

1 Fair Information Practices [U.S. Dept. of Health, Education and Welfare, 1973]  
 2 =====  
 3  
 4 1. Collection limitation.  
 5  
 6 There must be no personal data record keeping systems whose very  
 7 existence is secret.  
 8  
 9 2. Disclosure.  
 10  
 11 There must be a way for an individual to find out what information  
 12 about him is in a record and how it is used.  
 13  
 14 3. Secondary usage.  
 15  
 16 There must be a way for an individual to prevent information about  
 17 him that was obtained for one purpose from being used or made  
 18 available for other purposes without his consent.  
 19  
 20 4. Record correction.  
 21  
 22 There must be a way for an individual to correct or amend a record  
 23 of identifiable information about him.  
 24  
 25 5. Security.  
 26  
 27 Any organization creating, maintaining, using, or disseminating  
 28 records of identifiable personal data must assure the reliability  
 29 of the data for their intended use and must take precautions to  
 30 prevent misuse of the data.  
 31  
 32  
 33  
 34  
 35  
 36  
 37  
 38  
 39  
 40  
 41  
 42  
 43  
 44  
 45  
 46  
 47  
 48  
 49  
 50  
 51  
 52  
 53  
 54  
 55  
 56  
 57  
 58  
 59  
 60  
 61  
 62  
 63  
 64  
 65  
 66  
 67  
 68  
 69  
 70  
 71  
 72  
 73

74 Privacy Guidelines [Organization of Economic Cooperation and Development, 1980]  
 75 =====  
 76  
 77 1. Collection Limitation.  
 78  
 79 There should be limits to the collection of personal data and any  
 80 such data should be obtained by lawful and fair means and, where  
 81 appropriate, with the knowledge or consent of the data subject.  
 82  
 83 2. Data quality principle.  
 84  
 85 Personal data should be relevant to the purposes for which they are  
 86 to be used, and, to the extent necessary for those purposes, should  
 87 be accurate, complete and kept up-to-date.  
 88  
 89 3. Purpose specification.  
 90  
 91 The purposes for which personal data are collected should be  
 92 specified not later than at the time of data collection and the  
 93 subsequent use limited to the fulfilment of those purposes or such  
 94 others as are not incompatible with those purposes and as are  
 95 specified on each occasion of change of purpose.  
 96  
 97 4. Use limitation principle.  
 98  
 99 Personal data should not be disclosed, made available or otherwise  
 100 used for purposes other than those specified in accordance with  
 101 Paragraph 9 except:  
 102  
 103 (a) with the consent of the data subject; or  
 104  
 105 (b) by the authority of law.  
 106  
 107 5. Security safeguards principle.  
 108  
 109 Personal data should be protected by reasonable security safeguards  
 110 against such risks as loss or unauthorized access, destruction,  
 111 use, modification or disclosure of data.  
 112  
 113 6. Openness principle.  
 114  
 115 There should be a general policy of openness about developments,  
 116 practices and policies with respect to personal data. Means should  
 117 be readily available of establishing the existence and nature of  
 118 personal data, and the main purposes of their use, as well as the  
 119 identity about usual residence of the data controller.  
 120  
 121 7. Individual participation principle.  
 122  
 123 An individual should have the right:  
 124  
 125 (a) to obtain from a data controller, or otherwise, confirmation  
 126 of whether or not the data controller has data relating to  
 127 him;  
 128  
 129 (b) to have communicated to him, data relating to him  
 130  
 131 1. within a reasonable time;  
 132 2. at a charge, if any, that is not excessive;  
 133 3. in a reasonable manner; and  
 134 4. in a form that is readily intelligible to him;  
 135  
 136 (c) to be given reasons if a request made under subparagraphs (a)  
 137 and (b) is denied, and to be able to challenge such denial;  
 138  
 139 (d) to challenge data relating to him and, if the challenge is  
 140 successful, to have the data erased; rectified, completed or  
 141 amended.  
 142  
 143 8. Accountability principle.  
 144  
 145 A data controller should be accountable for complying with measures  
 146 which give effect to the principles stated above.

147 CSA Model Code for the Protection of Personal Information  
 148 =====  
 149 [Canadian Standards Association, 1995]  
 150  
 151 "The need for privacy protection in the absence of privacy laws for  
 152 the private sector has led the Canadian Standards Association (CSA) to  
 153 develop a generic privacy code ... which private-sector organizations  
 154 could use as a model. What is novel about the CSA's approach is that,  
 155 although the code is voluntary, an attempt has been made to build in  
 156 an oversight mechanisms to address the historic lack of enforcement of  
 157 voluntary codes. ...  
 158  
 159 The CSA privacy code, like most, is modeled on the OECD guidelines,  
 160 except that it strengthens two components: "consent" by having it  
 161 stand alone as a completely separate principle, and "challenging  
 162 compliance," which strengthens a person's right to challenge an  
 163 organizations' compliance with any of the principles, not simply  
 164 refusals of access of the accuracy of the collected data. As well,  
 165 accountability was considered to be so fundamental that it was placed  
 166 first in the list of 10 principles."  
 167  
 168 [Update Feb. 2004: The CSA privacy code has since been codified into  
 169 law, the Personal Information Protection and Electronic Documents  
 170 Act. It came into effect in 2001, with the health provisions  
 171 implemented in 2002, and commercial activities covered as of January  
 172 2004. For more information, [www.privcom.gc.ca/](http://www.privcom.gc.ca/)]  
 173  
 174  
 175  
 176  
 177  
 178  
 179  
 180  
 181  
 182  
 183  
 184  
 185  
 186  
 187  
 188  
 189  
 190  
 191  
 192  
 193  
 194  
 195  
 196  
 197  
 198  
 199  
 200  
 201  
 202  
 203  
 204  
 205  
 206  
 207  
 208  
 209  
 210  
 211  
 212  
 213  
 214  
 215  
 216  
 217  
 218  
 219

220 1. Accountability.  
 221  
 222 An organization is responsible for personal information under its  
 223 control and shall designate a person who is accountable for the  
 224 organization's compliance with the following principles.  
 225  
 226 2. Identifying purposes.  
 227  
 228 The purposes for which personal information is collected shall be  
 229 identified by the organization at or before the time the  
 230 information is collected.  
 231  
 232 3. Consent.  
 233  
 234 The knowledge and consent of the individual are required for the  
 235 collection, use or disclosure of personal information except where  
 236 inappropriate.  
 237  
 238 4. Limiting collection.  
 239  
 240 The collection of personal information shall be limited to that  
 241 which is necessary for the purposes identified by the  
 242 organization. Information shall be collected by fair and lawful  
 243 means.  
 244  
 245 5. Limiting use, disclosure and retention.  
 246  
 247 Personal information shall not be used or disclosed for purposes  
 248 other than those for which it was collected except with the consent  
 249 of the individual or as required by law. Personal information shall  
 250 be retained only as long as necessary for the fulfilment of those  
 251 purposes.  
 252  
 253 6. Accuracy.  
 254  
 255 Personal information shall be as accurate, complete and up-to-date  
 256 as is necessary for the purposes for which it is to be used.  
 257  
 258 7. Safeguards.  
 259  
 260 Personal information shall be protected by security safeguards  
 261 appropriate to the sensitivity of the information.  
 262  
 263 8. Openness.  
 264  
 265 An organization shall make readily available to individuals  
 266 specific information about its policies and practices relating to  
 267 its handling of personal information.  
 268  
 269 9. Individual access.  
 270  
 271 Upon request, an individual shall be informed of the existence, use  
 272 and disclosure of personal information about the individual and  
 273 shall be given access to that information. An individual shall be  
 274 able to challenge the accuracy and completeness of the information  
 275 and have it amended as appropriate.  
 276  
 277 10. Challenging compliance.  
 278  
 279 An individual shall be able to challenge compliance with the above  
 280 principles with the person who is accountable within the  
 281 organization.