Principles

Markle Guiding Principles

Nine principles that provide a multi-layered approach that should be built into any information-sharing system or network in order to ensure confidentiality and privacy of patient data.

1. **Openness and Transparency**. Protecting privacy requires a broad and universal policy and practice of transparency and openness about the developments, practices and policies with respect to the way personal data is handled. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
2. **Individual Participation and Control.** Individuals should control and have the right to:
    - Obtain from a data controller confirmation of whether or not the data controller has data relating to him/her;
    - Have communicated personal data relating to him/her within a reasonable time (at an affordable charge, if any) that is readily intelligible;
    - Be given reasons if a request is denied and to be able to challenge such denial;
    - Challenge data relating to him/her and have personal data erased, rectified, completed or amended.
3. **Purpose Specification and Minimization.** The purposes for which personal data are collected (and accessed) should be specified in a timely manner and the subsequent use limited to the fulfillment of those purposes (as are specified on each occasion of change of purpose).
4. **Collection Limitation**. Personal data should only be obtained and collected by lawful and fair means and, when appropriate, with the knowledge or consent of the data subject.
5. **Use Limitation.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.
6. **Data Integrity and Quality.** Personal data should be relevant to the purposes for which they are be used and should be accurate, complete, relevant and kept-up-to-date.
7. **Security Safeguards and Controls.** Reasonable security safeguards must be built to protect against data loss, unauthorized access and modification, destruction, use, or other threats to data in a networked environment.
8. **Accountability and Oversight.** Violators and data controllers should be held accountable for complying with measures that give effect to the principles stated above.
9. **Remedies.** Legal and financial remedies must exist to address any security breaches or privacy violations.

Online Privacy Alliance (OPA) Guidelines:[1]

OPA is a U.S.-based organization which provides a general framework in which any U.S. company can operate, calling for customization and enhancement as appropriate to a company's business or industry sector. These guidelines generally provide as follows:

1. **Adoption and Implementation of a Privacy Policy.** An organization should adopt and implement a policy for protecting the privacy of individually identifiable information.
2. **Notice and Disclosure**. The privacy policy should be clear, easy to find, and available at or prior to the time individually identifiable information is collected. It should state "what information is being collected; the use of that information; possible third-party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access. It should also disclose the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization."
3. **Choice/Consent**. Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected or where there is third-party distribution of such data unrelated to the purpose for which it is collected. At a minimum, individuals should be given the opportunity to opt out of such use or third-party distribution.
4. **Data Security.** Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. Organizations should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.
5. **Data Quality and Access**. Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used. Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

---

[1] Quoted from C Varney (ed), "Privacy and Security Best Practices," November 12, 2003. Liberty Alliance. https://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf, accessed 20 November, 2005.

Organization for Economic Cooperation and Development Guidelines[2]

The OECD is an international organization focusing on global economic cooperation and development. OECD guidelines on the protection of privacy and trans-border flows of personal data are close to the European approach to privacy. Unlike the United States, Europe has more comprehensive privacy statutes and vests significant authority in its regulatory bodies to enforce privacy legislation. OECD's guidelines set forth the following eight principles:

1. **Collection Limitation.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Article 9 (the purpose specification principle) except: (a) with the consent of the data subject; or (b) by the authority of law.
5. **Security Safeguards.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation**. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

---

[2] Adapted from C Varney (ed), "Privacy and Security Best Practices," November 12, 2003. Liberty Alliance. https://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf, accessed 20 November, 2005.

Liberty Alliance Information Practices[3]

1. **Notice**. Consumer facing Liberty-Enabled Providers should provide to the Principal clear notice of who is collecting the information, what information they collect, how they collect it (e.g., directly or through non-obvious means, such as cookies), how they provide choice, access, security, quality, relevance and timeliness to Principals, whether they disclose the information collected to other entities, and whether other entities are collecting information through them. Providing notice is particularly important for Service Providers who may seek additional information beyond what is provided through other Liberty-Enabled Providers.

2. **Choice**. Consumer facing Liberty-Enabled Providers should offer Principals choices, to the extent appropriate given the circumstances, regarding what personally identifiable information is collected and how the personally identifiable information is used beyond the use for which the information was provided. In addition, consumer facing Liberty-Enabled Providers should allow Principals to review, verify, or update consents previously given or denied. The Liberty Specifications provide for both access permissions to allow a Principal to specify whether and under what circumstances a Service Provider can obtain given attributes, as well as an "envelope" for the discovery of or negotiation of usage directives as part of profile sharing. Both aspects of the privacy capabilities established by the Liberty Specifications should be fully implemented in a responsible manner and be easy for the Principal to configure. In particular, Liberty-Enabled Providers should provide for "usage directives" for data through either contractual arrangements, or through the use of Rights Expression Languages, as well as implementing the access authorization elements contained in the Liberty Specifications that permit the Principal to make certain choices regarding collection and use of personally identifiable information.

3. **Principal Access to Personally Identifiable Information** (PII). Consumer facing Liberty-Enabled Providers that maintain PII should offer, consistent with and as required by relevant law, a Principal reasonable access to view the non-proprietary PII that it collects from the Principal or maintains about the Principal. Access should not be construed to require access to proprietary data, public record data, or aggregate data.

4. **Quality**. Consumer facing Liberty-Enabled Providers that collect and maintain personally identifiable information should permit Principals a reasonable opportunity to provide corrections to the personally identifiable information that is stored by such entities.

5. **Relevance**. Liberty-Enabled Providers should use PII for the purpose for which it was collected, or the purposes about which the Principal has consented.

6. **Timeliness**. Liberty-Enabled Providers should retain PII only so long as is necessary or requested and consistent with a retention policy accepted by the Principal.

7. **Complaint Resolution.** Liberty-Enabled Providers should offer a complaint resolution mechanism for Principals who believe their PII has been mishandled.

8. **Security**. Liberty-Enabled Providers should take reasonable steps to protect and provide an adequate level of security for PII.

---

[3] Adapted from C Varney (ed), "Privacy and Security Best Practices," November 12, 2003. Liberty Alliance. https://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf, accessed 20 November, 2005.

From the eHealth Initiative Toolkit

5 Privacy Principles of Fair Information Practices

1. **Notice.** The existence and purpose of record-keeping systems must be known to the individuals whose data is contained therein.
2. **Choice.** Information must be collected only with the knowledge and implicit or explicit permission of the subject, used only in ways relevant to the purpose for which the data was collected, and disclosed only with permission of the subject or in accordance with overriding legal authority (such as a public health law that requires reporting of a serious contagious disease).
3. **Access**. Individuals must have the right to see records of information about them and to assure the quality of that information (accuracy, completeness, and timeliness). In healthcare, records are rarely deleted or replaced, but this principle implies that there is at least a due process for individuals to amend poor quality information about them.
4. **Security**. Reasonable safeguards must be in place for the confidentiality, integrity, and availability of information.
5. **Enforcement**. Violations must result in reasonable and consistently applied penalties to deter violators and in reasonable mitigation efforts to offset the effects of a breach as much as possible.

Security Principles

Since one of the principles of fair information practices is security, it should be clear that you cannot have privacy (or confidentiality of private information) without security measures to protect the information from being used or disclosed in ways that violate the other principles. The characteristics of confidentiality, integrity, and availability are the backbone of health information security. To support all three, security must be implemented as a careful balance of administrative, technical, and physical safeguards which are tailored to the particular information systems environment of each installation. This is best done through a risk assessment of the information systems environment followed by ongoing risk management through the selection, implementation, and monitoring of reasonable and appropriate measures to minimize the risks while controlling the costs. This flexible and scalable approach is the basis for the HIPAA security rule, taken because security threats and solutions evolve too quickly to be writ in stone (as it were) in the form of federal regulation.

Security involves the documentation of the implementation of reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic health information.

It is important to identify and make known the person responsible for the development and implementation of the policies and procedures as well as the implementation and ongoing maintenance of security measures for the HIE.

In general, particular attention must be paid to the following areas of security when designing the policies, procedures, and agreements for HIE:

- User identification and authentication
- User authorization
- Role based access control
- Transmission security
- Minimum necessary
- Audit trail and information system activity review
- Response to security incidents including reporting, sanctions, and mitigation


Privacy and
Confidentiality
WORKSHOP
SEPTEMBER 13-14, 2006 : NASHVILLE, TN
PRINCIPLES. PRACTICES. IMPLEMENTATION.