Health Care Fraud and Medical Identity Theft in BC, Canada and the USA

By John Dumfries, CGA, CFE, CIA
Agenda

• Discuss reasons for the new BC CareCards, & the features & limitations of the new BC CareCards.
• Discuss problems with the existing BC CareCard system.
• Examine health care fraud and Medical Identity Theft in BC, Alberta, Ontario & USA. (problems, solutions and current research)
• Discuss results of my survey regarding the public’s perception of CareCards and Medical Identity Theft in BC.
New Health CareCards

- The BC government announced on May 20, 2011, that they will be replacing the existing health CareCards with new smart cards that have enhanced security features.
- This will cost approximately $10 million to implement and $28 million each year to operate over the next 5 years.
- BC’s health ministry estimates it is being defrauded of potentially $260 million every year. This is based on The Canadian Health Care Anti-fraud Association estimate that health fraud is between 2% and 10% of total health care dollars.
- The ministry also stated that it would implement anti-fraud detection software and hire more staff to operate the system.
- The government also plans on amending the information and privacy law that will allow secure online access to health records.

Health Care Fraud and Medical Identity
Theft in BC, Canada and the USA
Reasons for new CareCards

• There are 9.1 million BC CareCards in circulation for a population of only 4.5 million.

• CareCards currently do not have modern security features and are easy to counterfeit and therefore it is a possibility that medical identity theft occurs.

• The new CareCards will better enable an electronic health care record system.
New CareCard features

The new BC CareCard will have the following security features:

- Counterfeit-prevention devices like a security chip, holographic overlays and laser engraving of the cardholder’s image and signature, plus a second “ghosted” image printed at a different depth than the primary photo.

- New polycarbonate card stock, which is much more tamper-resistant and durable.

The card will be free and only those over 19 will have to re-enrol.

Drivers will be able to re-enrol when they renew their driver’s licence every five years. Non-drivers will have a similar cycle.
Present CareCard system

- A fee is not charged for a card issued when a person first enrolls with MSP or for the first gold CareCard issued to a senior.
- A fee may be charged to replace a lost, damaged or stolen card.
- If payment is required, the fees are $20 for one card, and more depending on the number of cards that need to be replaced in a family.
- According to the Ministry of Health website, Using a Personal Health Number other than the one issued to you or allowing someone to use your number is an offence under the Medical Protection Act.
- The website also mentions how to report fraud.

http://www.health.gov.bc.ca/msp/infoben/carecard.html#replace
New CareCard limitations

• No mention by the government that the new cards will detect and prevent all forms of health care fraud and abuse.

• No mention by the government that the new cards will detect and prevent health care practitioner identity theft.

• The new CareCard as part of an electronic health record system may cause information to be more vulnerable to data breaches.
Definition of Medical Identity theft

The World Privacy Forum’s 2006 report “The Information Crime that can Kill you” defines Medical Identity Theft as “when someone uses a person’s name and other parts of their identity without the victim’s knowledge or consent to obtain medical services.”
Consequences of Medical Identity theft

• CareCards can be counterfeited and sold on the black market.

• Stolen CareCards or personal health information can be used to conduct financial identity theft.

• Addicts can abuse the system either by receiving prescription or non-prescription drugs.

• People use medical services that they are not entitled to receive. This causes records to be inaccurate.
Solutions to Health Care Fraud in BC

- Billing Integrity Program
- Other Investigations
- Identity theft and the Canadian Criminal Code
- Canadian Identity Theft Support Centre
Preventing Health Care Fraud: Billing integrity program (BIP)

The two main methods BIP monitors payments for services rendered by practitioners:

**Service Verification Audits** - Each year, approximately 75,000 survey letters are sent to patients to confirm that they received services which have been billed to MSP.

**Practitioner Profiles** - The annual profile report is an analysis of the type and number of insured services, registered specialties, that a practitioner has billed to MSP. Each practitioner within an individual peer group is then compared against the group average statistics.

Billing integrity program since 2005 has recovered $8 million. $1.6 million has been recovered so far this fiscal year (2011/2012).

[http://www.health.gov.bc.ca/msp/infoprac/bip.html](http://www.health.gov.bc.ca/msp/infoprac/bip.html)
Other examples of preventing Health Care Fraud

• The ministry states that in 2009/10, it discovered 376 fraud cases with a total dollar value of $936,000.

• A survey of 399 cards in 2010 indicated that 94% of patients claiming MSP coverage were legitimate residents of BC.
Identity Theft and the Canadian Criminal Code

The Identity theft crime bill, came into force on January 8, 2010 and created the following offences which are subject to 5-year maximum prison sentences:

• Obtaining and possessing identity information with the intent to use the information fraudulently in the commission of a crime;
• Transferring or selling identity information to another person with knowledge of the possible criminal use of the information; and,
• Unlawfully possessing or trafficking in government-issued identity documents that contain information of another person.

Now the courts can order the offender to pay the identity theft victim for costs incurred to rehabilitate their identity.

The offender can be ordered to pay restitution for actual economic losses.
Canadian Identity Theft Support Centre

- Canada's first support centre to provide resources for victims of identity theft opened in downtown Vancouver in March 2012.
- It is a charitable organization primarily funded by the federal Justice Department, the support centre is modelled on the Identity Theft Resource Center based on San Diego who also helped train staff.
- The centre won't publicize the exact location of its offices in order to protect the four full-time staff members from identity thieves.
- They plan on releasing fiscal & complaints data in 6 months.
- http://idtheftsupportcentre.org/media/in-the-news/
Medical Identity Theft in Alberta

In October 2004, Auditor General Fred Dunn examined the occurrence of medical identity theft. The following are some of the results:

- In some regions near the U.S. border there were twice as many health numbers than residents;
- One Albertan was issued 60 duplicate or replacement health cards, while 32,440 people had received five or more;
- 123 municipalities had at least 2 health numbers for every person counted in the Dec. 2003 census;

Mr. Dunn estimated that if 1% of the province's $8-billion annual health spending was lost due to fraud, taxpayers were losing $80 million a year.

Specifically regarding medical identity theft, in 2002-2003, a Health Ministry investigator reviewed 105 cases and found 54 ineligible numbers.
Medical Identity Theft in Ontario

• In 1995, Ontario issued health care cards with the person’s photo and they will have to be renewed every 5 years with a proof of residence. This system was estimated to have cost $30 million per year for 3 years but prevent $65 million per year in fraud.

• Ontario government officials estimated that in 1993, 400,000 health cards existed that could not be accounted for. In 2005, there was approximately 300,000 extra cards issued.

• Another 1993 health ministry report estimated that approximately 60,000 ineligible people from outside Ontario received health care services at a total cost of $85 million.

• The Ministry of Health concluded that in one investigation approximately 588 Americans might be receiving free health care that lived near the Ontario, Quebec and New York State borders.
Medical Identity Theft in Ontario

• According to police an Ontario Health care card sells for about $1,000 on the street.
• Of the 300,000 cards in 2005, 268,000 of those are in the Toronto area. 10,000 extra cards are in regions near the US border.
• The health ministry conducted a data integrity audit and they cancelled cards not used and did not respond to requests to receive a replacement card with a photo.
• Also, the health ministry cancelled 1,100 cards that had PO boxes as their address.
Medical Identity Theft in Ontario

The Ontario government also implemented the following security measures:

• legislation requiring health care providers to report suspected fraud and retain invalid cards;

• swipe readers and toll-free numbers for hospitals and clinics to validate cards; and

• special investigations unit to investigate fraud.
Medical Identity Theft in Ontario

In 1998 the Ontario Ministry of Health and Long Term Care with the Ontario Provincial Police created a team of 28 officers to investigate health care fraud.

The OPP health team defines User Fraud as “crimes related to receiving services or products that they are not entitled to or any crimes involving Ontario Health Cards”. The OPP health team also investigates Provider fraud and Drug Diversion.

Examples of User fraud (medical identity theft) are the following:
• Ontario residents who "lend" their cards to non-residents of Ontario;
• anyone who falsely obtains a legitimate health card; and
• anyone who receives health services or products illegally in Ontario;

OPP Health Fraud Investigation Unit from 1998 to 2000 investigated 500 cases, 60 involving fraudulent billing (average of $800,000 per case) with 25 charges laid and 18 physicians convicted.
Medical Identity Theft in Ontario

- Medical Review Committee recommended charges on 548 physicians from 1991-2002 and $36 million was recovered.

- This committee was cancelled due to doctor backlash.

- Estimated $13 million to $17 million loss in recoveries due to the cancellation of the committee from 2003 to 2006.

- Ontario reinstated the Payment Integrity Program which is much like BC’s Billing Integrity Program.
Example of health practitioner identity theft

Health practitioner identity theft is the theft of medical professionals' identity to obtain insurance payments for services that are either never rendered, or carried out by unqualified personnel. The Insurance Bureau of Canada issued nine official alerts regarding health practitioner identity theft in 2009 and 12 in 2010.

The following is an example of health practitioner identity theft:

• A rehab clinic investigated by the Financial Services Commission of Ontario was fined $144,000 in 2007 for stealing the identity of a Toronto psychologist and using it to make at least 29 insurance claims worth $136,000.
Health Care Data Breaches in Canada

- A nurse at Durham Region Health lost a USB key containing unencrypted personal information of 83,000 people in Dec. 2009.

- The USB key contained personal health information of people vaccinated against H1N1 in eight clinics from October to December 2009. It was dropped somewhere between the regional headquarters parking garage and the building. The USB key was never found.

- DRH agreed to pay $500,000 in a class action settlement (approx. $6 per record).

- Records containing the personal health information of nearly 6,500 Ontarians who took part in the colon cancer screening program may have gone missing though Canada Post’s Express Post service.
Health Care Data breaches in Canada

• A Regina doctor is being faulted for poor record-keeping practices after approx. 2,862 patient files were discovered in a paper-recycling bin behind a mall.

• These records were not properly marked and were stored in a non-secure storage area for 5 years prior to being recycled by cleaners.
Fair Warning Inc. Study of Canadian Data Breaches

• 3.7% of Canadians have been data breach victims of personal health information. According to a survey of 1,002 patients in October 2011 by Fair Warning Inc.

• Of those, 57% of victims were negatively impacted. 11% were victims of Medical Identity Theft and 11% had inaccurate medical records.
Canadian Research into Health Care Fraud and Medical Identity Theft

- Phonebusters/Canadian Anti-Fraud Centre

- Greyhead Associates (2006)

- Canadian Health Care Anti-Fraud Association (2004 Canadian Health Care Fraud Survey)

- Dr. Joan Brockman, SFU (May 2005)
Health Care Fraud in Canada

The 2004 Canadian Health Care Fraud Survey asked 109 senior health-care insurance professionals and claims processors.

The following is a summary of the results from organizations:

• 95% were healthcare claim fraud victims, Half had over 30 incidents of fraud
• 77% discovered fraud through a claims review process
• 69% detected fraud from receiving external tips
• 87% indicated that Health care providers were responsible for fraud
• 9% indicated that individual policyholders were responsible for fraud

Top 2 types of fraud according to the survey:
90% - Billing for services not provided
68% - Up-coding (charging for a more expensive procedure than provided)
Medical Identity Theft in US

According to the March 2011 Ponemon Institute study, an estimated 1.49 million Americans were medical identity theft victims at an average cost of $20,663.

- 49% of medical identify theft victims lost their health coverage,
- 50% had to make payments to the healthcare providers in order to regain their health insurance coverage, and
- 28% were misdiagnosed or received mistreatment due to inaccurate medical records.

The June 2012 Ponemon Institute study (released yesterday), an estimated 1.85 million Americans were medical identity theft victims at an average cost of $22,346.

31% of the survey respondents said they let family members use their information to obtain medical care.

Medical Identity theft is estimated to have a $41.3 billion impact on the U.S. economy, up from $30.9 billion in 2011.
Medical Identity Theft in US

In the 2011 FTC report, Medical Identity Theft is estimated to be 1.3% of all identity theft complaints (19% of all complaints) received in 2008, 2009, 2010.

A 2011 survey conducted by PWC Health Research Institute of 600 executives from US hospitals and physicians, health insurers, and pharmaceutical companies found that 36% of provider organizations had experienced medical identity theft.

A survey by Nationwide Insurance in 2012 among 2,001 adults found that only (15%) of insured adults say they are familiar with medical identity theft. Of that 15% only (38 percent) could correctly define “medical identity.”
Cost of health care fraud in US

• Health care fraud is estimated by the World Privacy Forum’s 2006 report to be between 3% to 10% of all health care costs or 80 to 120 billion dollars per year.

• A stolen medical identity in the US has a $50 street value, according to the WPF – whereas a stolen social security number is only $1.

• According to an 2008 estimate from the FBI, Healthcare fraud is costing American taxpayers between $70 billion to $234 billion annually.
Solutions to health care fraud & medical identity theft in the US

• Smart cards
• Identity theft Red Flags Rules created by the Federal Trade Commission
• Medical record privacy legislation such as HIPAA and the HITECH Act
• Biometrics such as palm vein recognition and iris scanning during the registration process
• Analytical and predictive anti-fraud software
Smart cards as a solution in the US

The following is a summary of smart card uses in health care according to the Smart Card Alliance:

- Supporting privacy and security requirements mandated by HIPAA
- Providing a secure carrier for portable medical records
- Reducing administrative costs by reducing paperwork
- Reducing healthcare fraud
- Providing secure access to emergency medical information
- Holding encrypted patient information, compute a digital signature or biometric template.

In 2011, the SCA estimated that Medicare Fraud is $60 billion per year. SCA stated that a smart Medicare ID could reduce fraud by 66%, for a net annual savings of $37 billion.
Biometrics

• The Patient Secure Identity (PSI) system identifies patients through palm vein recognition.
• Patients initially enroll by using a photo ID and other verification data but don’t have to use their SSN or ID once enrolled.
• There is less chance of duplicate patient records or fraudulent use of SSNs, IDs and insurance cards.
• The PSI system integrates with the electronic medical record system and patients can be quickly identified in case of an emergency.
• Health care providers considered palm recognition the most secure of all other biometric options and the least invasive.
Red Flags Rules

The Federal Trade Commission created the Red Flags Rules for creditors in the United States. The Red Flag Rules require:

• Health Care providers (clinic, hospitals but not physicians) to implement a program that will prevent and detect fraud such as suspicious account activity or suspicious documents (personal identifying information).

• Health Care providers are also supposed state possible actions the health care provider will take in event of Identity theft.

• The health care providers will have to train staff and have the program approved by the board of directors.

• Penalties for non-compliance are up to $2,500 per violation discovered by the FTC.
Legislative solutions

- American Health care providers have to comply with the Health Insurance Portability and Accountability Act (1996).
- The authors of the Exploring Medical Identity theft study concluded that (HIPAA) does not address medical identity theft and poses barriers for victims.
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted in 2009 addresses the privacy and security concerns associated with the electronic transmission of health information.
- Specifically the HITECH Act states new breach notification requirements and new rules for the accounting of disclosures of a patient's health information.
Office of the Inspector General
Department of Health and Human Services

• The Department of Health and Human Services (HHS) mandate is to protect the health of all Americans and providing essential human services.
• Medicare program is the nation’s largest health insurer, handling more than 1 billion claims per year.
• Medicare and Medicaid together provide health care insurance for one in four Americans.
• Medicare 65 and older, and/or with certain disabilities.
• Medicaid based on various living and income circumstances.
• List of OIG Most Wanted Health Care fraud Fugitives on their website.
Results of the Office of the Inspector General HHS Investigations in 2011

- HHS budgeted $1.7 billion in Fraud Detection costs in 2011.

- Healthcare fraud charges against 1,430 defendants, 743 criminal convictions.

- 977 new investigations of civil healthcare fraud and recoveries of about $4.1 billion.
Office of the Inspector General
HHS Investigations in 2012

- February 2012 A physician, the office manager of his medical practice, and five owners of home health agencies, were charged in a nearly $375 million health care fraud billing scheme.

Health Care Fraud and Medical Identity
Theft in BC, Canada and the USA
May 2012 charges were laid against 107 individuals, including doctors, nurses and other licensed medical professionals, for their alleged participation in approximately $452 million Medicare false billing schemes.
Medicaid Card fraud

- In 2006, Federal authorities charged 16 people, including 8 New York City employees, with conspiring to defraud the government by buying, selling or renewing Medicaid identification cards.

- Hundreds of cards were sold for $300 to $400 apiece and then used for medical and prescription-drug benefits in a scheme that cost the government $3.9 million in 2004.
Health Care Data Breaches in the US

Department of Health and Human Services states that there has been a total of 385 breaches affecting over 19 million individuals since breach reporting notification requirements went into effect in August 2009. For a breach to be reported, it must affect 500 individuals or more.

Of the 385 breaches of protected health information:
- 39% occurred on a laptop or other portable device
- 25% occurred on a desktop PC or server
- other sources of breaches included paper records/documents
- 60% resulted from malicious intent such as theft or hacking
- Other breach methods included mistakes by employees
Health Care Data Breaches in the US

According to the Privacy Rights Clearinghouse three of the top 6 breaches in all US based organizations in 2011 were in the health care industry.

• A laptop was stolen containing protected health information of 4.2 million people.

• Nine data servers containing sensitive health information of 1.9 million current and former policyholders went missing from a data center.

• Backup tapes stolen from a car resulted in the exposure of protected health information from approximately 5 million patients of military hospitals and clinics.
Cost of HIPAA violations

HHS announced in March 2012 that Blue Cross Blue Shield (BCBST) has agreed to pay $1.5 million to settle claims that BCBST violated HIPAA in connection with the theft in 2009 of 57 unencrypted hard drives containing protected health information of over 1 million individuals.

Large Enforcement Actions Since 2009

- CVS Caremark Co.: $2.25 million, February 2009
- Rite Aid: $1 million, July 2010
- Massachusetts General Hospital: $1 million, February 2011
- Cignet Health fined (not a settlement action) in February of 2011 - $4.3 million civil money penalty, the largest fine for such violations.
Summary of US researchers

- The Federal Trade Commission has compiled Identity theft statistics since 1998 based on complaints received by the Consumer Sentinel Network (comprised of various law enforcement agencies). They also have reported medical identity theft specifically since 2001.

- World Privacy Forum (2006) conducted interviews with stakeholders and researched existing medical identity theft statistical reports, civil and criminal cases.

- Booz Allen Hamilton conducted a town hall meeting of industry experts (2009).

- The Exploring Medical Identity Theft paper (2009) conducted a survey of 133 compliance officers that work in the medical industry.

- Ponemon’s Third Annual Survey (2012) on Medical Identity theft used a web based sampling plan consisting of a general sample of US consumers.
Summary of recommendations from US Researchers:

• Victims of financial identity theft can use the credit reporting system to recover. Medical identity theft victims lack similar resources.

• It is difficult for medical identity theft victims to determine where the theft took place because patient records are shared with various medical providers.

• Patients should monitor their credit reports and medical records.
Summary of recommendations from US Researchers:

• Most cases of medical identity theft occur through the emergency department.
• Time constraints in admitting and registration departments may result in lack of compliance with policies and procedures related to ID verification.
• Ignorance of medical identity theft result in people being vulnerable.
• Victims are willing to share the health care information with family members.
Summary of recommendations from US Researchers:

- Identity theft prevention should be a condition of licensing or accreditation for health care providers.
- Compliance with medical identity theft policies and procedures should be monitored.
- Reducing use of SSN during Admission and registration could reduce medical identity theft.
- Educate the public, medical staff and law enforcement of medical identity theft.
- Conduct systematic, structured surveys on the frequency of medical identity theft.
Analysis of survey participants

• Total response rate was approximately 36%.

• 70 individuals responded to all questions.

• 35 respondents were female while 35 respondents were male.

• 49 respondents (70%) were in the 30-44 age range.

• Respondents were from a variety of occupations.
Background survey questions results

• 43 respondents were aware of medical identity theft while 27 were not aware. (ignorance makes potential victims vulnerable)
• 24 respondents (or knew of someone that) had been victims of identity theft.
• None of the respondents loaned out their cards to family members
• 9 respondents lost their card, 5 of those informed the Ministry of Health.
• 22 respondents read the May 20th, 2011 Vancouver Sun article where the government announced the new health CareCards.
• 34 respondents were more concerned with Financial Identity Theft as compared to Medical Identity theft while 30 respondents neither agreed or disagreed.
Public Perception of the new health CareCards

Agreed that the government should implement the new health care cards to prevent medical identity theft. 70%

Agreed that 9 million cards in circulation is potential for fraud. 73%

Benefits of the new enhanced security cards will not exceed its costs. 61%
What is the most important impact of the new smart health care cards?

- Improve and maintain the accuracy of medical records: 41%
- Improve efficiency of registration and billing processes: 29%
- Reduce medical identity theft: 20%
- Reduce other health care fraud and abuse: 10%
What is the worst consequence of medical identity theft?

- Addicts gaining access to prescription and non-prescription drugs: 9%
- Causing lineups/wait times to increase: 4%
- Personal medical records being incorrect: 33%
- Use of services not entitled to: 20%
- Waste of resources (Doctor/Nurse time, machines): 34%

Health Care Fraud and Medical Identity Theft in BC, Canada and the USA
Canadian Alternatives to reducing Medical Identity Theft

- Stronger and Consistent authentication procedures at registration will reduce Medical Identity Theft: 71%
- Government should use Facial Recognition Software like ICBC to authenticate users of the health care system: 53%
- New Identity Theft law will protect me from Medical Identity Theft: 51%

Health Care Fraud and Medical Identity Theft in BC, Canada and the USA
US Alternatives to reducing Medical Identity Theft

- Agreed that Ministry of Health should use anti-fraud software: 64%
- Agreed that Canada should implement Health Care specific privacy legislation: 57%
- Agreed identity theft red flags should be implemented in Canada: 71%
- Did not agree with use of biometrics: 70%
Role of Stakeholders in reducing Medical Identity Theft

- BC Ministry of Health needs to improve how it processes changes to health coverage: 59%
- Onus is on stakeholders to protect information and not the individual: 24%
- BC Ministry of Health needs to improve how it assists victims of medical identity theft: 56%
- BC Ministry of Health needs to improve how they protect information: 59%
- Stakeholders should research medical identity theft more: 60%
- Stakeholders should educate public more about medical identity theft: 64%

Health Care Fraud and Medical Identity Theft in BC, Canada and the USA
Comments from survey participants

• I have never really seen fraud but have worked with the Min of Health before and the **procedure to get BC Medicare is very easy and I'm sure duplications exist or family members using each others CareCard.**

• I have not had a problem with medical identity theft but strongly agree with the CareCards having better security features.

• Healthcare fraud is not as important as lack of access to healthcare service for a lot of BC residents.

• **Working in the health care field you get a large number of the families sharing CareCards.**

• Cards should have a picture of the card carrier on them.
Comments from survey participants continued

• It's too easy to get a name-change on the BC CareCards and also to get replacement cards since all I had to do was make a phone call and one was mailed out.
• There is no proper system of reporting possible id theft in the community pharmacy.
• I know someone has discontinued the CareCard and not paid the MSP annual fee for many years but the CareCard is still valid. I think Ministry of Health should improve process.
• As a medical technologist working in the Delta hospital, I have seen Pt. Roberts (U.S) residents using BC CareCard to register on our system and I was told that no question should be asked. Also, I know a bunch of people have incorrect name on CareCard because of the transcription error in the CareCard issuing process. However, because it is so troublesome and cost money to correct it, none of them request the correction.
Summary of survey results

- Slightly more respondents (73% versus 70%) agreed that the excess cards in circulation being a problem of fraud as suppose to agreeing that the government should issue the cards.
- Respondents stated that the benefits of the new CareCards will not exceed the costs of implementation.
- Respondents agree that stakeholders should become more involved in protecting and educating the public regarding medical identity theft.
- Respondents agree that the Ministry of Health should improve it’s processes of CareCard changes, how it assists medical identity theft victims and improve how it protects personal health information.
- Respondents agree that a US style Red Flag reporting system, and stronger and consistent authentication procedures (two forms of ID) would be effective methods of reducing medical identity theft.
- Majority of Respondents are against using biometrics.
Conclusion

• Medical Identity theft is a special type of Identity Theft and should be tracked and investigated separately from Identity Theft and Health Care fraud.

• Most people are not aware of Medical Identity Theft and this means that they are vulnerable to become victims. This lack of awareness occurs possibly because individuals aren’t as directly effected as compared to “regular” financial identity theft.

• Medical Identity theft is the crime that can kill you, as it may effect an individuals medical records in Canada and the US. Medical Identity Theft victims maybe given the wrong treatment or in the US they may be denied insurance coverage.

• Even if Medical Identity theft and Health Care Fraud doesn’t impact people directly creates inefficiencies with the system. We are all taxpayers and have to pay for fraud, waste and abuse, so we should care. One dollar lost to Fraud is one less dollar to spend on Hospitals, Nurses, Doctors and equipment.
Resources:

- Canadian Health Care Anti Fraud Association: [http://www.chcaa.org/blog/](http://www.chcaa.org/blog/)
- Canadian Identity theft Support Centre [http://idtheftsupportcentre.org/idtheft/](http://idtheftsupportcentre.org/idtheft/)
- Ministry of Health Billing Integrity Program [http://www.health.gov.bc.ca/msp/infoprac/bip.html](http://www.health.gov.bc.ca/msp/infoprac/bip.html)
- World Privacy Forum [http://www.worldprivacyforum.org/medicalidentitytheft.html](http://www.worldprivacyforum.org/medicalidentitytheft.html)