AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 114

Electronic Medicare Fraud: Current & Future Risks

Russell G. Smith

Medicare, Australia's universal health insurance scheme, has been in operation in various guises for almost 25 years now. It is administered by the Health Insurance Commission (HIC), which processes claims and makes payments under various government programs relating to the provision of health services. Much of the HIC's work is now carried out using computers and, in the future, the bulk of claims and payments will be made from computer terminals located in professional practices and pharmacies. It will also be possible to make payments through the use of electronic funds transfers made direct to bank accounts.

This paper examines the nature and extent of current forms of fraud and inappropriate practice in relation to Medicare and whether future technological developments will make matters better or worse.

Adam Graycar
Director

The Health Insurance Commission (HIC) processes claims and makes payments in respect of the provision of health services and other benefits under a number of government programs in Australia. These include the Medicare scheme, the Pharmaceutical Benefits scheme, the Childcare Cash Rebate scheme, the Australian Childhood Immunisation Register, the Department of Veterans' Affairs Treatment Accounts, Office of Hearing Services and the Better Practice Program. Between 1976 and 1998, the HIC was also responsible for Medibank Private, a private health insurance fund, although since May 1998, the HIC no longer administers this fund.

At present, the HIC makes extensive use of information technology in processing and paying claims and benefits and recording data on transactions carried out with health care providers and patients. Claims are made and payments processed through a national network of 226 Medicare Customer Service Centres, located throughout Australia and connected online to a computer at the HIC's central office in the ACT. During 1997–98 more than 500 million raw service transactions were processed by this network.

The largest volume of claims come from providers who direct-bill the HIC. In 1997–98, approximately 72 per cent of services were direct-billed, either through the submission of paper claim forms or electronically using the HIC's "Medclaims" system, following which payment is made either by cheque or by electronic funds transfer direct to the provider's bank account. Some providers also make use of an EFTPOS type of device in order to transmit information to the HIC; payments are then made by credit card. At the beginning of June 1998, 2,616 sites were transmitting claims electronically to the HIC, accounting for 42 per cent of direct-bill claims.

The HIC also enables patients' claims for refunds to be made electronically in certain circumstances. A receipt from a provider for a paid, itemised account may be presented for refund either in person, without completing a claim form, or by giving details by

May 1999

ISSN 0817-8542
ISBN 0 642 24108 2

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

or call AusInfo toll free on 13 24 47

telephone using the HIC's "Teleclaims" system, introduced in 1995. In 1997, the trial of an electronic kiosk began in various rural pharmacies. Customers could make a claim by inserting their Medicare card and entering details of the claim on a touch screen. Payments in connection with these claiming systems may be made in cash if the claimant is present at an HIC Customer Service Centre; by cheque; or by direct credit to the claimant's bank account. In addition, in June 1998, trials began in each of the two Territories of "Medicare Connect", which enables patients to make claims electronically from doctors' surgeries which are linked electronically to the HIC. Pharmaceutical claims may also be made by claimants sending facsimiles from pharmacies with appropriate facilities. Approximately 600 "Easyclaim" fax devices are being installed in pharmacies throughout Australia.

Between 1 July 1997 and 30 June 1998, 128,023 Medicare services to the value of $7,461,353 were processed by electronic funds transfer—a relatively small proportion of the 202 million Medicare services billed, to the value of $6,334 million, in the same year. The number of claims processed electronically, however, continues to increase each year (HIC 1998).

The Commonwealth Government has determined to provide all appropriate government services online by 2001 and the HIC is, accordingly, well advanced in its achievement of this target. The Government's *Project Gatekeeper* aims to provide a common platform for the development of systems which rely upon public key cryptography and digital signatures. This strategy seeks to provide a system of secure electronic communications when dealing with Commonwealth government agencies such as the HIC on public networks (OGIT 1998).

This paper examines the nature of fraud and inappropriate practice existing at present in relation to the processing of claims for benefits, and how technological developments in the future may exacerbate such problems or, hopefully, reduce them.

Fraud and Inappropriate Practice at Present

At present funds may be illegally obtained from the HIC by health service providers and their employees; health service users; and other members of the public intent on defrauding the government. The most common offences investigated by the HIC relate to claims for Medicare or Pharmaceutical benefits made by means of false or misleading statements. The most common misleading statements relate to misrepresentations of the item number claimed by, for instance:

- claiming a prolonged consultation when only a standard consultation was provided;
- claiming that two services were provided, for instance an X-ray of the spine and pelvis, when only one, say an X-ray of the spine, was rendered;
- claiming pharmaceutical benefits when medications have not been supplied (Brandt 1998).

Other offences include forging a patient's name on a Medicare assignment of benefit form (*Crimes Act 1914*, s. 67), and aiding or abetting (*Crimes Act 1914*, s. 5) or conspiring with another person to commit a crime (*Crimes Act 1914*, s. 86).

The maximum penalties for these offences provided by the *Health Insurance Act 1973*, the *National Health Act 1953* and the *Crimes Act 1914* are substantial. For instance, section 128A of the *Health Insurance Act 1973* provides a strict liability offence of making a false statement without knowledge which carries a maximum penalty of a $2,000 fine. Making a false statement with intent carries a maximum penalty of a $10,000 fine, five years' imprisonment, or both (s. 128B). An offence under s. 29D of the *Crimes Act 1914* of defrauding the Commonwealth, carries a maximum penalty of a $100,000 fine, ten years' imprisonment, or both.

Fraud may also be perpetrated by patients who make false or misleading statements when seeking to obtain benefits, and by employees of health service providers, such as medical receptionist staff or practice managers, who make false claims on behalf of their employers. Sub-section (2) of section 128A of the *Health Insurance Act 1973* specifically creates a strict liability offence for employees or agents who make false or misleading statements which are then used in connection with a claim for benefits, while sub-section (2) of section 128B creates a like offence if carried out with intent.

The incidence of members of the public lodging forged medical or optometrical accounts appears to be increasing, particularly through the use of computer generated forged accounts. One recent case involved an individual who obtained almost $33,000 through the submission of false accounts for diagnostic imaging services. A number of other offenders have recently been convicted and sentenced to terms of imprisonment arising from the use of forged accounts (HIC 1998, Professional Review Supplement, p. 22).

For the year 1997–98, the HIC's Annual Report indicates that a total of 2,812 complaints of alleged fraud and inappropriate practice were recorded on its National Information Register; whilst $7.6 million in benefits paid incorrectly were recovered or were in the process of being recovered from providers and the public.

During the year 1996–97, 28 cases of public fraud against Medicare were referred to the Director of Public Prosecutions, with 17 of these being prosecuted successfully. Three cases of public fraud against Medicare were referred to the Australian Federal

Police, whilst 24 were referred to State police services. Six Pharmaceutical Benefits scheme "doctor shopping" cases were also successfully prosecuted. Eleven cases of provider fraud and one case of pathology inducement were successfully prosecuted. Three cases of pathology inducement and 19 cases of Medicare provider fraud were referred to the Director of Public Prosecutions.

During the year 1997–98, 43 members of the public were successfully prosecuted for fraud against Medicare and a further 23 were prosecuted for offences against the Pharmaceutical Benefits system. Seven medical practitioners were successfully prosecuted for fraud against Medicare, with one medical practitioner being found guilty of defrauding Medicare of $998,000.

These relatively small numbers of cases prosecuted represent the most serious offences detected by the HIC. Most cases of inappropriate practice are detected through the use of the HIC's artificial neural networks, or computerised modelling systems, with many of those detected being interviewed and counselled rather than criminally prosecuted. In 1997–98, for example, 779 providers were counselled in respect of questionable claims which they had made.

Electronic Payments Systems of the Future

In the future, the vast bulk of claims for benefits will be made electronically through the use of computers. So that providers and patients can communicate securely with the HIC, systems need to be devised to enable the recipient of the communication to be sure of three essential elements:

- the communication came from an identifiable individual;
- the communication had not been read by a third party; and
- the contents of the communication had not been tampered with after sending.

The most secure systems that have been designed for electronic communications in recent times involve the use of public key cryptography and digital signatures (see the description of these in OGIT 1998).

In simple terms, individuals making use of the system would use an electronic key pair (a digital data stream, probably contained on a computer chip card known as a token) which would enable the holder to secure any communication sent. Keys would only be issued to those who could prove their identity to an appropriate degree of certainty, and access to the key would be restricted through the use of passwords or some biometrically based system such as a fingerprint or retinal scanner.

Public key systems would make use of a public key and private key pair. Each key would consist of two very long numbers (with up to 500 decimal digits) which would relate to each other mathematically, but which would make it practically impossible to determine the private key value with knowledge only of the public key value. Even if one knew the mathematical process (algorithm) used to generate the pair, it would not be possible to reproduce the private key simply by knowing the public key. The private key would be kept secret by the holder (the HIC and the provider would each have their own private and public key pairs), while each corresponding public key would be publicly available. Any document signed using a private key would only be verifiable through the use of the corresponding public key.

In making a claim to the HIC, providers or patients would make use of the key pair to authenticate the fact that the claim had come from the individual in question. Software would also be used which would enable the recipient of the communication to be certain that the communication had not been read by anyone else and that it had not been tampered with after sending.

Encrypted communications that had been secured with a so-called "digital signature" would be transmitted to the HIC from an authorised personal computer at the provider's address, connected via a modem to the public telecommunications network. Alternatively, communications could be sent from public kiosks located at pharmacies or other public locations, or even from homes. The detailed procedures involved in the use of digital signatures would not be readily apparent to users, who would operate appropriately designed software by clicking a mouse and responding to specific password or biometric identification prompts.

The introduction of such a system nationally would mean that each of the 19.1 million people who are currently enrolled with Medicare would be provided with a cryptographic token, probably contained on a smart card. User authentication devices, such as PINs, passwords or pass-phrases, or biometric characteristics, such as a fingerprint or retinal image, would be required. These would have to be registered when cards are issued and procedures would need to be in place to deal with faulty or lost cards or access devices. An elaborate education campaign would also be required to instruct providers and patients in the use of the system—and to persuade them that it was secure and that information transmitted would be held securely and confidentially.

The system would have many benefits: the possibility of forging benefit assignment forms would be reduced, and forgery of patients' signatures by providers or their staff would be more difficult than at present. If biometric identifiers were used, then legal evidentiary problems concerning the scope of an employee's authority would be reduced. Communications would also be carried out almost instantaneously, thus avoiding current delays in effecting payment.

Fraud and Inappropriate Practice in the Future

The risk of fraud and illegality that might arise out of such an electronic claiming and payment environment would be present at each stage in the process of making claims and receiving payments:

- establishing authority to use the HIC's system;
- gaining entry to personal computers and tokens;
- preparing claims;
- encrypting data;
- transmitting data across telecommunications networks;
- gaining access to the HIC's computers;
- receiving the transmission at the HIC;
- processing the claim at the HIC;
- authorising payment;
- communicating with the HIC's bank;
- transferring funds to the recipient's bank; and
- ensuring that duplicate claims are not made in respect of the same service.

Many of these risks are well known and strategies have been adopted to reduce them (see National Research Council 1997; Stone 1998).

Inappropriate claiming

At present, most "leakage" in terms of the inappropriate payment of benefits takes place through providers making claims in respect of items not carried out, or making higher level claims in respect of lesser forms of services actually provided. The HIC's artificial neural networks provide an effective means of detecting such inappropriate practice and would continue to do so in any electronic claiming system in the future.

An important safeguard operating at present is for patients to sign paper vouchers at the time services are provided. This provides some check against providers making claims in respect of non-existent patients or patients who have never attended for the consultation in question. If an entirely electronic system were introduced, it would be essential for patients to be involved in the process of registering the claim with the HIC. This could take place by patients being required to digitally sign an electronic form in the presence of the provider, or at least at the practice address in the presence of a clerical assistant. If appropriate "user friendly" software were devised, patients could also indicate the length of the consultation or even the general nature of the consultation, thus preventing claims being made in respect of fraudulent item numbers.

The creation of false identities

One of the most frequently used means of carrying out computer based fraud in the community at present involves the creation and use of false identities.

The possibility arises of providers creating phantom referrals in respect of legitimate patients. This has already taken place through the use of paper based documents and the same type of fraud would be facilitated in an electronic system. In one recent case being prosecuted by the HIC, a psychiatrist is alleged to have made claims amounting to more than $1 million in respect of false referrals received from more than 100 general practitioners over approximately a 6-year period. The phantom referrals were, in fact, never made by general practitioners but fabricated by the psychiatrist through forging signatures and creating false referrals and benefit assignment forms (see Cauchi 1998).

Another possibility involves internal fraud by an HIC officer, who could create a false provider number and manipulate the billing system to credit funds into that provider's account. This has already taken place within the existing system. In 1997, for example, two former HIC employees were convicted of defrauding the Commonwealth by creating false provider accounts and making illegal claims to the combined value of more than $45,000 (HIC 1997, Professional Review Supplement, p. 23).

The principal means by which false identity fraud could be carried out in a public key technology framework would be for offenders to submit false documents to organisation registration authorities in order to have cryptographic key pairs issued to them for use in fraudulent ways. The Government has proposed that key pairs would only be issued to individuals who were able to establish their identity to an appropriate degree of assurance by supplying multiple and independent primary sources of identification, such as those used to open a bank account. Organisation registration authorities would, accordingly, need to have procedures in place to verify the identities of individuals to whom key pairs are issued.

Security of key pairs

Project Gatekeeper has already identified a number of other security risks associated with the introduction of a public key authentication framework. These related to the choice of algorithms; key generation and optional distribution; key management and transfer of security; proof of possession; physical, personnel and administrative security; and accreditation.

Keys could be kept on the hard drive of a computer with the cryptographic service activated by a smart card inserted into a personal computer. Smart cards could also be used to sign a digital signature and to authenticate the identity of a user. In addition to the risks associated with compromising access mechanisms used to protect keys held on computer hard drives, such as PINs, passwords and biometric devices, the possibility exists that smart card tokens themselves could be altered or counterfeited. Theft of keys and unauthorised use of tokens represent some of the greatest

weaknesses of a public key system. They could prove to be a major impediment to successful prosecution as it might be alleged that a key was stolen and used without the knowledge or authority of the person to whom it was legitimately issued.

Sender authentication

Sender authentication is generally based upon one or more of four criteria:

- something that you have (e.g. a card);
- something that you know (e.g. a password);
- something related to who you are (e.g. a fingerprint); or
- something indicating where you are located (e.g. a telephone line used in a callback system).

Each of these means of identifying the sender of a communication entails security risks:

- cards could be stolen;
- passwords guessed or cracking programs used to reveal them;
- fingerprint systems could be compromised; and
- location based systems tricked into believing that the user is located where he or she, in fact, is not (see Denning 1999).

Elaborate systems have been devised to overcome these problems and, when used in conjunction with basic education of users as to the risks they face, have been highly effective (see Denning 1998). Generally, however, biometrically based systems are the most effective in authenticating users of computer systems and these are beginning to be used in various health care settings, such as for gaining access to medical records (*Nursing Review* 1998). In Connecticut in the United States, fingerprint scanners were introduced in 1996 in order to prevent social security fraud. Recipients of welfare cheques were required to undergo fingerprint scanning prior to collection of their payments. The introduction of the technology cost US$5.1 million, but is said to have saved the state US$9 million in fraudulent claims (Denning 1999, p. 324).

Data transmission

A further issue concerns the integrity of data in the process of transmission through telecommunication networks. The possibility arises that data could be manipulated as the act of transmission takes place, either through tee-ing into telephone cables or conducting surveillance of electromagnetic radiation (EMR) from computer equipment and using the information to fabricate fraudulent records. The use of acceptable levels of cryptography provides one solution to the problem of interception, as encrypted data which may be intercepted would be unreadable without the application of the appropriate decryption key. The adequacy of encryption as a security measure depends, of course, upon the strength of the encryption system used and the determination of the attacker.

Content authentication

Issues relating to content authentication would generally be dealt with through the use of a hashing algorithm, which would create a message digest for use in determining whether or not a communication had been altered between transmission and receipt (see OGIT 1998). In order for the HIC to be able to rely upon electronic communications in subsequent legal proceedings, message digests could be archived in the HIC's central computer, thus avoiding situations in which providers or patients would claim to have lost the electronic document in question. Because the content of the document would be secured through the use of the hashing algorithm, senders would be unable to claim that the document held by the HIC was other than the one transmitted.

Payment diversion

Internationally, there have been examples of electronic funds transfer fraud perpetrated against financial institutions, and the HIC could be subject to these same forms of illegality which could involve funds being transferred from the accounts of legitimate recipients to those created illegally. Most of these cases have involved employees within financial institutions making use of confidential information in order to carry out the illegal funds transfers, or passing on confidential security information to external confederates (see Grabosky and Smith 1998, ch. 8; Denning 1999).

The HIC has already been subject to fraud perpetrated by insiders and the possibility exists that those with the technological skills could attack the HIC's electronic claiming and payment system internally. In 1998, for example, a customer service officer created fraudulent computer generated accounts in respect of psychiatric services. The officer submitted forged paper claim forms in support of the accounts. She was convicted of submitting and processing false claims and unlawfully accessing data (s. 76B(1) *Crimes Act 1914* (Cwlth)) and was fined $1,500 and ordered to make restitution of $5,834 (HIC 1998, Professional Review Supplement, p. 22).

Conclusions

At present, the HIC makes considerable use of computers in carrying out its claiming and payment operations. Computers also play a key role in detecting fraud and inappropriate practice. The continued expansion and development of these detection systems means that opportunities for fraud should be minimised, although their operation would need to be closely monitored in order to ensure that new opportunities for illegality have not been inadvertently created.

It is unlikely that the HIC, or

any other government agency, could devise a system entirely free from risk in terms of illegal and fraudulent conduct and, indeed, any system which sought to achieve such a level of security would be so unwieldy as to make its operation virtually impossible. The aim should be the introduction of systems which minimise risks, whilst at the same time provide for simple yet efficient operation. A system based upon public key cryptography, although technically complex in its structure could, through the development of appropriate software, be easy to use for both providers and members of the public, whilst not unduly lowering standards of security.

Most existing forms of fraud and inappropriate practice could be adapted for commission in a paperless, electronic environment and existing fraud control measures could similarly be used for their prevention and detection. The possibility arises, however, that individuals might seek to commit acts of electronic fraud while unaware of the security measures in place. Some might succeed in the short term, although it is likely that their activities would be promptly uncovered and enforcement proceedings taken.

Although existing Commonwealth legislation has already been amended in a number of respects to encompass computer based forms of illegality, and further reforms are being considered at present, it may be appropriate for some new criminal offences to be created. A new offence could, for example, be enacted of communicating with the HIC electronically in order to obtain a financial advantage by deception. Similarly, an offence could be created of facilitating the commission of an act of dishonesty against the HIC by enabling another person to make use of one's private encryption key or acting recklessly in relation to the storing or use of a cryptographic key or token.

Finally, the creation of an Electronic Communications Code of Conduct would be beneficial in setting out clearly the rights and responsibilities of those making use of the system, and in determining rules for resolving any disputes which might arise. Such a code could include:

- guidelines on users' obligations in maintaining computer hardware in a secure environment;
- principles to be observed for obtaining, storing securely, and using encryption keys and tokens;
- rules setting out the rights of third persons who communicate electronically with the HIC;
- the HIC's obligations regarding security and privacy of data;
- principles to be observed for determining liability and the allocation of loss arising from the use of the HIC's systems; and
- requirements regarding the communication of the code to users, similar to those which exist at present in the Electronic Funds Transfer Code of Conduct.

Although this paper has raised a number of security concerns relating to the HIC's current and future operations, the benefits arising from an electronic system could prove to be considerable if the system is appropriately designed and carefully implemented. Some specific security weaknesses in the existing claiming and payment system would be overcome, whilst an entirely electronic system would have clear benefits in terms of efficiency and accountability.

Acknowledgments

The author is grateful to officers of the Health Insurance Commission for their assistance in the preparation of this paper.

References

Brandt, P. 1998, "Fraud control by the Health Insurance Commission: A multi-faceted approach", in *Health Care, Crime and Regulatory Control*, ed. R. G. Smith, Hawkins Press, Sydney.

Cauchi, S. 1999, "Psychiatrist accused of $1m fraud", *Age* (Melbourne), 6 January, p. 5a.

Denning, D. E. 1998, "Cyberspace attacks and countermeasures", in *Internet Besieged: Countering Cyberspace Scofflaws*, eds D. E. Denning & P. J. Denning, ACM Press, New York, pp. 29-55.

Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, New York.

Grabosky, P. N. & Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney.

Health Insurance Commission (HIC) 1997, *Annual Report 1996-97*, Australian Government Publishing Service, Canberra.

Health Insurance Commission (HIC) 1998, *Annual Report 1997-98*, Australian Government Publishing Service, Canberra.

National Research Council (US), Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure 1997, *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington.

Nursing Review 1998, "Fingerprints open records", vol. 3, no. 10, p. 14.

Office of Government Information Technology (OGIT) 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, Australian Government Publishing Service, Canberra.

Stone, T. 1998, "Organized crime and Medicare fraud", *Crime and Justice International*, vol. 14, nos 18 & 19, pp. 14-15.

Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.