

Appendix KK

A Checklist of Responsible Information-Handling Practices

*Case: A credit bureau mailed a credit report to a man who had requested it, and mistakenly included the credit report of a woman who had no connection to him. To make matters worse, the woman's credit report had been "flagged" by the credit bureau for security purposes.**

* All case studies reported in this fact sheet are true stories taken from the PRC hotline log.

Many privacy abuses are the result of errors and carelessness by those who handle personal information. Some are caused by inadequate security. Responsible information-handling practices begin with the development of privacy policies in the workplace and the implementation of regular training programs.

This checklist provides an overview of key points to consider when preparing information-handling policies and conducting privacy audits within your organization. The checklist can be used by private, public and not-for-profit organizations alike. Not all points will be relevant to your organization. Some situations may require you to take more stringent steps than those listed here, for example, the confidentiality requirements of medical records (1).

The citation numbers in the checklist refer to the Resources section at the end of the checklist. For example, (1) refers to the first source listed in the references section.

The checklist is divided into two sections. Section I lists the major issues to consider when drafting privacy principles to safeguard the personal information of your clients, users, members, customers, and so on. Section II includes considerations for the development of intra-organizational privacy policies concerning employee records, electronic monitoring, and electronic mail.

I. DEVELOPMENT OF PRIVACY POLICIES TO GUIDE CUSTOMER / CLIENT RELATIONS

A. Organizational Policies

1. Does your organization/company/agency have policies which outline its privacy practices and expectations for handling the personal information of your clients, customers, users, members and/or listees? (9) (12) (15) (19)
2. Are your organization's privacy policies communicated regularly--in employees' initial training sessions, in regular organization-wide training programs, in employee handbooks, on posters and posted signs, on company intranet and Internet web sites, in brochures available to clients? Are all employees who handle personal information included in the training programs, including temporary employees, back-up personnel, and contract staff?

B. Privacy Principles

The major components of effective privacy policies are listed here, adapted from the fair information practices developed by the Organization for Economic Cooperation and Development (OECD). Although designed to guide the development of national privacy legislation (14), these principles are also appropriate for organizations.

1. **Openness.** There should be a general practice of openness about practices and policies with respect to personal information. Means should be available to establish the existence and nature of personal information and the main purposes of its use.
2. **Purpose specification.** The purpose for collecting personal information should be specified at the time of collection. Further uses should be limited to those purposes.
3. **Collection limitation.** The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of the subject. Only that information necessary for the stated purpose should be collected, nothing more.
4. **Use limitation.** Personal information should not be disclosed for secondary purposes without the consent of the subject or by authority of law.
5. **Individual participation.** Individuals should be allowed to inspect and correct their personal information. Whenever possible, personal information should be collected directly from the individual.
6. **Quality.** Personal information should be accurate, complete and timely, and be relevant to the purposes for which it is to be used.

7. **Security safeguards.** Personal information should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure. Access to personal information should be limited to only those within the organization with a specific need to see it.
8. **Accountability.** Someone within the organization, such as the Chief Privacy Officer or an information manager, should be held accountable for complying with its privacy policy. Privacy audits to monitor organizational compliance should be conducted on a regular basis, as should employee training programs. (11)

There are many variations of fair information principles. The industry group Online Privacy Alliance, for example, has developed a set of principles for use on web sites. (13) Industry-oriented policies often lack such key principles as purpose specification, use limitation, and accountability. See also web site seal programs: TRUSTe, BBBOnline, and WebTrust. (18)

C. Data and Network Security

Security of personally identifiable information, whether stored in electronic, paper or micro-graphic form, is the topic of many books (19), journals, trade magazines, and conferences. Only the major points are listed here. For additional information, consult professional and trade associations (4) (10), as well as libraries, your nearest technical bookstore, and the Web.

1. Do you have staff specifically assigned to data security? Do staff members participate in regular training programs in order to keep abreast of technical and legal issues?
2. Is physical access restricted to computer operations and paper/micrographic files which contain personally identifiable information? Do you have procedures to prevent former employees from gaining access to computers and paper files?
3. Are sensitive files segregated in secure areas/computer systems and available only to qualified persons?
4. Do you have audit procedures and strict penalties in place to prevent telephone fraud and theft of equipment and information?
5. Do all employees follow strict password and virus protection procedures? Are employees required to change passwords often, using "foolproof" methods?
6. Is encryption used to protect sensitive information (a particularly important measure when transmitting personally-identifiable information over the Internet)?
7. Do you regularly conduct systems penetration tests to determine if your systems are hacker proof?

8. If your organization is potentially susceptible to industrial espionage, have you taken extra precautions to guard against leakage of information? (3)
9. Does your organization conduct employment background checks, especially for persons who have access to sensitive information? If so, is the organization in compliance with federal and state laws regarding "investigative consumer reports?" (8)

D. Some Additional "Common Sense" Security Practices

Case: A medical office photocopied more of a car accident victim's record than necessary and released extremely sensitive but irrelevant information to the insurance company. Information about the woman's child, given up for adoption 30 years ago, eventually became part of the court record, a public document.

1. When providing copies of information for others, do employees make sure that nonessential information is removed and that personally identifiable information which has no relevance to the transaction is either removed or masked (the process of "redacting" or "severing" the record)?
2. Are employees trained never to leave computer terminals unattended when personally identifiable information is on the screen? Do you use password-activated screen-saver programs?
3. Are all employees who handle personal information--including temporary, back-up and contract staff--trained to be able to detect when they are being "pumped" for personal information by unauthorized and unscrupulous persons? "Pretext" interviews, also known as "social engineering," are more common than might be expected and are the stock in trade of persons bent on finding out confidential personal information to which they are not entitled.

E. Records Retention and Disposal

Case: An automobile dealer did not shred its loan applications before tossing them into the garbage. A "dumpster diver" retrieved one and used the financial information to commit thousands of dollars of fraud against someone who had applied for a car loan.

1. Does your organization have a records retention/disposal schedule for personally identifiable information, whether stored in paper, micrographic or magnetic/ electronic (computer) media? (1) (5)
2. When disposing of computers, diskettes, magnetic tapes, CD-ROMs, hard drives and any other electronic media which contain personally identifiable materials, are all data erased with a proven utility program and/or physically destroyed?

3. When disposing of waste and recycling paper, are all documents which contain personally identifiable information placed in secure padlocked containers or shredded? Does your recycling company certify its disposal/destruction methods? Is it bonded?

F. Facsimile Transmission

Case: A medical doctor who was filing for bankruptcy faxed a financial document to his attorney. He entered the wrong telephone number, and the document was instead transmitted to the local newspaper.

1. Is the fax machine in a supervised area, off limits to unauthorized persons? Is use restricted to authorized personnel only?
2. Is the fax machine used exclusively for sending nonconfidential materials?
3. When sending documents, do all users complete a cover sheet which indicates the sender's and receiver's names, addresses and telephone numbers?
4. When confidential materials are sent, is notice of their confidential nature indicated on the cover sheet?
5. Do users always check the receiver's telephone number before transmitting documents? Do users compare the number displayed with number being called to check for errors? Do users check the transmission report after the fax has been sent?
6. When transmitting confidential materials, is the recipient notified in advance that the document is being sent? Does the sender check with the receiver to make sure the document has been received?

G. Answering Machines and Voice Mail Systems

Case: Message left on the wrong answering machine when the phone number was misdialed: "Hello Mrs. Weaver. This is Judy from the County Parole Office. You called earlier about your daughter Crystal? She has already been taken to the California Youth Authority [juvenile detention center]."

1. Are precautions taken for situations when confidential and highly sensitive messages are expected to be left on answering machines or voice mail systems? Is the number of the call recipient verified for accuracy? Is permission asked of the intended call recipient to leave confidential messages? Are non-specific messages left when prior permission has not been obtained from the call recipient?

H. Wireless Communications

Case: As people stood in line to enter the theater, the cellular phone conversation of one theater-goer was overheard by those nearest her. It soon became obvious that the woman was a medical doctor, talking about the care of a patient.

Conversations on cellular and cordless phones are vulnerable to eavesdropping because the signals are transmitted over radio waves. Anyone with a radio scanner can listen to your conversations unless you use newer mode digital devices that use encrypted data transmission and/or a transmission technology that cannot be deciphered by common radio scanners.

1. Are wireless phones strictly forbidden for conversations involving confidential information (for example, a patient's medical care or a law suit) unless secure digital models are used?
2. Are wireless phone users cautioned to talk out of earshot of others nearby who might hear their half of the conversation?

I. Portable Computers and Work-at-Home Situations

1. Does the organization have policies and procedures for safeguarding personally identifiable information when transported outside of the office by portable computers and hand-held personal organizers?
2. For employees who work at home, including temporary and contract staff, does the organization have policies, procedures and training programs which emphasize responsible information-handling practices?
3. Is the network connection between home and work secure?

J. Social Security Numbers (SSNs) and the Use of Personal Identifiers

Case: The supervisor of a unit within a large state government agency sent an electronic mail message to every employee, listing all their names and Social Security numbers, disregarding the privacy and fraud implications of releasing that information.

The use of SSNs for record-keeping purposes and personal identifiers should be strongly discouraged, and preferably prohibited. Proliferation of SSNs puts customers and employees at risk of allowing unscrupulous persons to obtain the number for fraudulent purposes, for example, obtaining credit card accounts in another person's name. (See the Privacy Rights Clearinghouse identity theft publications, www.privacyrights.org/identity.htm.)

1. If the organization uses the SSN as a record-keeping number, does it offer its clients and/or employees the option of using an alternative number?

2. Does the organization have a strict policy prohibiting the display of SSNs on any documents that are widely seen by others, for example, time cards, parking permits, employee rosters, mailing labels, paycheck stubs, health insurance cards?
3. If the organization requires an access code for certain transactions (i.e., ATM cards, computer access, phone banking, security system codes, building access cards, passwords), does it prohibit the use of SSNs, or any part of the SSN such as the last four digits, as personal identifier numbers?

K. List Security Guidelines

Case: Before departing the singles dating service office, a fired employee stole a computer diskette containing the supposedly confidential mailing list of all its clients. He sold the list to other dating services in the area.

Does your organization maintain information on clients, customers, potential customers, users, and/or members? Does your organization make its lists available to other entities by selling, renting, or exchanging them? If so, the Direct Marketing Association (DMA) recommends that the following guidelines be practiced. These are adapted from DMA's "Fair Information Practices Checklist." (6) The use of the word "customer" below can be altered to fit your specific situation; it can apply to "clients," "members" and "users" alike.

1. Opt-out program

- a. Does your organization offer its customers name removal options? Are they effectively communicated?
- b. Do you subscribe to the DMA's name removal services, the Mail Preference Service (MPS) its Telephone Preference Service (TPS), and/or its E-mail Preference Service (EMPS)? (6) Are MPS, TPS, and EMPS names removed prior to list rentals or exchanges?

2. Security practices

- a. Is someone in your organization responsible for list security? Is someone responsible for keeping up to date on current laws and regulations regarding fair information practices?
- b. Are your lists physically secure?
- c. Are there sufficient restrictions on your employees to protect against unauthorized access, [for example, audit trails, strict penalties for violation]?
- d. Does your organization instruct its employees that customer data are confidential [in initial employee orientations and ongoing training programs]?
- e. Does the organization have adequate security to prevent remote access to your lists via computer?
- f. Does your organization ensure that list recipients employ sufficient safeguards? Does your organization make sure that security measures are in place during the

transfer of lists? Do you ensure the secure and timely return or destruction of lists used by other entities? Do you use a monitoring system to track list usage [such as the use of decoy names, called “seeding”]?

3. Use of marketing data

- a. Is your organization collecting only those consumer data that are pertinent and necessary for the purpose at hand?
- b. Are you sensitive to a consumer's expectation that some personal information may be considered confidential and should not be used for marketing?
- c. If your organization contributes customer data to a cooperative database, are you satisfied about the database's security?

4. Data accuracy

- a. Does your organization have the means to update its customer data?
- b. Are customer data reviewed/revise by your organization on a regular basis?
- c. Are customer inquiries regarding data accuracy answered promptly and to the customer's satisfaction?

5. Additional tips

The Privacy Rights Clearinghouse suggests these additional list security guidelines:

- a. Do you disclose up-front the intended uses of the data that are collected?
- b. Do you allow the data subjects to inspect and correct data held about them?

II. DEVELOPMENT OF PRIVACY POLICIES TO GUIDE EMPLOYEE RELATIONS

A. Inhouse Organizational Privacy Policies

1. Does your organization/company/agency have policies for handling the personal information of your employees? Such policy statements typically concern hiring procedures, personnel records, medical records, discipline procedures, electronic mail usage, electronic monitoring, and Internet access.

This document focuses on electronic mail/voice mail and electronic monitoring. (7) (9) (12) (15) (19)

B. Electronic Mail (E-Mail) and Voice Mail Systems

Case: Charles was absent from work for a month on disability leave. Upon his return, he was shocked to discover that his supervisor had changed his password and listened to his voice mail messages.

1. Does your organization have a policy regarding the privacy expectations of its employees, as well as any third party users (i.e., clients, customers), who use the e-mail and/or voice mail systems? Are those policies effectively communicated to all employees and third-party users? Points to include in your policy:
 - a. the purpose for which the system is to be used (business only? personal matters allowed? no trade secrets discussed?);
 - b. penalties for misuse;
 - c. who is authorized to access e-mail/voice mail messages; the disposition of e-mail/voice messages when the employee is on temporary but extended leave;
 - d. the retention/purge schedule for files, including retention procedures for possible use as legal evidence;
 - e. expectations for privacy (none? only in files marked "private"?);
 - f. password creation/change procedures;
 - g. the use of encryption (prohibited? allowed? required for sensitive communications?);
 - h. safeguards concerning copying and forwarding messages, especially messages containing personally identifiable data;
 - i. how the policy is communicated; employee notice and training programs.

C. Electronic Monitoring

An increasing number of employers are using a variety of employee monitoring practices: telephone systems which allow supervisors to listen to telephone calls, computer keystroke monitoring systems which can determine work productivity, web-surfing monitoring, video monitoring systems, and locational detectors.

1. Does the organization have a policy that states the types of monitoring being conducted, the purposes of monitoring, and the uses made of monitoring data?
2. Does the policy include procedures to safeguard sensitive personal information encountered in the process of monitoring?
3. Is this policy communicated to all employees at time of hiring and in ongoing training programs?
4. Does the policy include provisions for employees to appeal adverse decisions based on data collected by the monitoring system?
5. If telephone monitoring is being conducted, does the organization provide telephones that are not monitored which can be used for personal calls (at least pay-phones)?

Resources

1. American Health Information Management Association, 233 N. Michigan Ave. #2150, Chicago, IL 60601. (312) 233-1100. Its newsletter, *In Confidence*. Web: www.ahima.org
2. American Management Association (AMACOM). 1601 Broadway, New York, NY 10019. (212) 586-8100. See authors Hubbartt and Overly below. Web: www.amanet.org
3. American Society for Industrial Security, 1625 Prince St., Alexandria, VA 22314. (703) 519-6200. Web: www.asisonline.org
4. Association for Computing Machinery, 1515 Broadway, New York NY 10036. (800) 342-6626. Web: www.acm.org
5. Association of Records Managers and Administrators, ARMA International, 13725 W. 109th St., Lexesa, KS 66215. (913) 341-3808. Web: www.arma.org
6. Direct Marketing Association, 1120 Avenue of the Americas., New York, NY 10036-6700. (212) 768-7277. Web: www.the-dma.org
7. Electronic Messaging Association (now The Open Group), *EMA Privacy Policy Toolkit: Access to, Use, and Disclosure of Electronic Messaging on Company Computer Systems in the 21st Century*. (June 2000) Web: www.ema.org/restricted/documents/index.htm
8. Federal Trade Commission, "Using Consumer Reports: What Employers Need to Know." Web: www.ftc.gov/bcp/online/pubs/buspubs/credempl.htm
9. Hubbartt, William S. *The New Battle Over Workplace Privacy*. (New York: American Management Assoc., 1998). Web: www.amanet.org
10. Institute of Electrical and Electronics Engineers, 3 Park Ave., 17th Fl., New York, NY 10016. (212) 419-7900. Web: www.ieee.org
11. International Association of Privacy Officers, 1211 Locust St., Philadelphia, PA 19107. (800) 266-6501. Web: www.privacyassociation.org
12. Lotito, Michael J. and Lynn C. Outwater. *Minding Your Business: Legal Issues and Practical Answers for Managing Workplace Privacy*. (Society for Human Resource Management, 1997) Web: www.shrm.org
13. Online Privacy Alliance, Hogan and Hartson, 555 13th St. NW, Washington, DC 20004. (202) 637-5600. Web: www.privacyalliance.com
14. Organisation for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. (202) 785-6323. Web: www.oecd.org
15. Overly, Michael R. *E-Policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets*. (New York: American Management Assoc., 1999). Web: www.amanet.org
16. Privacy and American Business, 2 University Plaza, # 414, Hackensack, NJ 07601. (201) 996-1154. Web: www.pandab.org and www.privacyexchange.org
17. Society for Human Resource Management, 1800 Duke St., Alexandria, VA 22314. (703) 548-3440. See author Lotito above. Web: www.shrm.org
18. Web privacy seal programs: Web sites: www.bbbonline.org, www.truste.org, and www.webtrust.org
19. Wood, Charles Cresson. *Information Security Policies Made Easy: A Policy Construction Kit*. Baseline Software. Contains over 1,100 already written policies in a printed manual and CD-ROM. (800) 829- 9955. Web: www.baselinesoft.com

Fact Sheet 12: Information-Handling Practices

Copyright © 1995-2002. Utility Consumers' Action Network / Privacy Rights Clearinghouse
Jan. 1995, Revised May 2002

This copyrighted document may be copied and distributed for nonprofit, educational purposes only. The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse. This fact sheet should be used as an information source and not as legal advice. It was originally developed under the auspices of the University of San Diego.

Privacy Rights Clearinghouse
3100 – 5th Ave., Suite B
San Diego, CA 92103

Voice: (619) 298-3396
Fax: (619) 298-5681
E-mail: prc@privacyrights.org
Web: www.privacyrights.org

Source: Used with permission, May 2002.