| Original Version—May 25, 1994 | Revised Version | Change |
|---|--|--|
| B. Information Integrity Principles | | |
| Participants in the NII rely upon the integrity of the information it contains. It is therefore the responsibility of all participants to ensure that integrity. In particular, participants in the NII should, to the extent reasonable: | Personal information should not be improperly altered or destroyed. | Principle has been revised to focus on tradi- tional security definition of data integrity— guarding against improper alteration or de- struction. Data quality attributes provisions have been moved to new principle: Informa- tion Quality Principle, below. |
| Ensure that information is secure, using whatever means are appropriate; Ensure that information is accurate, timely, complete, and relevant for the purpose for which it is given. | | |
| C. Information Quality Principle (NEW) | | |
| (Partly contained in Information Integrity Prin- ciple.). | Personal information should be accurate, timely, complete, and relevant for the pur- pose for which it is provided and used. | New principle, but broken out of old Integrity. |

OLD II. Principle for Information Collectors (i.e. entities that collect personal information directly from the individual)— This principle has been deleted and its provisions moved to the Information Users Principles as the new "Notice Principle."

| Original Version—May 25, 1994 | Revised Version | Change |
|--|-----------------|--|
| A. Collection Principle Before individuals make a decision to provide personal information, they need to know how it is intended to be used, how it will be pro- tected, and what will happen if they provide or withhold the information. Therefore, col- lectors of this information should tell the indi- vidual why they are collecting the informa- tion, what they expect it will be used for, what steps they will take to protect its con- fidentiality and integrity, the consequences of | | Principle moved to and combined with the Principles for Information Users. |
| fidentiality and integrity, the consequences of providing or withholding information, and any rights of redress. | | |

New II. Principles for Information Users (i.e. Information Collectors and entities that obtain, process, send or store personal information).

| Original Version—May 25, 1994 | Revised Version | Change |
|--|--|--|
| A. Acquisition and Use Principles | | |
| Users of personal information must recognize and respect the stake individuals have in the use of personal information. Therefore, users of personal information should: | Users of personal information should recog- nize and respect the privacy interests that individuals have in the use of personal in- formation. They should: | The assessment in paragraph 1, now pre- cedes a decision to collect data, not merely the data collection itself. |
| Assess the impact on personal privacy of current or planned activities before obtaining or using personal information. | 1. Assess the impact on privacy of current or planned activities in deciding whether to obtain or use personal information. | The original paragraph 3, placing responsibil- ities on users to assure data quality has been moved to the Information Quality Prin- ciple in Section I to emphasize that this is a responsibility of all parties. |
| Obtain and keep only information that could reasonably be expected to support current or planned activities and use the information only for those or compatible purposes. Assure that personal information is as accurate, timely, complete and relevant as necessary for the intended use | Obtain and keep only information that could be reasonably expected to support current or planned activities and use the informa- tion only for those or compatible uses. | |

B. Notice Principle (This is a new principle for this section. It recognizes that notice is a critical element in the successful establishment of the Principles as a working set of guidelines. Adequate notice will ensure that information acquisition and usage occurs within the knowledge and consent of the individual who provides it. Because users may wish to use information for purposes that are incompatible with that knowledge and consent, the principle states that before such use can occur, the individual must be renotified and his or her consent obtained.)