Users of personal information should take reasonable steps to prevent the information they have from being disclosed or altered improperly. Such users should use appropriate managerial and technical controls to protect the confidentiality and integrity of personal information.

27. On the NII, personal information is maintainted in a networked environment, an environment that poses tremendous risk of unauthorized access, disclosure, alteration, and destruction. Both insiders and outsiders may gain access to information they have no right to see, or make hard-to-detect changes in data that will then be relied upon in making decisions that may have profound effects.

28. For example, our national health care system expects to become an intensive participant in the NII.

Through the NII, a hospital in a remote locale will be able to send x-rays for review by a renowned radiologist at a teaching hospital in another part of the country. The benefits to the patient are obvious. Yet, such benefits will not be reaped if individuals refuse to send such sensitive data because they fear that the NII lacks safeguards needed to ensure that sensitive medical data will remain confidential and unaltered.

29. In deciding what controls are appropriate, information users should recognize that personal information should be protected in a manner commensurate with the harm that might occur if it were improperly disclosed or altered. Also, personal information collected directly from the individual should be protected in accordance with the information provided to the individual pursuant to the Notice Principle (II.B).

30. Finally, technical controls alone cannot provide adequate protection of personal information. Although technical safeguards are well-suited to protect against unauthorized outsiders, they are less well suited to protect against insiders who may be able to alter or delete data improperly without breaching any technical access controls. Therefore, to protect personal information, information users should adopt a multi-faceted approach that includes both managerial and technical solutions. One management technique, for example, could strive to create an organizational culture in which individuals learn about fair information practices and adopt these practices as the norm.

II.D. Fairness Principle: Individuals provide personal information on the assumption that it will be used in accordance with the notice provided by collectors. Therefore, users of personal information should enable individuals to limit the use of their personal information if the intended use is incompatible with the notice provided by collectors.

31. Two principles work together to ensure the fair use of information in the NII. The Acquisition and Use Principle (III.A.2) requires information users to use personal information only for current or planned activities or for compatible uses. In conjunction with this principle, the Fairness Principle requires users to enable individuals to limit incompatible uses of personal information. Juxtaposed, these two principles highlight again the interactive and interrelated relationships on the NII, which require participants to share the power and responsibility for the proper use of personal information.

32. An incompatible use occurs when personal information is used in a way neither reasonably contemplated nor consented to by the individual when the information was collected. As explained earlier, the scope of this consent depends principally on the notice provided by the information collector pursuant to the Notice Principle (II.B) and obtained by the individual pursuant to the Awareness Principle (III.A).

33. An incompatible use is not necessarily a harmful use; in fact, it may be extremely beneficial to the individual and society. For example, society may benefit when researchers and statisticians use previously collected personal information to determine the cause of a potentially fatal disease such as cancer.

34. On the other hand, without some limitation, information use may know no boundaries. Without a Fairness Principle, personal information provided under the terms disclosed and obtained pursuant to the Notice (II.B) and Awareness (III.A) Principles may be used in ways that violate those terms and thus go beyond the individual's understanding and consent. To guard against this result, before information is used in an incompatible manner, such use should be communicated to the individual and his or her explicit or implicit consent obtained. The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate. It is the responsibility of the

data user to ensure that the individual is able to prevent such incompatible use. Implicit in this principle is the idea that the original data collector will convey to every new user information about the original notice.

35. Having said this, it must be recognized that the Fairness Principle cannot be applied uniformly in every setting. There are some incompatible uses that will have no effect on the individual's information privacy interest. Research and Statistical studies may be an example. Obtaining the consent of the individual to participate in such studies will add cost and administrative complexity to the process without affecting the individual's information privacy interests. In other cases, the information is for a significant public need that would be thwarted by giving the individual a chance to limit its use, and society recognizes the need and authorizes the use in a highly formal, open way (typically in legislation). An example would be the collection of data to support a law enforcement investigation where obtaining a suspect's consent to a new use of what has become investigatory data would be unlikely and even asking for such consent could be potentially counterproductive to the investigation. Nevertheless, given the interactive possibilities that the NII offers, data users should be creative about finding ways to satisfy the Fairness Principle.

II.E. Education Principle:

The full effect of the NII on the use of personal information is not readily apparent, and individuals may not recognize how their lives may be affected by networked information. Therefore, information users should educate themselves, their employees, and the public about how personal information is obtained, sent, stored, processed, and protected, and how these activities affect individuals and society.

36. The Education Principle represents a significant addition to the traditional Code of Fair Information Practices. There are many uses of the NII for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activity outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.