European Union Directive on Data Protection and Safe Harbor

By: Daniel H. Orenstein, Esq., Goulston & Storrs, Boston, MA 02109

This memo describes the most significant elements of the European Union's Directive on Data Protection, and the Safe Harbor that was developed between the U.S. Department of Commerce and the European Commission to address compliance with the Directive. Please contact me with any questions/comments.

1. Background. The European Union Directive on Data Protection (the "Directive"), which became effective October 25, 1998, established a number of legal principles aimed at protecting personal data privacy and the free flow of data within the European Union. The Directive requires each EU Member State to establish privacy protections which comply with the Directive. In addition, Member States are prohibited from transferring any personal data to countries which do not ensure "adequate" protection of personal data. Under the Directive, the terms "personal data" and "personal information" mean data about an identified or identifiable individual that are within the scope of the Directive.

2. Principles Established in the Directive. The Directive established principles with respect to data quality, the processing of personal data, protection of the data subject, and access to information by the data subject. Member States are to establish laws that conform to the principles in the Directive.

3. Principles Specific to Health Care Data. The Directive provides that Member States shall prohibit the processing of data concerning health, except where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health-care services, and where the data is processed by a health professional subject under national law or rules to an obligation of professional confidentiality, or is processed by another person subject to an equivalent obligation of confidentiality.

4. Data Transmitted to the United States. The United States has been deemed by the European Commission to be a country which currently does not ensure adequate protection of personal data under the standards articulated in the Directive. Member States are therefore generally prohibited from transferring personal data to organizations in the United States pursuant to the Directive. The prohibition applies to personal data collected by United States organizations (including companies) electronically, including via the Internet.

5. Safe Harbor for Data Transmitted to the United States. The U.S. Department of Commerce and the European Commission negotiated a "Safe Harbor," approved by the

European Commission in July, 2000[1]. If an organization in the United States complies with the Safe Harbor, the Directive's "adequacy" standard will be deemed to be satisfied for purposes of data transmissions to such organization. The Safe Harbor documents consist of the "Safe Harbor Privacy Principles" and a set of "Frequently Asked Questions" (collectively, the "Principles"). Organizations that wish to benefit from the Safe Harbor must (i) comply with the Principles, (ii) annually certify in writing to the Department of Commerce the organization's agreement to comply with the Principles, and (iii) include a declaration of compliance with the Principles in a published policy statement. The Principles are as follows (as excerpted from the "Safe Harbor Privacy Principles"):

- **Notice:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

- **Choice:** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

  For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

[1] The European Commission approved the Safe Harbor over the objection of the European Parliament, which expressed concern over the adequacy of individual appeal rights under the Safe Harbor. While a challenge to the European Commission's action is not expected, the European Commission may take action in the future to revise the Safe Harbor to address such concerns.

- **Onward Transfer:** To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

- **Security:** Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

- **Data Integrity:** Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

- **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- **Enforcement:** Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out

of failure to comply with the Principles by organizations announcing their adherence to them and consequencesfor such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

(1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

6. The Directive and HIPAA. It is unclear whether comprehensive privacy regulations, such as those required under the final privacy rule promulgated under HIPAA, will be deemed by the European Commission to provide "adequate" protection of data transmitted to organizations that are subject to the regulation's requirements. In the meantime, organizations that wish to receive data transmissions from European organizations should consider complying with the Safe Harbor. An effective approach might be to integrate compliance with the Safe Harbor into the policies and procedures that the organization adopts to comply with the HIPAA final privacy rule.

DHO/February 2001