simulations are therefore of interest for the large European countries, and that the results of this report could usefully be extrapolated.

Details of the report can be found in Appendix 1. The study highlights three aspects of the fight against fraud, abuse and errors:

- Productivity gains from the systematic fight against errors are five times higher than those from the fight against fraud.
- Sharing data, in particular personal medical files, is a powerful tool in the fight against fraud and errors.
- Long-term investment will be needed to see the gains from information technology.

>> The implementation of a paperless medical file will provide much greater economic gains for administrative activities thanks to the quality of data.

Using Electronic Health Records is a best practice, since it promotes an essential component of any system: the quality and availability of data. That being said, there are other initiatives which could be implemented alongside this, or independently, which can be classified in two main groups: fraud anticipation and detection tools, particularly in database networking, data mining tools, strong authentication solutions (such as microchip cards) and predictive models. The second group should not be disregarded, and includes human resources and skills, in particular

## Recommandations

>> The progress that has been made should not detract from the fact that there remains much to be done in all countries, in terms of regulations, organization, cooperation, training, setting targets, measures, audits, and even communicating with the general public. Readers can consult the long list of measures and recommendations set out by countries (French Court of Audit) and transnational organizations (EHFCN).

### The quality of the data gathered is a priority

The American foundation FORE places particular emphasis on the technological investment and data collecting methods required, which form the basis for all high-quality analyses and detection. FORE underscores the need to provide solutions for data integrity, ensuring it is consistent, available and secure. It stresses the need to reliably identify and authenticate those involved and make them liable through non-repudiation in order to establish a secure digital network, including certification, electronic signatures and a public key infrastructure (PKI), through implementation of a microchip card type system. FORE stresses that these components are essential for implementing electronic personal medical files.

## Conclusion

>> **The best practices in the fight against fraud can be found in a comprehensive approach;** all components (legal, technical, organizational, etc.) must make progress at the same rate. Because the ways in which fraud is committed is continually shifting, it must be tackled on an ongoing basis using the appropriate means.

Even if this overall approach takes time and is initially difficult and costly, it provides a considerable return on investment. Implementing a consistent, shared information system in particular helps to **reduce the amount of errors more than reducing fraud,** by creating a virtuous circle of efficiency, accountability and transparency. The United States' experiences and the successes of the banking sector should serve as a guide, even if adopting some concepts should be subject to in-depth analysis first.

We will therefore conclude with the seven general summary recommendations set out for the Obama administration by FORE this year:

> Information sharing must be promoted.
> Real-time data consolidation and analysis are the spearhead measures to be taken for detection and prevention.
> Prepayment checks and audits need to increase considerably.
> Private and public organizations must protect insured parties, and suspend or reject fraudulent claimants.
> Healthcare professionals who commit fraud must be sanctioned by suspending their medical license.
> Everyone's identity must be better protected.
> Investment in innovation aimed at combating fraud (prevention, analysis, processing, etc.) must be maintained.

**"The results are still not sufficient, and we only recover a fraction of the amounts stolen… Legal, financial and technological resources must back up the government's strong commitment." FORE, 2011**

# Chapter 5: Recommendations for implementation

## Fighting fraud by design

>> Information technologies must be regarded as essential and indispensable for improving healthcare information systems. They are powerful tools to achieve potentially considerable results in the fight against fraud and abuse, as well as in the elimination of errors.

The quality of data entered automatically at the source, the protection of data confidentiality and the identification of claimants (as well as the protection of entitlements) are issues in all healthcare systems. It is therefore not surprising that microchip card technology has been included in the deployment of most universal healthcare and private healthcare programs over the last 20 years.

Eurosmart will set out nine recommendations regarding the use of this technology. They have been drafted following discussions with our customers and feedback from our project teams.

Although microchip cards for healthcare professionals and claimants enable identification, paperless procedures, and the creation of secure digital networks, they only serve as a means to facilitate organizational change.

Healthcare systems that are designed to expedite the transition to paperless procedures (in particular using electronic claim forms) usually achieve this goal. Systems that have not been designed in this way—or have not taken into account the fight against fraud—tend to produce disappointing results, which are of course difficult to assess in this area.

Microchip cards are therefore powerful catalysts for projects with the specific goal of fighting fraud, and which implement the resources needed to obtain the most from this technology. In this respect, the fight against fraud is driven by human endeavor in the design of healthcare systems, rather than by the technology itself.

In each of our healthcare projects, the effects of “card” technology are completely dependent on organizations’ ability and intent to use it. This technology can boost system capacity, produce impressive results and overhaul practices.

**In 2010, more than 1 billion electronic claims were processed in total in France (85% of all claims), saving around three billion sheets of paper.**

**“In France, for example, people have been using the Vitale card since 1998, and there are 67% fewer administrative personnel in French healthcare facilities than in American facilities.” Newsweek, February 2010**

**In that sense, the French program achieved its goals.**

### IT systems have incorporated anti-fraud measures since the 2000s

The first decade of the 21st century has been a transitional period. Before this period, the only example of the implementation of automated systems was in making procedures paperless to increase administrative productivity, or to set up collaborative tools (claim forms and/or prescriptions/medical data, etc.). The fight against fraud has been included in all new systems implemented after the turn of the century. Slovenia has been at the forefront of this change. It began to invest in e-Healthcare 20 years ago, and now has one of the most advanced healthcare systems in the world.

The “e-Health 2010” strategic plan in place at present is the second generation of the system launched at the start of the 2000s. It provides a nationwide network of information systems, ensuring that transparent information and electronic services are provided to all stakeholders, in a secure and efficient manner.

>> Slovenia was one of the first countries in Europe to introduce microchip healthcare cards. Launched in 1996, the Slovenian healthcare card program was deployed nationwide during the summer of the year 2000. ZZZS, the Slovenian national health insurance organization, in charge of the national system of health insurance cards, is systems integrator for the program, and supplies the cards to citizens. The entire solution is compatible with existing infrastructures.

Today, the country is in the process of renewing and updating the 2 million electronic health insurance cards already in circulation within its borders. By rolling out next-generation eHealth solutions, Slovenia is improving online services for healthcare professionals, helping them to complete their administrative tasks more swiftly and exchange medical information and communicate with hospitals and other healthcare professionals in a simple, secure way.

> This approach enables the inclusion of all healthcare fields and a comprehensive view of patient health, with interaction between all sub-records, and better prevention of iatrogenesis.
> It provides a better statistical or even epidemiological overview, and better-substantiated tools for decision-making and the establishment of general approaches.
> It also improves fraud verification and prevention efficiency, with new integrated mechanisms and improved identification and analysis tools.

The issue of benefits verification, for instance, was resolved with a simple mechanism in the microchip cards: expiration date management. The following rules were implemented: cards are valid for three months for students and foreigners, a year for private-sector employees, and three years for retirees and public-sector employees.

Cardholders must renew their card (mainly through pharmacies) before the expiration date, to be able to continue using it. Entitlements therefore have expiration dates, within limits acceptable for all.

>> Similarly, Algeria completely overhauled its healthcare system, which was based on the French model, between 2006 and 2007, before deploying the new system between 2009 and 2011. Algeria was able to draw from the experience of European countries and integrate new mechanisms into this system, in particular to curb the repeated abusive use of cards, and the exceeding of card limits.

Algeria used the same concepts as Slovenia, but also included additional components:
> A counter to keep track of card expenditures and block the card in the event of the card limit being exceeded.
> A counter to keep track of transactions, verify the use of the card and prevent it from being used for fraud.

In this way, the card of a patient who visits their doctor for the fourth time in a week will be blocked, making it impossible for the transaction to be processed. The counter can be unblocked by providing a satisfactory explanation during a prior visit to a doctor certified by the Algerian universal healthcare fund (Caisse Nationale d'Assurances Sociales des travailleurs salaries, or CNAS).

For these latest deployments, at the end of the 2000s, identification issues became a major problem, in particular for countries implementing health insurance systems for the first time. This is the case for Mauritania in 2007, Gabon in 2008, and Mali in 2011. Other countries will soon launch systems: Senegal, Burkina Faso, Benin and Ivory Coast.

**Since 2009, the new Algerian electronic healthcare system (CHIFA) is used in all of the country's 48 districts. More than 5,500,000 CHIFA cards have been issued. More than 13,500 practitioners are identified using tokens (USB dongles equipped with microprocessors). The country has learned from the past experiences of European countries, and included restrictions, especially for exceeded card limits, and the repeated abusive use of cards in the new system.**

>> For Gabon in particular, it was clear in 2008 that all resources should be implemented to avoid the health insurance program becoming a magnet for the citizens of neighboring countries, and to ensure that the generosity of the program would not lead to its collapse, due to the abuse of entitlements.

Beneficiaries must therefore be individually identified so that only they can access the care they are entitled to. It was decided each claimant in Gabon would receive a non-transferrable, individual health insurance number, with entitlements recorded on a biometric microchip card. So Gabon implemented a strong cardholder authentication system, based on fingerprints. Patients must present their card and identify themselves with a fingerprint to access third-party payments when visiting healthcare professionals.

No central database for fingerprints is required, since data is checked offline by the processor of the microchip card itself, which compares the fingerprint in its system with the one the fingerprint reader registers for the patient in the room.

Finally, large countries that began to implement paperless claims processing first are now either replacing their systems or redesigning them.

In 2011, Germany began to deploy a new healthcare card system, taking into account the fight against fraud, with mechanisms to check patient entitlements online, strong cryptographic systems to authenticate cardholders, etc.

The French National Assembly has just completed its report on the fight against social fraud, and its recommendations will certainly have consequences for the current system.

## Nine recommendations based on Eurosmart's experience

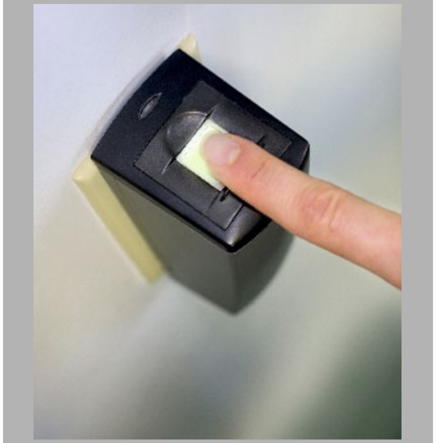
### 1 - Take stock of feedback from existing systems and stakeholders

France has a good long-term database structure, thanks to the use of the Vitale card. This can be seen in the amounts recovered by the French health insurance fund (Caisse Nationale d'Assurance Maladie, or CNAM) since 2007. Only a posteriori checks could be verified, since data accuracy was the key to conducting investigations.

In place for more than 10 years, the Slovenian system is still considered in its infancy by the Slovenian authorities. However, following its implementation, progress has been made in the fight against fraud.

In Algeria, the system put a stop to organized fraud involving patients and healthcare professionals, thanks to restrictions linked to the spending counter, whose results were compared with spending limits.

In Gabon, the system is still in the trial stages, but the use or card/fingerprint equipment guarantees the identity of the person covered by universal health insurance.



### 2 - Set up a central body to manage the system as a whole

Projects that succeeded in deploying their system quickly and efficiently were managed in this way. Slovenia has the ZZZS and Algeria has the CNAS—specific departments to implement solutions from end to end. This type of integrated project team, which defines specifications and deployment procedures, is not in place in larger countries such as France or Germany, which have several organizations in charge of sub-systems of the overall system.

This “overall system» organization is in charge of the definition (legal, technical and procedural), implementation, results and budgets of the system.

### 3 - Adopt paperless procedures that enable more structured administrative and medical data for consistent data quality through smart card usage

The greatest ally in the fight against errors and fraud is consistent administrative and medical data entry, which should be automated wherever possible.

In order to be useful and relevant, data stored in electronic healthcare records must be structured, as well as use consistent medical terminology and semantics. To be practical, data must be easy to access for users.

It should be noted that France has the best information and database for medical procedures, thanks to over 85% of claim forms in 2011 being electronic. This has led to sound knowledge of administrative data, thus enabling excellent a posteriori checks.

The SESAM-Vitale system has other virtues, such as the classification of healthcare procedures and illnesses, which has helped adapt the heath insurance information system for medical purposes, a requirement to be able to calculate reimbursements not just based on administrative invoicing data, but based on the care and procedures prescribed.

## 4 - Implement microchip card technology to make a priori checks simple and efficient

Technology should be used in applications for which it is particularly effective, to integrate checks for:

- The nature of care
- The validity of entitlements
- Cardholder authentication
- Maximum amounts (for transactions, frequency, in total, etc.)
- The number of transactions per month

In a “patient-centric” approach, these checks can be balanced out by sending insured parties information by SMS or email. It may also be a good idea to inform users when their card is used (“Your card has just been used”). Another good practice borrowed from the banking sector, for international payments, for instance.

Innovation can probably be achieved by focusing on customer relations, and rethinking the relationship between social insurance organizations and insured parties. The “contractual” and “responsible” side of the approach can be highlighted, in a balance that is perfectly in tune with the original spirit of rights and responsibilities in the founding social contract.

## 5 - Rather than make healthcare professionals enforce regulations, delegate this task to card technology

It will be much easier and more comfortable for healthcare professionals to delegate this task to an electronic device (Algeria: the transaction counter blocks the card after the fourth visit in a week).

Another example is if electronic parameters flag a risk of fraud, then the transaction is canceled, and the patient and/or healthcare professional must have recourse to a back-up procedure. This back-up procedure also needs to be secure, but both parties must also make particular efforts to “curb” potential fraud.

## 6 - Implement back-up procedures (hard copies), ensuring that they are highly secure

When a back-up procedure is required (lack of card, network, etc.), other proven practices can be used. Inspiration can again be found in the banking sector, with practices including paper and forms produced by certified organizations that integrate technology such as incremental numbering, holograms, watermarks, etc.

New secure cryptographic barcodes, which can be used in particular for electronic prescriptions, and read when documents are printed by pharmacy equipment (the same applies to reading barcodes on medication), are also simple ways to check for fraud, abuse and errors when filling prescriptions (multiple use of prescriptions, forgery of prescriptions with added information, etc.).

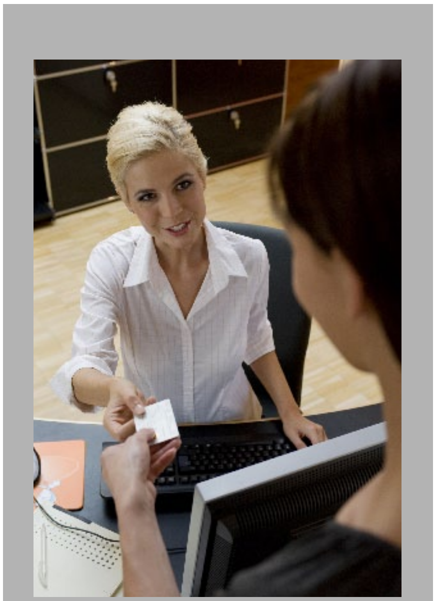
## 7 - Ensure that the entire system is highly secure

As in any system, the security of a healthcare system is only as strong as its weakest links. It is therefore important to set up an overall system without security flaws (procedures, communications). At a technical level, only products certified according to international standards (shared criteria) should be implemented.

## 8 - Validate the identities of patients and professionals using a secure face-to-face registration process

When analyzing the systems implemented by our customers, we found that strong identification measures are essential to determine who is paying, for whom, and for what. Identification is essential to streamlining healthcare spending, for checks and, above all, to ensure the universal healthcare system itself can be maintained over the long term. “It would be illusory to think that the supply of services could remain anonymous,” one of our interviewees noted.

This identification, due to the healthcare coverage entitlements linked to it, highlights the importance of upstream processes, in particular the quality of registration procedures and identification data (documents). In all cases, Eurosmart recommends secure “face-to-face” registration, and the presentation of proof of identity to ensure that the right person receives the card.



Finally, electronic registration/delivery procedures for personal documents—such as those in place for passports in many countries—could be coordinated.

Of course, the duplication of technology and procedures to check and manage identities should be avoided for nationwide projects such as electronic identity cards, passports, driver’s licenses, residency cards, etc.

## 9 - Leverage the experience of key industry players

To succeed in such a challenging but achievable goal, government agencies and health insurance organizations should liaise with global technology partners able to integrate the power of IT and smart card technologies in particular to fight fraud.

It is important they engage partners and suppliers with long-standing experience and global footprint in digital security, strong identification, authentication and biometrics.

Suppliers involved in eHealth programs but also national eID programs can better anticipate enrolment, issuance, post-issuance and electronic verification issues and opportunities in federating national resources. As they participate in the definition of the specifications, security proofs and compliancy requirements, they can offer strict compliancy with standards and specifications that form the basis for global interoperability.

Previous experience, especially a proven track-record in eHealthcare but also in identification, will ensure higher efficiency in fighting fraud characterized by best practice sharing.

Suppliers with experience in eGovernment will also enable its clients to integrate with other national eGovernment initiatives seamlessly.

# Conclusion

>> Using cards speeds up the transition to paperless, electronic procedures and data exchanges, which are also formidable catalysts for the modernization of systems. In terms of administration, the results obtained are impressive.

**Yet this technology is often under-used** at present, in areas where it will produce excellent results.

- **Strong identification and authentication** for patients and healthcare professionals are key features of microchip cards, and should be implemented in the healthcare sector. Yet this is not the case in many countries.

- Implementing healthcare cards with an identification number and PIN or biometric authentication would enable the creation of personalized, **online services**, a quintessentially «patient-centric» approach, yet these initiatives are still in the development stages.

- The ability to **verify benefits**, expiration dates, repeated and multiple uses is on the whole under-used.

- Thus far, the benefits of paperless, electronic medical data exchanges have not been fully tapped.
  Yet cards have a crucial role to play in **creating consistent databases**, with the automatic reading of data, and the temporary or permanent **confidential local storage** of additional data such as blood groups, allergies, chronic diseases and associated treatments.

Electronic services that have already been implemented in European countries and in the rest of the world—with identification systems, electronic signatures and electronic authentication—clearly show that the key elements (microchip cards, public key infrastructure, authentication, etc.) of a modern healthcare system can rely on robust technology to rise to the challenges presented by fraud, abuse and errors.

**This robust technology can strike at the heart of fraud mechanisms,** often with minimal investment in infrastructures, and without major changes for patients and healthcare professionals. Smart card technology is an invaluable asset to combat healthcare fraud in the interest of all.

# Appendix 1: FORE study

**FORE – Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities – 009/2005).**

**State 1 (Status quo) :** No National Health Information Network (NHIN). Some electronic medical files, electronic claims and databases, but no aggregation of clinical data, and no interoperability.

**State 2 (Early NHIN):** Start of the national network. At this stage, clinical transactions, laboratory results and prescriptions are common, and electronic medical files are increasingly used, but there is very little interoperability.

**State 3 (Intermediate NHIN):** There is a national healthcare network. Interoperability between tools, and the amalgamation of servers for medical files enable clinical data and records to be shared by professionals. Clinical vocabularies are widely used, and ICD-10 (medical classification for diseases, signs and symptoms) has been implemented. Intelligent coding tools have been implemented for claims.

**State 4 (Advanced NHIN):** The national healthcare network is widely used. Interoperability enables clinical, administrative and financial data to be aggregated; analysis tools can then be used on this data to detect fraud profiles.

In the following tables, the overall approach to make healthcare data procedures paperless has other benefits apart from in the fight against fraud. In this sense, the research institute includes “indirect” costs and benefits in order to enable the overall calculation of ROI.

In this model, fraud amounts by type and then for the four stages of the development cycle are assessed.

## Fraud-Related Costs

**In this table there is a total of $158 billion in fraud, which decreases progressively as the system matures. We can see specific investment linked to analysis tools (intelligent costs and analytic tools) of more than $6 billion.**
**A large amount of fraud is linked to weaknesses in controlling information systems: identification fraud and false claims.**

| Table 1 – Fraud-Related Costs<br>Population : All US<br>295 743 134 | States of the World (in millions) | | | |
|---|---|---|---|---|
| | 1 - Status | 2 - Early | 3 - Intermediate | 4 - Advanced |
| Costs Fraud-Related | | | | |
| Identity Theft for Any Purpose | 1 166 $ | 1 400 $ | 1 050 $ | 700 $ |
| Faked Services Under Fictitious Provider ID | 8 872 $ | 5 323 $ | 1 774 $ | 237 $ |
| Faked Services Under Real Provider ID | 37 $ | 48 $ | 22 $ | 7 $ |
| Unnecessary services for revenue only | 25 878 $ | 31 053 $ | 10 351 $ | 5 176 $ |
| Upcoding & mis representation of treatment | 22 181 $ | 26 617 $ | 4 436 $ | 2 218 $ |
| Govt. Investigation & Prodsecution | 286 $ | 343 $ | 372 $ | 400 $ |
| Non-commercial Investigation & Prosecution | 429 $ | 515 $ | 558 $ | 601 $ |
| Intellignet costs | - $ | 450 $ | 900 $ | 1 080 $ |
| Analytic Tools | - $ | 540 $ | 540 $ | 2 700 $ |
| **SUBTOTAL** | (58 849) $ | (66 289) $ | (20 003) $ | (13 118) $ |

## Non Fraud-Related Costs

Table 2 outlines non-fraud related costs for a high-performance system—the astronomic amount of nearly $232 billion, with nearly 74% allocated to interoperability issues (organization, procedures, technical frameworks, etc.) and 13% for data storage.

| Table 2 – Non Fraud-Related Costs<br>Population : All US<br>295 743 134 | States of the World (in millions) | | | |
|---|---|---|---|---|
| | 1 - Status | 2 - Early | 3 - Intermediate | 4 - Advanced |
| Costs Non Fraud-Related | | | | |
| **Capital Investment** | | | | |
| Physicians | 880 $ | 968 $ | 1 012 $ | 1 056 $ |
| Hospitals | 2 780 $ | 3 058 $ | 3 197 $ | 3 336 $ |
| Other Providers | 1 080 $ | 1 188 $ | 1 242 $ | 1 296 $ |
| **Operating Costs** | | | | |
| Physicians | 240 $ | 264 $ | 276 $ | 288 $ |
| Hospitals | 720 $ | 792 $ | 828 $ | 864 $ |
| Other Providers | 380 $ | 418 $ | 437 $ | 456 $ |
| Data Storage | 1 461 $ | 5 843 $ | 11 686 $ | 14 607 $ |
| **Interoperability transition costs** | | | | |
| Physicians | - $ | 4 355 $ | 12 194 $ | 13 936 $ |
| Hospitals | - $ | 11 980 $ | 33 544 $ | 38 336 $ |
| Other Providers | - $ | 8 130 $ | 22 764 $ | 26 016 $ |
| **SUBTOTAL** | (7 541) $ | (36 996) $ | (87 180) $ | (100 191) $ |

## Benefits gained from the fight against fraud are then calculated.

| Table 3 – Fraud Management-Related Benefits<br>Population : All US | States of the World (in millions) | | | |
|---|---|---|---|---|
| 295 743 134 | 1 - Status | 2 - Early | 3 - Intermediate | 4 - Advanced |
| Benefits - Fraud Management-Related | | | | |
| Govermment Recovery | 1 144 $ | 1 258 $ | 2 860 $ | 4 576 $ |
| Private Sector Recovery | 458 $ | 504 $ | 687 $ | 916 $ |
| Conversion to ICD 10 | - $ | - $ | 90 $ | 110 $ |
| Digital tracing for Fraud | - $ | 53 $ | 111 $ | 111 $ |
| Patient Verification of Dx & Procedure | - $ | 89 $ | 185 $ | 185 $ |
| Provider Verification of Dx | - $ | 1 800 $ | 5 700 $ | 8 400 $ |
| Digital certificates & Signatures | - $ | 786 $ | 1 638 $ | 1 638 $ |
| Reduction in record retrieval time | - $ | 2 359 $ | 5 504 $ | 7 076 $ |
| Authentification | - $ | 393 $ | 819 $ | 819 $ |
| IDs only from card swipes | - $ | 393 $ | 819 $ | 819 $ |
| Avoided time spent for fraudulent claims | 131 $ | 786 $ | 2 621 $ | 2 931 $ |
| **SUBTOTAL** | 1 733 $ | 8 422 $ | 21 033 $ | 28 581 $ |

Tables 3 and 4 show the gains from implementing the system.
Benefits from the fight against fraud only make up 15% of the total benefits.

| Table 4 – Non Fraud Management-Related Benefits<br>Population : All US | States of the World (in millions) | | | |
|---|---|---|---|---|
| 295 743 134 | 1 - Status | 2 - Early | 3 - Intermediate | 4 - Advanced |
| Benefits - Non Fraud Management-Related | | | | |
| Real time patient data for ER situations | 1 271 $ | 7 626 $ | 12 710 $ | 15 887 $ |
| Less time tracking identity for $$ eligibility | 786 $ | 4 717 $ | 7 862 $ | 9 828 $ |
| Less use of paper | 322 $ | 1 932 $ | 3 221 $ | 4 026 $ |
| Less staff to manage paper | 1 048 $ | 6 290 $ | 10 483 $ | 13 104 $ |
| Less consumer time integrating benefit info | 89 $ | 532 $ | 887 $ | 1 109 $ |
| Avoided Medication Errors | 254 $ | 1 525 $ | 2 542 $ | 3 177 $ |
| Avoided Clinical Errors | 444 $ | 2 662 $ | 4 436 $ | 5 545 $ |
| Avoided Duplicate Diagnoses | 2 597 $ | 15 582 $ | 25 969 $ | 32 462 $ |
| Avoided Unnecessary Surgeries | 844 $ | 5 065 $ | 8 442 $ | 10 552 $ |
| Avoided Liability for Medical Error | 36 $ | 288 $ | 432 $ | 540 $ |
| Less physician $$ due to avoided error/waste | 3 381 $ | 20 294 $ | 40 588 $ | 50 735 $ |
| Less pharmacy $$ due to avoided error/waste | 1 691 $ | 10 147 $ | 20 294 $ | 25 368 $ |
| Less time provider shopping | 177 $ | 1 065 $ | 1 774 $ | 2 218 $ |
| Less consumer time managing med records | 89 $ | 532 $ | 887 $ | 1 109 $ |
| **SUBTOTAL** | 13 031 $ | 78 258 $ | 140 528 $ | 175 660 $ |

The study highlights three aspects of the fight against fraud, abuse and errors:

> Productivity gains from the systematic fight against errors are five times higher than those from the fight against fraud.

> Sharing data, in particular personal medical files, is a powerful tool in the fight against fraud and errors.

> Long-term investment will be needed to see the gains from information technology.

# Bibliography & online sources

- Transparency International http://www.transparency.org/
- European Healthcare Fraud & Corruption Network (EHFCN) www.ehfcn.org
- EHFCN 2009-2010 Annual Report http://www.ehfcn.org/media/documents/AR_May2010_final_email.pdf
- "National Health Expenditures Aggregate, Per Capita Amounts, Percent Distribution, and Average Annual Percent Growth: Selected Calendar Years 1960-2009", World Health Organization
  http://www.cms.hhs.gov/NationalHealthExpendData/downloads/tables.pdf
- "Gross domestic product 2010", World Bank http://siteresources.worldbank.org/DATASTATISTICS/Resources/GDP.pdf
- "Millionenbetrug im Gesundheitswesen - auch hier brauchen wir neue Gesetze", KKH Allianz (Germany)
  http://www.kkh-allianz.de/fileserver/kkhallianz/files/1449.pdf
- German Ministry of Health http://www.bmg.bund.de/
- "Transparenzmängel, Korruption und Betrug im deutschen Gesundheitswesen" (Germany)
  http://www.transparency.de/uploads/media/Gesundheitspapier_Version_05.pdf
- Federal Bureau of Investigation (USA)
  Healthcare Fraud: http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud
  Trends : http://www.fbi.gov/news/stories/2010/june/health-care-fraud/health-care-trends
- 2010 Health Care Fraud and Abuse Control Program Report, Office of Inspector General, US Department of Health and Human Services (USA) http://oig.hhs.gov/publications/hcfac.asp
- "Combating Health Care Fraud in a Post-Reform World: Seven Guiding Principles for Policymakers", National Health Care Anti-Fraud Association, October 6, 2010 (USA)
  http://www.sas.com/resources/asset/health-insurance-third-party-white-paper-nhcaa.pdf
- "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities ", ONC Health Care Anti-Fraud Project, September 30, 2005 (USA) http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031699.pdf
- "Healthcare Fraud: The Schneider Pill Mill Case" (USA) http://i-sight.com/case-study/schneider-pill-mill-investigation/
- "ID Theft Infects Medical Records", Los Angeles Times, September 25, 2006
  http://articles.latimes.com/2006/sep/25/business/fi-medid25
- "Medicare Fraud Estimates: A Moving Target?", The Sentinel
  http://www.smpresource.org/Content/NavigationMenu/AboutSMPs/MedicareFraudEstimatesAMovingTarget/Medicare_Fraud_Estimates.pdf
- "Medicare Program Integrity (USA): Activities to Protect Medicare from Payment Errors, Fraud and Abuse", July 29, 2011
  http://www.gao.gov/products/GAO-11-592
- 2006, 2007, 2008, 2009, 2010 and 2011 reports on social fraud in France, Dominique Tian, member of the French National Assembly
- "L'usurpation d'identité ou l'art de la fraude sur les données personnelles", Guy de Felcourt, CNRS Éditions, 2011 (France)
- French Ministry of Health www.sante.gouv.fr
- "Assurance-maladie : la fraude des professionnels pèse lourd", Le Figaro, August 9, 2011
  http://www.lefigaro.fr/conjoncture/2011/08/09/04016-20110809ARTFIG00279-assurance-maladie-la-fraude-des-professionnels-pese-lourd.php
- "Les fraudes sociales estimées à 20 milliards d'euros par an", Le Figaro, June 21, 2011
  http://www.lefigaro.fr/conjoncture/2011/06/21/04016-20110621ARTFIG00742-les-fraudes-sociales-estimees-a-20-milliards-d-euros-par-an.php
- French National Assembly
  http://www.assemblee-nationale.fr/13/rap-info/i3603.asp
- Cour des Comptes (France)
  http://www.ccomptes.fr/fr/CC/documents/RELFSS/Rapport_securite_sociale_2010_septembre_2010_chapitre_8.pdf
- NHS Counter Fraud (UK) http://www.nhscounterfraud.nhs.uk/noflash.html
- Measuring the cost of fraud, PKF Accountants (UK), March 2011
  http://www.pkf.co.uk/pkf/news/press_release/measuring_the_cost_of_fraud&goto=5
- The UK Cards Association (UK)
  http://www.theukcardsassociation.org.uk

## About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work into dedicated working groups (communication, marketing, security, electronic identity).

Members are largely involved in research and development projects at the European and international levels.

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

EUROSMART
The Voice of the Smart Security Industry

## Contact us:

**EUROSMART**
Rue du Luxembourg 19-21
B-1000 Brussels
Tel. (+32) 2 506 88 38
Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com
Visit our website ! www.eurosmart.com