A SELF-TRAINING MANUAL FOR MARYLAND STATE EMPLOYEES

JUNE 2008

Protecting Privacy in State Government

A SELF-TRAINING MANUAL FOR MARYLAND STATE EMPLOYEES

Protecting Privacy in State Government

Special Thanks To:

California Office of Information Security & Privacy Protection
www.oispp.ca.gov

Table of Contents

In this Manual

All state employees have a duty to protect privacy. Your job may require you to routinely work with personal information. Or you may only occasionally come into contact with it on the job. In either case, you have the ability and the duty to handle it properly. Protecting personal information is essential to protecting the privacy of your fellow Marylanders.

The Manual will give you basic information on how to manage personal information responsibly in your job.

- You will learn about the basic information privacy laws that apply to state government.
- You will learn some good – and bad – practices for handling personal information in your job.
- You will learn how to recognize and report an information security incident.
- You will learn some of the consequences of mishandling personal information, both for you and for those whose information is involved.
- You will take quizzes at the end of each section to help you review what you've learned.

Reading through the Manual is one step towards developing a greater awareness of privacy. Think about what you can do to contribute to a culture that respects privacy in your workplace.

Section 1: Why Protect Privacy?

In This Section

You have various duties in your job with the State of Maryland. An important part of every State employee's job is protecting the personal information managed by your department. In this section, you will learn why protecting personal information – protecting privacy – is everyone's job.

It's the law!

Right To Privacy

The Constitutions of Maryland and of the United States guarantee a fundamental right to privacy.

Security Breaches

In recent years, the news has been filled with stories about companies and government agencies notifying individuals that their personal information was on a stolen laptop or involved in some other kind of security breach. The law requires notifying people of such breaches, to give them the opportunity to take steps to protect themselves from possible identity theft. Such incidents are expensive for a state department. In addition to the hard costs of mailing notices to large groups of people, the agency also faces a loss of public confidence.

Identity theft

Stealing personal information has become a popular way for dishonest people to make money. Law enforcement calls identity theft the crime of our times. It is a crime whose victims are harmed financially and in other ways. The growth of this crime in recent years puts an increased burden on all organizations, including state government, to protect the personal information in their care.

Public Trust

People entrust their most sensitive personal information – tax, financial, and medical information – to state agencies. In most cases, they have no choice. Consumers can choose another bank or store if they're not happy about how their personal information is handled. But they can't go to another DMV to get a driver's license, or to another Tax Board to pay their state taxes.

This places a special obligation on government employees. If we fail to protect personal information or to use it properly, we can undermine our citizens' faith in government. Protecting personal information means protecting people. It's a matter of public trust.

Test Your Knowledge of Section 1

1) TRUE OR FALSE: Protecting personal information is something that only banks and other companies have to be concerned about.

2) TRUE OR FALSE: If people don't trust a state department, they don't have to turn over their personal information in order to use a government service.

3) CHOOSE THE CORRECT ANSWERS: Which of the following are good reasons for a state department to protect privacy?

   a) The Constitution and state laws require it.

   b) Identity thieves want to steal personal information collected by state agencies.

   c) Responding to a privacy breach costs a state department.

   d) All of the above.

4) FILL IN THE BLANKS: Law enforcement calls _____ _____ the crime of our times.

Answers

1) False: See page 3.

2) False: See page 3.

3) D: See page 1 and 2.

4) Identity theft: See page 3.

Section 2: Identity Theft and Its Impact

In This Section

Identity theft is taking someone else's personal information and using it for an unlawful purpose. It is a serious crime with serious consequences. In this section, you will learn about the different types of identity theft and what they cost victims and businesses.

Types of Identity Theft

Existing accounts

There are several types of identity theft. The most common type is the use of an existing credit account. More than half of reported identity theft is the use of someone's existing credit card account.[1] Recovering from this type of identity theft has become fairly easy. If you discover a purchase you didn't make when reviewing your monthly credit card statement, you simply call your bank and follow up with a letter disputing the charge. It generally leads to the charge being removed. Federal law limits liability for an unauthorized credit card charge to $50 when you report it, and often there's no charge at all.[2]

New accounts

New account identity theft is when a thief uses information like your name and Social Security number to open new credit accounts. This type of identity theft can be much more difficult to deal with. The victim often doesn't find out for many months, perhaps when contacted by a debt

[1] All the statistics on identity theft cited in this Manual are from the Javelin Strategy study of January 2006, a random sample survey of 5,000 U.S. adults.

[2] Fair Credit Billing Act, 15 U.S. Code Section 1666.

collector. It takes many phone calls, letters, and hours of work to clear up this type of identity theft.

Employment & medical identity theft

An identity thief may use a victim's Social Security number when applying for work. This can lead to increased tax obligations for the victim. A thief may get medical treatment in the victim's name. Medical identity theft not only means unauthorized payments, but it can also pollute the victim's medical records with inaccurate information. This can put the victim at risk of receiving inappropriate medical treatment.

"Criminal" identity theft

"Criminal" identity theft is often the most difficult type to resolve. All identity theft is a crime, but the term "criminal" here means using someone else's identifying information when arrested or charged with a crime, thereby creating a criminal record for the victim. The victim may be repeatedly arrested, and then released following a fingerprint check. The victim may be unable to find work because of inaccurate information in a background report.

Identity Theft Facts

Between eight and nine million U.S. adults were victims of identity theft each year from 2005 to 2007.[3] That represents about 4% of adults, a high incidence for a crime.

According to law enforcement, identity theft is a low-risk, high-reward crime. The risks are low because a thief doesn't have to face his victim and because it's a non-violent crime with lower penalties than armed robbery. The reward is high, with an average of more than $5,000 for each identity theft incident, compared to less than $100 in a robbery.

Cost of Identity Theft

In 2006, the average victim spent $535 repairing the damage done by an identity thief. This includes costs such as postage for certified mail letters to creditors and credit bureaus, photocopying, and legal fees.

---

[3] Statistics on the incidence and cost of identity theft are from the Javelin Strategy& Research Survey Reports of 2007 and 2008.

It took 25 hours, on average, for a victim to clear up his or her situation. New account or criminal identity theft can amount to hundreds of hours of phone calls, letter writing, and office visits over many months, or even years.

The total cost of identity theft in the U.S. in 2007 was over $45 billion. Victims paid about $5 billion of this, and the rest was paid by merchants and financial institutions. Because consumers ultimately pay the business costs through higher prices for goods and services, we all pay for identity theft.

Test Your Knowledge of Section 2

1) TRUE OR FALSE: When an identity thief opens new credit accounts in the victim's name, the victim usually learns about it within a month.

2) FILL IN THE BLANK: Identity theft is stealing someone's personal information and using it for _____ purposes.

3) TRUE OR FALSE: The use of someone's personal information when charged with a crime can be the most difficult type of identity theft for a victim to deal with.

4) CHOOSE THE CORRECT ANSWER: Identity theft costs the average victim:

   a) $50 and 2 hours of work

   b) $5,700 and 20 hours of work

   c) $535 and 25 hours of work

   d) $100 and 5 hours of work.

5) TRUE OR FALSE: The total cost of identity theft in the U.S. in 2007 was $45 billion.

6) FILL IN THE BLANKS: A key type of information identity thieves use to open new accounts is someone's _____ _____ _____.

Answers

1) False: See page 6.
2) Unlawful: See page 6.
3) True: See page 7.
4) C: See page 7 and 8.
5) True: See page 8.
6) Social Security number. See page 6.

Section 3: State Government Privacy Laws

In This Section

This section gives an overview of the main privacy laws that apply to all Maryland state agencies. These are not the only laws on protecting personal information in government. There are state laws that protect specific kinds of personal information, such as HIV diagnoses, tax information, and driver's license information. There are also federal laws that apply to certain state agencies.

Information Practices Act

The basic privacy law that applies to all state agencies is the Maryland Personal Information Protection Act (MPIPA). This law sets the requirements for agencies on the management of personal information.

The MPIPA defines personal information as "any information that is maintained by a department that identifies or describes an individual." The broad definition includes information such as the following:

An individual's first and last name in combination with a:

- Social Security number
- Driver's License Number

- Financial Account Number
- Individual Taxpayer Identification Number
- Medical Information

The MPIPA allows agencies to collect only the personal information they are legally authorized to collect. Individuals have the right to see their own records and to request that any errors be corrected. It requires agencies to use reasonable safeguards to protect personal information against risks such as unauthorized access, use, or loss. We'll cover some examples of practices for safeguarding personal information in the next section of this Manual.

Public Records Act

The MPIPA interacts with the Maryland Public Information Act (MPIA). The MPIA makes most state records open to the public, with certain exceptions. The MPIPA requires protecting personal information, even when it is part of a record that is open to the public. That's why state agencies routinely black out or otherwise delete personal information before releasing public records. Check with your legal department or the Office of the Attorney General if you have questions.

Consequences

There are penalties for violating the MPIPA, both for a department, which may be sued, and for an employee, who may be disciplined.

- An individual may bring a civil action against a department that violates the Personal Information Protection Act if the violation results in an adverse impact on the individual.
- An employee who intentionally violates the Act may be subject to disciplinary action, including termination.
- An employee who willfully obtains a record containing personal information under false pretenses may be guilty of a misdemeanor, with a monetary penalty and/or prison.

Notice of Security Breach Law

Included in the Maryland Personal Information Protection Act (MPIPA) is the requirement that departments must notify people promptly if certain personal information is "acquired by an unauthorized person." Such a breach might be the loss or theft of a laptop containing personal information, an intrusion into a state computer system by a hacker, or the mailing of a disk containing information to the wrong person.

Warning of possible identity theft

The law was passed to alert people when their personal information may have fallen into the wrong hands, putting them at risk of identity theft. Someone who receives a notice of a breach can take steps to defend against the possibility of identity theft. For example, if your Social Security number is involved in a breach, you can place a fraud alert or a security freeze on your credit files, which will protect you from new accounts being opened using your information.

The personal information that triggers the notice requirement is the kind that identity thieves want. It is a name plus one or more of the following numbers:

- Social Security number
- Driver's license
- Financial account number, such as a credit card or bank account number
- Medical information
- Health insurance information

If the information is encrypted, or scrambled so that it is unreadable, there is no requirement to notify individuals.

State policy on notification

State policy requires agencies to notify individuals whenever an unauthorized person has acquired unencrypted personal information of the type listed above. This policy applies whether the information is in digital format, such as on a computer or CD, or in paper format, such as on an application or in a letter.

Social Security Number Protection Act

Key to the vault for identity thieves

The Social Security Number Protection Act seeks to protect against identity theft using Social Security numbers. With a name and a Social Security number, an identity thief can open new credit accounts and commit other financial crimes in the victim's name. This law applies to state agencies and to other entities in Maryland. It prohibits the public posting or display of Social Security numbers. It also specifically bans certain types of public posting – such as printing the number on ID cards, for example, health plan and student ID cards.

Test Your Knowledge of Section 3

1) TRUE OR FALSE: A state department can collect personal information for any reasonable purpose.

2) CHOOSE THE CORRECT ANSWERS: Which of the following are possible penalties for violating the Maryland Personal Information Protection Act?

   a) A State department could be sued.

   b) A State employee could be disciplined or fired.

   c) A State employee who steals a department's personal information could be fined and sentenced to prison.

   d) All of the above.

3) FILL IN THE BLANKS: The type of personal information that could trigger a notification if it is acquired by an unauthorized person is name, plus one or more of the following: Social Security number, driver's license or _____ _____ number.

4) TRUE OR FALSE: A Maryland law prohibits printing Social Security numbers on health plan cards.

5) TRUE OR FALSE: A folder containing job applications, which include the applicants' Social Security numbers, is stolen from a State employee's car. The employee's department does not have to notify individuals of this, because the information was not in digital or "computerized" format.

Answers

1) False: See page 12.

2) D: See pages 12 and 13.

3) Financial account: See page 13.

4) True: See page 14.

5) False: See page 13.

Section 4: Recommended Privacy Practices

In This Section

Protecting personal information from unauthorized access, use, disclosure, modification, or destruction is one way to protect individuals' privacy. In this section, you will learn about good – and bad – practices for protecting personal information.

The practices described are recommended for all state employees and also for contractors who handle personal information. They are for the person in the cubicle, in the office, in the mailroom, or the warehouse – wherever state workers do their jobs.

Some of these practices may not be appropriate for a particular work situation. If you think that is the case for your job, contact your department's Information Security Officer or your Privacy Officer, if you have one. They can help you with procedures that will allow you to work efficiently, while protecting personal information.

Personal, confidential, or sensitive information

These practices are intended to protect personal information – but they would also protect other kinds of confidential state information. In addition to personal information, your department has other kinds of confidential and sensitive information it must protect. This may include security-related information such as descriptions of your department's computer network configuration, some financial information, or drafts of policy documents.

Personal Information = Money

Treat personal information like cash!

Law enforcement tells us that personal information – especially information such as names and Social Security numbers – is worth money. There's a black market for it and identity thieves use the information to steal money.

If you thought of personal information as cash, you would probably handle it differently, wouldn't you? For example, would you leave a pile of $100 bills lying on your desk, even if you're away just for a short meeting or a break?

This is how we should all think of the personal information in our care.

Know Where Personal Information Is

Where do you keep personal information at your workplace? Consider especially information such as Social Security numbers, driver's license numbers, financial account numbers, and medical information.

The first step to protecting personal information is to know where it is. Take a look around your workstation. Remember to look for information on employees, as well as consumers, licensees, and others. Places to look include the following:

- Your desktop computer
- Your workstation file drawers
- Your laptop, BlackBerry, and other portable devices
- Floppy disks, CDs, authorized USB flash drives, and other data storage media

Do you download personal information onto your computer? Do you put printouts containing personal information in file folders while you're working on them, and then leave the file in an unlocked drawer

in your workstation? Do you have CDs or floppy disks with personal information on them?

Keep Personal Information Only As Long As Necessary

Once you've located where you keep personal information in your workstation, consider whether you really need to keep it all. There are some kinds of records that we're required to keep for legal and policy reasons. Check with your supervisor for your department's record retention policies. But there are probably lots of other files – paper and digital – that we don't need to keep beyond the period when we're working on them.

- Develop the habit of regularly purging documents with personal information from individual file folders.
- Avoid downloading from databases onto your computer.
- Regularly delete what you do download onto your computer when you've finished using it.
- Regularly remove personal information that you're no longer using from laptops, authorized USB flash drives, and other portable devices.

Dispose of Records Safely

One way that identity thieves steal personal information is by going through trash. It's called "dumpster diving." Shred documents with personal and other confidential information before throwing them away. You can shred CDs in most shredders, too.

- Don't throw documents containing personal information into your wastebasket or recycling bin – shred them.

- Putting a file in your computer's recycle bin doesn't completely delete it from your computer. To protect personal information, computers and hard drives must be "wiped" or overwritten in a special manner before discarding. Consult your department's Information Security Officer or Privacy Officer for more information.

Protect Personal Information from Unauthorized Access

Not everyone in an office needs to have access to all files and databases containing personal information. Access to personal information – especially information like Social Security numbers, driver's license numbers, financial account numbers, and medical information – should be limited to those who need to use it to perform their duties.

- Don't give access to coworkers who are not authorized.

- Don't share your user ID or password or your key to the file cabinet with others.

- When in doubt about someone's access privileges, check with your supervisor.

Protect Personal Information in Workstations

Don't download "free" software onto your computer – it may not really be free! It could contain hidden spyware. Spyware can slow

down the operation of your computer, send annoying pop-up ads, or introduce a virus into your department's network. One kind of spyware, called a "keylogger," can record all your keystrokes, sending your user ID, password and other confidential information to someone else.

- Lock your computer when you leave your workstation. A good way to remember this is to think "**control-alt-delete, before you leave your seat.**"

- Use strong passwords. Don't use obvious facts or numbers as your password – not your Social Security number, your spouse's, child's or pet's name, not a birth date or anniversary.

Stronger passwords are made up of at least eight characters, including letters, numbers, and symbols. One way to create a memorable password that others can't guess is to use the first letters of a sentence that has meaning to you, then substitute numbers or symbols for some letters.

For example, "How much wood could a woodchuck chuck?" could be "HMWC1WC2?" (Don't use this example as your password.)

Remember, your password is like your toothbrush: Change it often, and don't share it!

Protect Personal Information in Transit

Transmitting information electronically can make our work easier and more efficient. But some of them, as well as some traditional means, can pose privacy risks if not used properly.

Email

Think of email as a postcard. It isn't private. It's also very easy to mistype an email address and send the message to the wrong person. Don't use email to send or receive personal information like Social Security numbers, driver's license or State ID numbers, financial account numbers, or medical information. If you have a business need to use email for

personal information, contact your Information Security Officer or Privacy Officer. There may be procedures you can use to improve security.

Voice mail

Don't leave personal information in a voice mail message. You don't know who will pick up that message. Instead simply leave a message to call you back.

Regular mail

Use secure procedures for regular mail, which often contains personal information. Mail thieves are after personal information to commit identity theft.

Fax

Don't send personal information by fax, unless you use security procedures. You don't know how long a fax will remain on a machine or who might see it or pick it up. If you need to fax personal information, make special arrangements with the recipient. Arrange for and confirm prompt pick-up of the fax. Also check the accuracy of the fax number and take care when keying it in.

Protect State Information at Home and Away

- Don't take or send state records containing personal or other confidential information out of the office unless you are authorized to do so by your supervisor.

- If you are authorized to work on state records away from the office, use only a state approved laptop or other state approved equipment to work on the records.

Your home computer may not have adequate security protections. Your children or others in your household may have downloaded harmful software that could allow the information to be stolen. Your computer may be used by others who are not authorized to see state records.

Consider the breach that resulted when a U.S. Department of Veterans Affairs employee took home computers containing personal information on over 26 million veterans and other military personnel. His home was broken into and the computers were stolen. As a result, the VA had to notify all of those individuals at great expense, and the individuals experienced anxiety about the risk to their identities. Congress held hearings and several VA employees lost their jobs.

Beware of Social Engineering Schemes

Social engineering is stealing personal information by deception. Identity thieves try to trick people into disclosing personal information. One common form is what's known as "phishing" – an email that looks like it's from a bank or a government department. It may ask you to confirm your password, account number, or Social Security number. It often claims to be part of an effort to protect you from fraud. The advice to consumers on phishing – which can take place over the phone as well as by email – is never give out your personal information unless you initiated the contact.

As a state employee, you may find yourself the target of this type of identity theft attempt. It may be part of your job to give information, including personal information, to people who call and ask for it. Social engineering schemes also target businesses and government agencies, relying on workers' desire to provide good customer service.

How do you know people are who they say they are?

How do you know that people who ask you for personal information are authorized to have it? Because of concerns about social engineering, it's important to verify the identity and the authority of anyone who requests personal information. When the request is made in person, verification is usually done by asking to see a photo ID card. When the request is made by phone, other procedures must be used for verification before giving out personal information. If you're not sure about your department's verification procedures, ask your supervisor.

Report Information Security Incidents

In order to be able to maintain good information security – to protect the information people give to us – employees must recognize and report information security incidents promptly.

Be alert to incidents that could expose personal information to unauthorized access, use, disclosure, modification, or destruction. The following are examples of incidents to report:

- Loss or theft of a laptop, BlackBerry, CD or other device
- Loss or theft of paper records
- Mailing documents containing personal information to the wrong person
- Hacking into state computer systems

When in doubt, report it!

Promptly report any security incident that involves information to your department's Information Security Office or Privacy Officer.

A Matter of Respect

Protecting privacy is a matter of respect – respect for our fellow citizens and others who entrust us with their personal information, and respect for our co-workers, whose information is also in our care.

Protecting personal information is not something that can be done alone. We all touch some personal information in our offices and we are all responsible for protecting it. Protecting personal information is protecting people.

Test Your Knowledge: Review

1) A Public Information Act request is made for a state document that contains the home addresses and Social Security numbers of several consumers. Which one of the following statements is true?

   a) The document is public and must be provided "as is" to anyone who makes a Public Records Act request for it.

   b) Because the document contains personal information, it isn't public and should not be given in response to a Public Records Act request.

   c) The document may be provided in response to a Public Information Act request, but only after the Social Security numbers has been blacked out.

   d) The document is not a public record if you created it on your computer for your own use in doing your job.

2) If you believe that incoming mail has been stolen from your office, where should you report it FIRST?

   a) To your supervisor

   b) To your department's Information Security Officer or Privacy Officer

   c) To the U.S. Postal Inspection Service

   d) To the local police department

3) Which of the following is the strongest – most secure – password for access to your computer?

   a) FLUFFY

   b) 9151950

c) ERICKSON

d) HMWC1WC2?

4) Which of the following is the most secure way to get the Social Security numbers of seven people to a co-worker, who is on a business trip, is authorized to have the information, and needs it to do his job?

a) Send the information in an email.

b) Call your co-worker and give him the information over the phone.

c) Leave the information in a voice mail message on your co-worker's cell phone.

d) Fax the information to your co-worker at his hotel.

5) TRUE OR FALSE: If you delete files from your computer – and empty the recycle bin – that means the data in the files is erased.

6) Which of the following would NOT be an information security incident to report to your department's Information Security Officer?

a) Loss of a laptop containing unencrypted information

b) Accidental mailing of an individual's medical records to the wrong person

c) Theft of your purse, which contained a CD with state data on it

d) Theft of a state-owned electric stapler

7) Which of the following should you do before leaving your workstation for a meeting?

a) Put documents, disks, other records containing personal information (including your purse) in a drawer or otherwise out of sight.

b) Press "control-alt-delete" and lock your computer.

c) Call your best friend and have a long chat.

d) Both a and b.

8) A state employee gives a printout of the names, addresses, and driver's license numbers of people who received unemployment benefits to a friend who wants to offer jobs to them. Which of the following are true?

a) The employee may be found guilty of a misdemeanor punishable by a fine and prison.

b) The employee may be fired.

c) The employee's department may be sued.

d) The employee will not be punished because his intentions were good.

Answers

1) C: See page 12.

2) B: See page 24.

3) D: See page 21.

4) B: See pages 21 and 22.

5) False: See page 20.

6) D: See pages 21 and 22.

7) D: See page 22.

8) A, B, and C: See pages 12 and 13.

Section 5: Additional Privacy Resources

Information for State Government

- Privacy training materials and practice recommendations from the California Office of Privacy Protection.

  www.privacy.ca.gov/state_gov/index.html

- Information security policies, guidelines, procedures, tools, and best practices related to incident notification, security and privacy awareness, operational recovery, risk management, and other valuable resources from the State Information Security Office.

  www.doit.maryland.gov

Information for Consumers

Information sheets on identity theft, financial and health information privacy, protecting your home computer, and other privacy topics from the Maryland Office of the Attorney General.

www.oag.state.md.us/consumer/index.htm