



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

University of Wollongong
Research Online

Faculty of Law, Humanities and the Arts - Papers

Faculty of Law, Humanities and the Arts

2016

Financial fraud in the private health insurance sector in Australia: perspectives from the industry

Kathryn Flynn

University of Wollongong, kflynn@uow.edu.au

Publication Details

Flynn, K. (2016). Financial fraud in the private health insurance sector in Australia: perspectives from the industry. *Journal of Financial Crime*, 23 (1), 143-158.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library:
research-pubs@uow.edu.au

Financial fraud in the private health insurance sector in Australia: perspectives from the industry

Abstract

Purpose - While financial fraud against the private health insurance sector in Australia has commonalities to other countries with similar health systems, in Australia fraud against the industry has garnered unique characteristics. The purpose of this article is to shed light on these features, especially the fraught relationship between the private health funds and the public health insurance agency, Medicare and the problematic impact of the Privacy Act on fraud detection and financial recovery. **Design/methodology/approach** – A qualitative methodological approach was used and interviews were conducted with fraud managers from Australia's largest private health insurance funds and experts in fields connected to health fraud detection. **Findings** – The industry profits from a robust regulatory framework, as well as the use of business and clinical rules and strong analytics. However, the sector is not uniform and the problems are not uniform. The fraud managers in the funds have differing approaches to recovery action and this range from police action, the use of debt recovery agencies, to de-recognition from the health funds. Most funds reported a need for more technological resources and higher staffing levels to manage fraud. They all viewed the Privacy Act as an impediment to managing fraud against their organizations and they desired that there be greater information sharing between themselves and Medicare. **Originality/value** – This paper contributes to knowledge of financial fraud in the private health insurance sector in Australia.

Keywords

sector, insurance, australia, perspectives, industry, fraud, financial, private, health

Disciplines

Arts and Humanities | Law

Publication Details

Flynn, K. (2016). Financial fraud in the private health insurance sector in Australia: perspectives from the industry. *Journal of Financial Crime*, 23 (1), 143-158.

Title: Financial fraud in the private health insurance sector in Australia: perspectives from the industry.

Abstract

Purpose - While financial fraud against the private health insurance sector in Australia has commonalities to other countries with similar health systems, in Australia fraud against the industry has garnered unique characteristics. The purpose of this article is to shed light on these features, especially the fraught relationship between the private health funds and the public health insurance agency, Medicare and the problematic impact of the *Privacy Act* on fraud detection and financial recovery.

Design/methodology/approach – A qualitative methodological approach was used and interviews were conducted with fraud managers from Australia’s largest private health insurance funds and experts in fields connected to health fraud detection.

Findings – The industry profits from a robust regulatory framework, as well as the use of business and clinical rules and strong analytics. However, the sector is not uniform and the problems are not uniform. The fraud managers in the funds have differing approaches to recovery action and this range from police action, the use of debt recovery agencies, to de-recognition from the health funds. Most funds reported a need for more technological resources and higher staffing levels to manage fraud. They all viewed the *Privacy Act* as an impediment to managing fraud against their organizations and they desired that there be greater information sharing between themselves and Medicare.

Originality/value – This paper contributes to knowledge of financial fraud in the private health insurance sector in Australia.

Keywords Australia, Claims leakage, Databases, Enforcement, Financial crime, Fraud, Identity theft, Medicare, Private health insurance, White-collar crime.

Paper type Research paper

Introduction

Compared to the U.S. and the U.K. the private health insurance sector (PHI) in Australia is favorably positioned to manage the challenges of fraud, waste and abuse. This is due to the respective roles of the public and private sectors; the level of government regulation; and fund information technology system controls. However, like the health sector in other countries, managing fraud presents difficulties; for some funds financial losses are large, fraud hard to detect and resources insufficient. In most cases staff and technological resources are aligned to the low rate of fraud that is discovered not to the amounts that remain invisible. This makes it hard for some fraud managers in the private health funds to make the case to their senior managers for improved technological and staff resources. There is a notion that the health insurance system itself is buffeted against fraud due to strict provider registration and the lack of coverage for high cost items like home health care and durable medical equipment, while ignoring the scope for fraud under a fee-for-service system and electronic claims processing. It is an area of white-collar crime where fraud can go undetected. In other words the funds don't know what they don't know, especially as new and emerging fraud schemes are an occurrence.

Private health insurance

Australia has 34 health funds with total revenue of \$19.9 billion and total benefits of \$16.9 billion (PHIAC Quarterly Statistics June 2014:11). Private health insurance in Australia is complimentary to Medicare; the country's publicly funded health insurance system. Under Medicare residents are entitled to subsidized treatment from medical practitioners, and other health professionals who have been issued with a Medicare provider number. Private health insurance covers those services not covered by Medicare, for example, private hospital care, dentistry, physiotherapy chiropractic, optometry, remedial massage and natural therapies, for example, aromatherapy, iridology, homeopathy, kinesiology, herbalism, yoga, Pilates and naturopathy. In some circumstances Medicare covers optometry, dentistry, physiotherapy and chiropractic. Private health insurance also covers things Medicare doesn't cover and they also cover what they do cover, that is the component of the Medical Benefits Schedule (MBS) item that takes place within the hospital. So Medicare pays 75% and the funds pay 25% and they pay above the (MBS) if there is a no-gap arrangement. So the funds cover services not covered by Medicare but Medicare also pays for MBS in a private hospital up to 75%. Those who elect to take out private health insurance are entitled to a means tested, government-funded rebate of 30 per cent on their insurance premiums. It increases to 35 per

cent for those over the age of 65 and 40 per cent for the over 70s. Private health insurance covers over 50 per cent of the Australian population with some form of health insurance.

Definition of fraud

Of all crimes committed in Australia fraud has been judged as the most expensive. According to the Australian Bureau of Statistics fraud and fraud-related offences are the largest category of all federal offences from all levels in Australian courts (Lindley, Jorna and Smith, 2012: 6).

The Australian government defines fraud as “dishonestly obtaining a benefit, or causing a loss, by deception or other means” (Commonwealth Fraud Control Guidelines, 2011: 4). For fraud to occur there has to be a proven intention to defraud. For it to be judged a criminal offence the behavior in question must demonstrate intention to defraud, recklessness or negligence (Commonwealth Fraud Control Guidelines, 2011:16) and in the health sphere this can be arduous. Health care fraud often does not come before the courts because it mostly involves high volume low-level instances of fraud, and the sheer volume of claims makes fraud conviction a challenge, as Dr. Tony Webber, former director of the Professional Services Review, outlines,

Because fraud is a criminal offence you have to prove beyond reasonable doubt, each and every instance of fraud and that’s extremely difficult...You have to have patients willing to testify in court, you have to have a huge document trail...and then you might prove ten instances, fifteen instances of fraud that might amount to five hundred dollars’ worth when someone who has been ripping off the system for many tens of thousands of dollars – so that is all you get back (Webber *pers. comm.* 2012).

For the private health insurance industry the solution to the definitional issue is to avoid the term fraud and use ‘claims leakage’. That way they don’t have to prove a defrauder’s intent which is a time consuming and difficult process. The term ‘claims leakage’ is not defamatory and it covers anything from fraud at one end to overservicing, to bad system controls and poor claims assessment. The term overservicing is the provision of services that are not medically necessary or clinically relevant. However, this could be a value judgment for what may be fraud to one practitioner to another could be doing what is necessary to achieve the best patient outcomes. Overservicing covers defensive medicine, over-cautiousness, practices arising from differences of medical opinion, habit or hospital policy, legal requirement, pressure from a corporate employer or personal profit (Sparrow 2000: 140,

153). By contrast, Medicare has adopted another name for overservicing and called it inappropriate practice. This is adjudicated by a separate agency, the Professional Services Review (PSR website). Inappropriate practice is a broader term than overservicing and includes a judgment by a PSR Committee as to whether certain services, provided by medical practitioners, would be judged unacceptable by their peers. It also makes an assessment on breaches of, what is called, the 80/20 rule, that is, whether there have been 80 or more professional attendances on each of 20 or more days in a 12 month period. The private health funds on the other hand manage both fraud and overservicing.

Some examples of claims leakage against the private health funds include: charging for services that were not provided; upcoding, that is, billing for a higher level of service when a lower level of service was provided; unbundling, that is, submitting bills for various tests or procedures individually when they are required to be billed together; falsifying a patient's diagnosis to justify tests or other procedures; ordering excessive pathology and radiology tests; referrals induced by kickbacks; padding of accounts; and identity fraud.

Doctors are not the only ones misusing the health funds. Hospitals, dentists, pharmacists, practice managers, allied health practitioners, receptionists, patients, staff in the private health funds, computer hackers and those involved in organized crime have all found ways of enriching themselves through healthcare fraud.

Not only are people keen to exploit the weaknesses of the health care system but also the system itself shapes the types of fraud likely to be found within it. The following structural features of both the Australian and the U.S. systems help explain the major fraud types: a fee-for-service structure where the bills are passed on to the insurer by the patients and the insurer assumes that the claims are true; private-sector involvement; electronic payment of claims and these claims not checked by staff; there is no checking that the services were in fact provided or that the patients' diagnoses are genuine and inadequate measures to deal with inappropriate practice (Sparrow 2008: 1152-1154).

The extent of fraud

The extent of health care fraud against the Australian private health insurance funds is unknown. Some suggest it is in the range of half a per cent to one and a half per cent, others suspect it is around seven per cent or higher. Fraud managers in the private health insurance

funds, who were interviewed for this study, argued that it is difficult to give a figure for the extent of fraud and overservicing for no one knows.

On the one hand there are fraudsters who understand that fraud, if well perpetrated, will remain invisible. If claims are reasonable, aligned to orthodox medical practice and are not excessive the fraud may not be uncovered. On the other hand, it is argued, most of the misuse of the funds is not caused by deliberate fraud but is caused by inappropriate practice and inappropriate billing procedures and there is a fine line between these practices and fraud (Webber *pers. comm.* 2012). Is it overservicing? Is it clinical incompetence? Where is the line to be drawn? These definitional issues present difficulties for gauging the extent of fraud (Sparrow 2000: 154). Health care fraud experts, Malcolm Sparrow in the U.S. and Jim Gee and Mark Button in Britain, undaunted by these challenges, assert that measurement techniques for health care fraud are available (Abramsky 2010: 7, Gee and Button, 2014: 9). The estimated fraud losses can then be used as the basis for calculating what is needed in terms of technological and staffing resources (Sparrow 2008: 1161).

Senior management in some of the private health funds view payments from a contradictory position: that which is positive, the speedy dispatch of claims and that which is negative, a cost centre that is a financial drain on the company due to the expense of pursuing fraud. The result is investigation departments may be left under-resourced in terms of staff numbers and new technologies to identify deviant behavior (Ebbers *et al.*, 2013: 2).

This is an industry that processes hundreds of millions of claims per annum, and makes these payments quickly and efficiently. Claims verification is through rules engines built into mainframe IT systems, and supplemented by clinical analytics. It is possible to verify claims by the rules engines but the rules may not be comprehensive. This can be an entry point for fraud. The cost of fraud can be considerable. It is here this business model reveals its downside; fraud drives up premiums and drives down productivity. In other areas of business life there is pressure for increased efficiency so as to gain a competitive advantage (Button *et al.*, 2012). This can be achieved by reducing staffing, capital, marketing and procurement costs. What is overlooked is that fraud is also a business cost but one if adequately addressed achieves gains in productivity (Gee *et al.*, 2010: 5).

Assessing the risk

The health care system in Australia has features in common with other fee-for-service health systems and has similar fraud vulnerabilities. On *Four Corners*, an Australian television investigative journalism program, broadcast in 2004, American academic Malcolm Sparrow made this distinction,

Australian culture is not the same as American culture but the nature of the fraud risks is tied directly to the structure of the payment system. And you and your Medicare program and your other fee-for-service programs have exactly the same structure as the traditional fee-for-service systems. So you face the same risks, whether you like it or not (Four Corners, ABC Television 2004).

Richard Bartlett, an official in the Commonwealth Department of Health, expressed a contrary viewpoint, he stressed that there is a fundamental difference between the health systems of Australia and the U.S.,

The American system is very different to ours. People can access specialists directly and do. You can make an argument that there are some checks and balances that exist here that they don't have...So I think there is an argument that can be made that they've got a different environment (Bartlett *pers. comm.* 2012).

He discussed the opportunities for fraud in the area of corporate medicine. Corporates are in primary care and specialist care, in optometry and allied health. The health care system works on the basis of individual doctors but does not capture the data about corporate links, so it's not set up to do that analysis well. As Bartlett described it,

A pattern for one person is far less convincing than if you know there are 40 doctors working for a corporate practice and you see that pattern repeated time and time again. Suddenly what you are starting to see is a pattern of behavior that may raise significantly higher levels of concern than if you are seeing it with one (Bartlett *pers. comm.* 2012).

Beyond this difficulty is the problem that the funds prefer to pay claims without any fuss and to pay them as quickly and expediently as possible (Fraud manager #4). This policy can have the negative effect of increasing the rate of claims leakage. One fraud manager noted that management was in disbelief at the extent of their fraud losses and their reaction was "oh, our systems wouldn't allow that" (Fraud manager #3). Not only is there a state of denial about losses from fraud but also if the fund were actively dealing with the issue it would

mean that there could be possible delays in the payment of claims. This is a direct challenge to the ethos of the health insurance industry which is to have the claim paid speedily and easily so as not to inconvenience fund members.

A fraud manager from one of the private health funds said, “the business could realize a bit more that we’re not just being difficult” (Fraud manager #3). It is not only those at the top of the organization with this attitude but also those working at the base. The call centre staff at times regards the demands of the claims review department as unrealistic and an impediment to a positive customer experience. When it is explained to these staff members that there are customers bent on their own enrichment at the expense of the funds they were wide-eyed. “Really. No. People wouldn’t do that” (fraud manager #3). Many of these personnel with direct contact with the public find fraud a foreign concept and struggle with the idea that some of their customers, providers, or health funds staff would want to exploit the insurance system. There is a lack of understanding that defrauders have a different mindset to their own; it is the mindset of those who have the motivation to defraud, and pursue their opportunity where there is the lack of capable guardianship (Cohen and Felson, 1979).

Fraudsters at work

The opportunities are abundant. The private health funds do not insist on customers presenting identification in order to obtain insurance coverage. This leaves the funds liable to be assailed by a type of scam along these lines; a customer takes out membership, defrauds a fund, cancels the membership and moves onto another fund, and defrauds it too and repeats this behavior until they have done the rounds of the funds. Then they come back to the first fund and take out membership as a “new” member, but this time with a disguised identity. They may slightly change their date of birth or the spelling of their name, for example, from John Smith to Jonathon Smith. The funds argue that Privacy legislation facilitates this type of fraud. The funds say they are not allowed by the *Privacy Act* to disclose such fraudulent behavior to other funds. As one fraud manager said, I cannot ring Medibank Private and say, “look John Smith of this address with this date of birth is coming your way and he has just ripped us off. Beware” (Fraud manager #3).

One fund manager said that they had seen innocent members being duped by another type of fraud. An ancillary provider could ask a customer to leave the membership card with them. The customer is trusting and hands over the card, which is left under the desk with boxes of

other health care cards, whose owners too are unaware that the card could be misused. The provider is part of a network of providers who get one membership card, swipes it and then passes on the card details from one provider to the next and the owner of the card might not notice that the limit on their card is declining if it is not been used regularly. It might take some time to realize that, for example, there is no physiotherapy benefit left to their membership because a provider has taken the details of the card and used it for their own advantage.

Most of the funds agreed that their best vulnerable area at this stage is on-line claiming platforms. One manager said if someone wanted to go onto their on-line platform they could walk away with hundreds of thousands of dollars. If they did it in small amounts to start off with the fund would not recognize it as a red flag in their system and the only reason they would see it is if they were actively looking for it. He cited this case of identity theft in a medical practice located across the road from a retirement village, where most of the residents are over the age of 80 and do not have access to a computer and the internet. The receptionists at the medical practice would have access to the full member details of their clients at the village. So they know the health fund, the full details of the mailing addresses, the date of birth, all the identifying information needed to register them with the company's on-line portal. They could then go in there register with those details, put in their own email addresses and activate that account and once in there go through and swipe through ten members or twenty members a week through that practice and that wouldn't show up as a red flag on the company's fraud detection system (Fraud manager #4).

Prosthesis

Highlighting areas of vulnerability to fraud a spokesman for Private Healthcare Australia (PHA), the industry's peak body, which represents 23 private health insurance funds covering 95% of the 12.4 million Australians enrolled in private health insurance, suggested the following examples. The private health funds reimburse members for surgically implanted prostheses, so this covers artificial hip joints, artificial knee joints, pacemakers, heart valves, cardiac stents, defibrillators and thousands of other items. Problems arise when a doctor will get, for example, a hip kit, get into theatre open it up have a look and say, "right that's the wrong size" and then get another one, find it is suitable, use it and then bill the fund for both of them. Doctors will only be paid for the prosthesis that they actually put into the patient. Now there are loan kits that the prosthesis suppliers give them so they can

calculate the correct size on site and so they don't have to open up any other prosthesis kits. Fraud can also occur when prosthesis suppliers give kickbacks to doctors to use a particular type of prosthesis, even when a better one is available.

One fraud manager said that as important as this instance is perhaps even more important is the case of doctors who are trained on a particular prosthesis or on a limited range of them. They get used to using that prosthesis. They are reluctant to learn to use another kit. The fund might suggest to doctors that they go back to the orthopedic registry and find that there are better kits available. The doctors might still be disinclined to take up the suggestion. A fraud manager commented until the government takes it off the prosthesis list they can use whatever they like (Fraud manager #1).

The funds would also look askance at the practice of a surgeon who is putting cardioverter defibrillators into every one of his patients with cardiac arrhythmias. Less than 10 per cent of all arrhythmias need cardioverter defibrillators and the remaining 90 per cent would need pacemakers. The position of the funds is that for mild atherosclerosis the current best practice model is that drug therapy is much more effective than stenting in the long term and if there is a doctor doing all stenting and not doing any drug therapy then there is an issue. In this case the funds would suspect the physician is upscaling their bills so those are the ones that the funds will review.

Cosmetic surgery – blurring the definitional boundaries

Paying benefits for plastic surgery is a contentious area for the health funds. Even in areas like reconstructive surgery, for example, surgery for congenital abnormalities like cleft palate and nasal deformities, surgery for skin grafts following burns injuries and surgery for facial bone fractures, the funds will only pay benefits if that surgery is covered by the particular policy that the customer has taken out. As a rule the health insurance funds and Medicare do not cover plastic surgery for cosmetic reasons. The intention of the legislation is that Medicare should not pay for cosmetic procedures. One fraud manager noted that Medicare's own data on their portal proves that it does pay for cosmetic procedures like rhinoplasties, lipectomies, liposuction, eyelid ptosis and others. This leaves the health funds in a dilemma; if Medicare pays for a cosmetic procedure should they pay as well. Many fraud managers maintain that they should draw a line in the sand and not pay benefits on cosmetic surgery.

Remedial massage and prostitution

Some fraud trends are state-based rather than national. The following pattern was apparent in New South Wales and Victoria but not in Western Australia. This scam concerned remedial massage therapy, which is covered by the health funds, but is an area open to abuse. Some brothels designate themselves as health centers, with prostitutes providing sexual services under the guise of “remedial massage”, and its patrons claiming for these services on their health insurance. This is source of frustration for legitimate professionally qualified remedial massage therapists who have worked for many years to lift the profile of the industry to the point where it is accepted as an allied health profession. The health funds are equally frustrated with the provision of benefits to prostitutes. They are now diligent in assessing the frequency of services from these remedial massage centers, and inquiring about the frequency of the services, whether the people are qualified as massage therapists, whether they are qualified through the appropriate association and whether the services are adult services. Action taken from the largest of the funds, Medibank Private, was to cancel the provider registrations of dozens of these remedial massage centers and refusing new applications from prospective remedial massage providers (Duff, 2013).

Detecting fraud

The scope for fraud is wide: the ingenuity of embezzlers manifold. Fraudsters are forever on the move in devising imaginative ways to overcome fraud controls. Gaming the system is the opportunist who beats ‘the rules’ (edits and audits) by billing correctly (Sparrow 2008). Given the vulnerability of health insurance systems to fraud there are a number of ways of managing the problem. The first is a low-tech approach, which is to encourage consumers to report suspicions they may have of irregularities in their insurance accounts. However, there are divergent views as to whether consumers are effective as a frontline defense against fraud. On the one hand, some think that consumers do report malfeasance and this is the case with both the private and public health insurance funds (Bull. of World Health Organ. 2009; Sparrow 2000, 85-90; Jonas 2014). Medicare, for example, has a strategy of encouraging the public to report fraudulent irregularities and that is successful, with over a thousand tip-offs in the period of a year (Scott and Branley, 2014). On the other hand it is the experience of one fraud manager that most consumers have a blind trust in their physicians. They have a mindset that is uncritical of certain medical practices, for example, high levels of pathology tests that can go unquestioned. They don’t report fraud and abuse, in fact, “they don’t question, they don’t ask and they don’t get a second opinion” (Fraud manager #3). Some

funds find that write-outs to their members gets them very little response. It can be the case that there can be collusion between the fund member and the provider and if one blows the whistle on the other, they are both implicated in fraud (Fraud manager #1).

As for high tech options for detecting fraud, the private health funds are beset by a number of challenges. It is not a topic at the forefront of management concerns in some funds as they prioritize the fast payment of claims rather than the accuracy of claims payment. For this reason some funds have labored to get management support for the purchase of sophisticated technological resources and qualified staff needed for fraud control. Cost is a strong determinate; the most advanced technologies are highly priced so it makes these tools expensive even for the large funds. One fraud manager said he has significant annual software license costs and has highly skilled staff; it is expensive, he admits, but he does get a good return on the investment. He emphasized that important as the software is, equally important is having staff with the right skill set. His staff component includes computer programmers, actuaries, statisticians, health economists, nursing personnel, and clinical consultants. They need to be adept at managing the technology, be fascinated by data and be able to see the patterns in it. Useful too is an understanding of systems and system controls and having a keen nose for suspicious transactions. Also valued is a resilient disposition to tolerate abuse by those they are investigating.

Prospective approaches to fraud control are rules based technologies applied to hospital, medical and ancillary claims data. All the major funds use rules engines for fraud detection. The rules are clinically based or as simple as a frequency cap. A rules engine that is embedded in the mainframe computing system checks claims and every claim is scrubbed through this rules engine overnight, to ensure that there are no breaches, or that there is no duplicate payment, and staff produce an exceptions report for the fraud manager to examine the next day. Over time the rules base needs to be tested, the system refined and new rules added. Some larger funds embed rules in their mainframe system basically of their own volition; other funds have a partnership with a software manufacturer for the continual cycle of improvement on the basic software. The rules engines have the potential to go live – to check claims in real time – that is at the time of actually making the claim.

Retrospective analytics cover predictive modeling, using statistical and data mining techniques that run through large volumes of healthcare data, provider profiling

to see who is outside the 75th percentile in their services, scoring algorithms, social network analysis and text mining (Srinivasan and Arunasalam, 2013).

Resources

Some health insurance fund managers are resigned to the fact that their departments are under-funded. One of the managers said that while his work was appreciated by his company this did not translate into the extra funds for fraud detection. Reflecting on his years with his department he said,

It has taken me quite some time to get the right people around me. Could they be better? Of course they could. Do I catch it all? Of course I don't. Is there more out there to be caught? Of course there is. So it is a matter of the balance – the commercial reality of how to go about getting it versus what you get at the end of the day (Fraud manager #2).

Echoing this sentiment was a manager from another fund who said if they want more resources, whether they staff or IT resources, they have to prove how much fraud there is and prove that there will be a measurable return on investment in the short term.

Recovery action

Once fraud is identified, fraud managers differed in their approaches to recovery action. One fraud manager argues for the use of rules and strong analytics. One takes an aggressive line saying that if the dollar amounts are significant he would go to the police, arguing that the carefully prepared police brief is the most effective approach, especially when police are well practiced in healthcare fraud recovery and are prepared to pursue action on the matter. This tool is used in conjunction with two other measures: derecognition from the health fund for a maximum of two years and referring the matter to the relevant professional association. Derecognition from the fund means members can still see the provider who has defrauded the fund but they will not receive a benefit. The professional associations for their part, when they have established that there is a sound case, are prepared to refer the matter to their ethics committee, who then take appropriate action (Fraud manager #2).

Another fraud manager said he is prepared to take a pragmatic approach: he demands the money be repaid and if the defrauders were recalcitrant he would consider a negotiated settlement. If a settlement cannot be agreed to, the matter would be referred to the police. Another fund used debt recovery agencies for amounts under \$3,000 and the police for amounts above that limit. The fraud manager commented that it takes quite a long time to

complete a police brief to the level of detail that is required and then it could take the police twelve months before the fund is told how the case is progressing - in all a frustrating process (Fraud manager #1). Another fund said that they recovered all outstanding debts themselves and did not use debt recovery agencies (Fraud manager #3).

Most recoveries come out of inappropriate practice, particularly with the private hospitals, as they are the ones with the largest payments. The funds will find coding issues with the hospitals on items that have been upcoded or with items that have not been billed properly. The funds make settlements with hospitals because they have contracts with the majority of the private hospitals. So there will be an agreement between the health fund and the hospital to audit on site. They will take a sample of all patients from that health fund. They will go through and check what is on their charts, how they have been billed and if there is a discrepancy and extrapolate from that against all the payments that have been made and they will make a recovery based on that amount. In cases that are disputed they use the state claims committee and the National Claims Committee to get a ruling on the interpretation of clinical coding for particular procedures.

One unusual response to fraud by one fund is not to take any action at all. This is where fund management had decided to override the recommendations of the fraud manager to take concerted action on fraud in the interests of preserving “good relationships” with a particular hospital, who had defrauded the fund (Fraud manager #4). This is poor business practice and left the fraud manager to reflect that the fund should be a lot harsher and really work to the letter of the law with the contracts.

Rate of Recovery

A spokesman for Private Healthcare Australia said that in his judgment the amount lost to claims leakage from the funds is in the range of one to one and a half per cent per annum, which is from \$200 to \$300 million a year. The health funds collectively recover around \$100 million a year. None of the fund managers regarded this amount as optimal.

When asked whether Medicare was able to deliver better results the answer was surprising. Medicare is able to recover approximately \$10 million per annum (PHA *pers. comm.* 2013) and supplements a low recovery rate with a low rate of prosecutions. The fund managers are puzzled at this performance as Medicare has a large investigative area and good analytic

tools at its disposal (Pearson *et al.*, 2006). Some of the fund managers attributed the success of their organizations to dealing with fraud, waste and abuse to the use of good analytics and rules to stop fraud prospectively and the importance of taking an aggressive line on illegal activities and then putting the matters into the hands of law enforcement and the professional bodies. The funds judged that Medicare's major focus is not on instigating tighter compliance procedures but attempting to educate providers to improve or change their practices.

The relationship between the private health insurance funds and Medicare

The Australian fund managers agreed sharing information between the private and public health insurance agencies is an important tool in fraud management as it is in other countries with similar health insurance systems (Saccoccio 2012, 2014). The fund managers understand that this operates on two levels: the first concerns information sharing on data analytics, emerging fraud trends, best practice and effective methodologies and the second is the sharing of actual payer data. The funds argue that a free exchange of information on these matters would work for the mutual benefit of all parties. Also taking this line was a recommendation contained in a confidential report into the investigative functions in the Health Insurance Commission (HIC), the predecessor of Medicare that said the organization "must use other ideas and learn from the experience of other areas, whether in the public or private sectors. The HIC should actively seek such information" (HIC/Blunn and Palmer Report 2001: 12).

This advice was not heeded then and is not heeded now. The funds find that Medicare frustrates their initiatives to share knowledge. This is a puzzle as the same schemes used to defraud Medicare migrate over to the private insurers and schemes perpetrated against private insurers make their way into Medicare. If a private health fund, for example, were losing \$30,000 due to fraudulent behavior by a provider, that same provider would be fraudulently gaining \$90,000 from Medicare, because the private health fund pays 25% of the claim and Medicare pays 75% (fund manager #3). The fund managers find the reluctance on the part of Medicare to share information is frustrating, inappropriate and inefficient, when, in fact, the exchange of intelligence on fraud control between the two sectors is legitimate, ethical and makes financial sense (fund manager #1). The funds are disappointed that Medicare is not prepared to share generic fraud patterns as Medicare's work in the out-of-hospital space compliments the work of the funds in the hospital space. In trying to

understand this situation the funds have conjectured that perhaps Medicare is constrained by the *Privacy Act* (fund manager #3), that they are stymied by their legislative overhead (Kovacs 2013; fund manager #2), or that they are hamstrung as individuals by the bureaucracy around them (fraud manager #2).

Information sharing between the private health insurance funds

The funds themselves are keen to share information with each other. The funds are aware that there is vast fragmentation of data and it is better to join up the data held by the separate funds to get a more complete view of providers, members and emerging fraud trends. To date nobody has been able to pull all the data together (Jonas *per. comm.* 2014). The major obstruction, as the funds see it, is the heavy hand of the *Privacy Act 1988* (Cth.). The funds have interpreted the relevant section of the *Act* to mean that it prohibits information sharing in two areas: on the publication of data on under-performing providers, overservicing providers and on the sharing of information on defrauders to fraud managers in other funds.

It would appear that currently the *Privacy Act* precludes the funds from sharing personal information if it is not for the primary purpose of the use of that information and that is the payment of benefits after a claim is made. The *Act* states,

If an APP [Australian Privacy Principle] entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Subclause 6.2 C states: A permitted general situation exists in relation to the use or disclosure of the information by the APP entity”. Chapter C.14 states a permitted general situation is where there is: “Suspected unlawful activity or serious misconduct”. Chapter C.20 states,

Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority. For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply (OAIC 2014).

It would appear the *Privacy Act* is indeterminate on this question and the funds have been left in a state of uncertainty as to whether they can communicate knowledge of illegal activity to other funds. So why is there this hesitancy on this matter? One explanation is that

at one time a Privacy Commissioner was asked by the funds could they proceed to share information between the funds on defrauders without fear of prosecution. The answer was well possibly they could but the Office of the Privacy Commissioner was looking for a test case (Jonas *pers. comm.* 2014). The Privacy Commissioner could make a determination on request and then if the funds were dissatisfied, they could take the issue to the Federal Court. The funds would have to pay the legal bills, which could be quite substantial. The private health funds would no doubt be adverse to setting themselves up for failure as well as carrying all the legal costs.

Conclusion

There are a number of strengths in the Australian health insurance system. There is strict provider registration, namely that the provider is the person they say they are and that they have the right qualifications. There are rules in the MBS schedule and the government says that they will pay for these items and no others. There are standardized clinical items which the funds pay both in hospital and in the ancillary sector. The private health insurance industry benefits from good product design and good clinical and business rules in their mainframe systems for the control of fraud waste and waste. In addition private and public health insurance is not liable to pay for durable medical equipment supplies or for home health care, areas that are ripe for exploitation.

Despite these attributes there are weaknesses. Fraud compromises the integrity of the private health insurance system, leaching from it millions of dollars every year. There is a lack of awareness among politicians, health administrators, staff in insurance companies and the general public about the scale of the problem. In a sense it is understandable that there is little community engagement with the issue as the idea of embezzlement and police investigations does not rest comfortably with the notion of professions dedicated to the healing arts and the common good. For some funds there are still problems convincing senior management of the technological resources they need. While the private health funds are quietly resigned to a lack of resources they are riled by the inhibitory effect of the *Privacy Act* on their best efforts at fraud control. They are also disappointed by the lack of a good working relationship with Medicare, as this works to the detriment of the two sectors in dealing with fraud issues, for the same schemes that are used to defraud Medicare are also used to defraud the private health funds.

The cost burden of fraud and overservicing is an unnecessary business expense to the funds and the profit shortfall is met with a rise in insurance premiums. Consumers are left unaware that insurance premiums are inflated to cover the costs of fraud. Fraud can be rationalized as a “business-acceptable risk” however, for those funds that are able to adequately address fraud will gain a competitive advantage. It seems that there is scope for new directions in fraud management by the funds, especially in the following areas, more extensive use of rules in mainframe high tech systems, better clinical and statistical skills for those working in this area, data sharing both between the private and public health insurance sectors, establishing an estimate of the extent of fraud and overservicing, consumer empowerment, identifying and building the tools for fraud detection, and taking effective recovery action when fraud is identified.

Acknowledgements

Funding for this article was from The Institute of Public Administration Australia, University of Canberra, Public Administration Research Trust Fund.

Thanks to Paula Arvela, Zoe Barker, Xiaoming Gao, Nicola Marks and Brian Martin for valuable comments on the draft of this paper.

Note

Interviewed for this study were: Dr. Tony Webber, Dr. Richard Bartlett, Greg Kovacs, David Jonas and fraud managers from four of the largest private health insurance funds in Australia.

References

Abramsky, S. (2010), *Interview with Malcolm Sparrow by Sasha Abramsky*, available at: <http://www.hks.harvard.edu/fs/msparrow/documents---in%20use/Malcolm%20Sparrow%20interview%20by%20Sasha%20Abramsky.pdf> (accessed 11 November 2014).

Australia. Attorney-General's Department (2011), *Commonwealth Fraud Control Guidelines*, March 2011.

Australia. Office of the Australian Information Commissioner (2014), *Australian Privacy Principles Fact Sheet 17*, available at: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles> (accessed 11 November 2014).

Australia. Office of the Australian Information Commissioner (2014), Chapter C – Permitted

General Situations, available at:

<http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-c-permitted-general-situations> (accessed 11 November 2014).

Australia. Privacy Act 1988 (Cth.), available at:

<http://www.comlaw.gov.au/Details/C201400076> (accessed 11 November 2014).

Australia. Australian Private Health Insurance Administration Council (2014), *Quarterly Statistics June 2014*, available at:

<http://phiac.gov.au/wp-content/uploads/2014/05/Qtr-Stats-Jun14.pdf> (accessed 11 November 2014).

Australia. Australian Private Health Insurance Administration Council (2013), *The Operations of the Private Health Insurers Annual Report 2012-2013*, available at:

<http://phiac.gov.au/wp-content/uploads/2013/12/2012-13-accessible-pdf.pdf> (accessed November 2014).

Australia. Australian Private Health Insurance Administration Council (2013), *Risk Management for Private Health Insurers*. Consultation Paper.

http://phiac.gov.au/wp-content/uploads/2013/01/130121_Risk-Management-Discussion-Paper.pdf (accessed 11 November 2014)

Australia. *Report of the Examination of the National Investigation Functions in the HIC*. The Blunn and Palmer Report (2001) Health Insurance Commission, Canberra.

Australia. Private Healthcare Australia (2013), Submission to the National Commission of Audit (Health and related expenditure).

<http://www.ncoa.gov.au/docs/submission-private-healthcare-australia.pdf> (accessed 11 November 2014).

Bulletin of the World Health Organization (2009), "Mobilizing the honest majority to fight health-sector fraud: An interview with Jim Gee", Vol. 87, Number 4: 254-255, available at:

<http://www.who.int/bulletin/volumes/87/4/09-040409/en/> (accessed 17 June 2014).

Button, G., J. Gee and Brooks, G. (2012), "Measuring the cost of fraud: an opportunity for the new competitive advantage", *Journal of Financial Crime*, Vol.19 No.1 pp. 65-75, available at:

<http://www.emeraldinsight.com/journals.htm?articleid=17004739> (accessed 11 November 2014).

Button, G., and Gee, J. (2013), *Countering fraud for competitive advantage: the professional approach to reducing the last great hidden cost*, Wiley, Somerset, New Jersey.

CMC-Hibis (2012), "Health Insurance Business Intelligence: Claims Leakage Detection" White paper, July, available at:

http://www.cmc-is.com/HIBIS_WHITE_PAPER_JULY_2012.pdf (accessed 11 November 2014).

Cohen L. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, Vol. 44 No. 4, pp. 588-608.

Douman, M. (2011), "Finding and preventing patterns in health insurance fraud – an Australian perspective", paper presented at Health Insurance Counter Fraud Group Annual Conference, 3 November, High Wycombe, U.K.

Duff, E. (2013), "Medibank clamping down on remedial massage parlours offering rebates for sex services", *Sydney Morning Herald*, 24 November, available at: <http://www.smh.com.au/nsw/medibank-clamping-down-on-remedial-massage-parlours-offering-rebates-for-sex-services-20131123-2y2m7.html> (accessed 11 November 2014).

Ebbers, M. Chintala, D. R., Ramjan P. and Sreenivasan, L. (2013), *Real-time Fraud Detection Analytics on IBM System z*, IBM Redbooks, New York, available at: <http://www.redbooks.ibm.com/redbooks/pdfs/sg248066.pdf> (accessed 11 November 2014)

Fullerton, T. and McDermott, Q. (2004), 'Doctoring the Figures', *Four Corners*, Australian Broadcasting Corporation Television, 6 September, available at: <http://www.abc.net.au/4corners/content/2004/s1193609.htm> (accessed 11 November 2014).

Gee, J., Button, M. and Brooks, G. (2010), *The Financial Cost of Healthcare Fraud: What Data from Around the World Shows*. London, MacIntyre Hudson LLP and Centre for Counter Fraud Studies University of Portsmouth, available at: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/The-financial-cost-of-healthcare-fraud.pdf> (accessed 11 November 2014).

Gee J. and Button, M. (2014), *The Financial Cost of Healthcare Fraud: What data from around the world shows 2014 Report*, BDO LLP and Centre for counter fraud studies, University of Portsmouth, available at: <https://fullfact.org/wp-content/uploads/2014/03/The-Financial-Cost-of-Healthcare-Fraud-Report-2014-11.3.14a.pdf> (accessed 11 November 2014)

Lindsay J., Jorna, P. and Smith, R.G. (2012), *Fraud against the Commonwealth 2009-10 Annual Report to Government*. Canberra, Australian Institute of Criminology, accessed at: http://www.aic.gov.au/media_library/publications/mr/18/mr18.pdf (accessed 11 November 2014).

National Health Care Anti-Fraud Association (2010), *Combating Health Care Fraud in a Post-Reform World: Seven Guiding Principles for Policymakers*, White Paper, available at: http://www.nhcaa.org/media/5994/whitepaper_oct10.pdf (accessed 11 November 2014).

Pearson, R.A., Murray W. and Mettenmeyer, T. (2006), Finding anomalies in Medicare, *Electronic Journal of Health Informatics* Vol. 1 No.1, e2, available at: <http://www.ejhi.net> (accessed 11 November 2014).

Saccoccio, L. (2012), "Examining options to Combat Health Care Waste, Fraud and Abuse" Statement of Louis Saccoccio before the United States House of Representative Energy & Commerce Subcommittee on Health, November 28, 2012, available at: <http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Saccoccio-Health-Combat-Healthcare-Waste-2012-11-27.pdf> (accessed 11 November 2014).

Saccoccio, L. (2014), "Preventing Medicare Fraud: How Can We Best Protect Seniors and Taxpayers" Statement of Louis Saccoccio before the United States Senate Special Committee on Aging, 26 March 2014, available at:

http://www.aging.senate.gov/imo/media/doc/Saccoccio_3_26_14.pdf (accessed 11 November 2014).

Scott, S. and Branley, A. (2014), “Australian Medicare fraud revealed in new figures, 1,116 tip-offs so far this financial year”, Australian Broadcasting Corporation Television, 7 March, available at: <http://www.abc.net.au/news/2014-03-06/australians-defrauding-medicare-hundreds-of-thousands-of-dollars/5302584> (accessed 11 November 2014).

Sparrow, M.K. (2000), *Licence to Steal: How Fraud Bleeds America’s Health Care System*, (2nd edition), Westview Press, Colorado.

Sparrow, M.K. (2008), “Fraud in the U.S. Health-Care System: exposing the vulnerabilities of automated payments systems” *Social Research* Vol. 75: No. 4: Winter, pp. 1151-1180.

Srinivasan, U. and Arunasalam, B. (2013), “Leveraging big data analytics to reduce health care costs” *IT Professional*, Vol. 15, Issue 6 Nov-Dec. pp. 21-28, available at: <http://www.computer.org/csdl/mags/it/2013/06/mit2013060021-abs.html> (accessed 11 November 2014).

Further reading

Moon, C.A. (2013), “Health Care Fraud and Abuse” in Kongstvedt, P.R. (Ed.), *Essentials of Managed Care* 6th edition, Jones & Bartlett Learning, Burlington, Massachusetts, pp. 422-434.

Morris, L. (2009), “Combating Fraud in Health Care: An Essential Component of Any Cost Containment Strategy”, *Health Affairs*, Vol. 28 No. 5, pp.1351-1356, available at: <http://content.healthaffairs.org/content/28/5/1351.full> (accessed 11 November 2014).

Transparency International, (2006). *Global Corruption Report 2006: Special Focus – Corruption and Health*. Berlin.

Webber, T.N. (2012), “What is wrong with Medicare?” *Medical Journal of Australia* Vol. 196 No.1, 16 January pp. 18-19, available at: <https://www.mja.com.au/journal/2012/196/4/what-wrong-medicare> (accessed 11 November 2014).

Corresponding author

Kathryn Flynn can be contacted at: flynn.kathy@gmail.com