THE NATIONAL HIPAA SUMMIT: INTERNATIONAL PRIVACY AND DATA SECURITY REQUIREMENTS

Presented by:Robert R. Belair

Mullenholz, Brimsek & Belair

(202) 296-2861 Bobbelair@aol.com

Washington, DC

October 16, 2000

PRIVACY ENVIRONMENT

- For the first time in U.S. history, privacy is a major domestic public policy issue
- Wall Street Journal poll -- Privacy is no. 1 concern for 21st century
- Almost 95 percent of the public is concerned about health privacy
- Legislative, regulatory, self-regulatory and judicial activity is intense
- Privacy is now a personal experience

SAFE HARBOR PRINCIPLES

- **Notice:**
  - **Provide notice before an organization collects, uses or discloses**
  - **Purposes**
  - **Uses**
  - **Types of recipients**
  - **Choice**

SAFE HARBOR PRINCIPLES

- **Choice:**
  - **Opt-out before information is disclosed to a third party or used for incompatible purpose**
  - **Opt-in for sensitive information including health information**

SAFE HARBOR PRINCIPLES

- **Onward transfer:**
  - **Notice and choice before any redissemination to a third party**
  - **Transfers to agents require that agent:**
    - **Be Safe Harbor compliant; or**
    - **Otherwise meet EU Directive; or**
    - **Enters into written agreement requiring compliance with Safe Harbor**

SAFE HARBOR PRINCIPLES

- **Security:**
  - **Reasonable precautions from loss, misuse, unauthorized access, alternation or destruction**
- **Data integrity:**
  - Relevance
  - Compatibility
  - Reliability
  - Accuracy
  - Completeness
  - Timeliness

SAFE HARBOR PRINCIPLES

- **Access:**
  - **Record subject must be able to review information**
  - **Correct, amend or delete inaccurate information**
  - **Exception for disproportionate burden or if violates rights or other individuals**

SAFE HARBOR PRINCIPLES

- **Enforcement:**
  - **Readily available and enforceable, independent, recourse mechanisms**
  - **Follow-up procedures for assessing compliance**
  - **Obligations to remedy violations and consequences for violations**

SAFE HARBOR COMPLIANCE

- **EC decision of July 27,2000 makes the July 21, 2000 Safe Harbor Principles operative**

- **Sept. 19,2000: DOC announces Nov. 1 start date. 65 Fed. Reg. 56534**

SAFE HARBOR COMPLIANCE

- **Organizations must self-certify their compliance with a privacy policy that meets Safe Harbor Principles. FAQ #6**

- **Can apply to DOC by letter to: Safe Harbor Registration, Department of Commerce, Room 2009, Washington, DC 20230; or online at www.ita.doc.gov/td/ecom**

SAFE HARBOR COMPLIANCE

- **Key elements of certification**
  - **Description of personal information received from EU**
  - **Adherence to a Safe Harbor compliant privacy policy and location where public can review policy**
  - **All personal information received from EU must be covered except HR data**
  - **Special undertakings for HR data**
  - **Annual certification**
  - **Immediate notice if no longer in compliance- could be violation of False Statements Act. 18 USC §1001**

SAFE HARBOR COMPLIANCE

- **Role of DOC**
  - **Will maintain a complete and updated public and online list of organizations certifying compliance**
  - **Will review certification statements for facial validity**
  - **Will not investigate or make own determination of compliance**
  - **Will refer complaints to the organization and to the FTC**

SAFE HARBOR COMPLIANCE

- **Role of DOC**
  - **Will maintain a public list of organizations which "persistently fail to comply". DOC first provides 30 days notice and opportunity to respond.**
  - **DOC questions? William Yue, Senior Counsel for Services, (202) 482-3623**

SAFE HARBOR COMPLIANCE

- **Role of the EC**
  - **Will not interrupt data flows from EC to U.S. during Safe Harbor implementation period Nov. 1, 2000 - ?**
  - **Will review Safe Harbor implementation status in “middle of 2001”**
  - **EC urges US organizations to enter Safe Harbor “as soon as possible”**
  - **EC will rely on US government agencies to make determination of non-compliance**

SAFE HARBOR COMPLIANCE

- **Role of the EC**
  - **Notwithstanding compliance determination, EC can cut off data flow if compliance action slow or uncertain**
  - **Data protection authorities will serve as an independent recourse mechanism**
  - **EC will conduct a comprehensive Safe Harbor review in 2003**

SAFE HARBOR COMPLIANCE

- **Role of the FTC**
  - **FTC has stated that a violation of Safe Harbor certification violates Section 5 of the FTC Act prohibiting "unfair or deceptive acts or practices". July 14, 2000 letter from FTC to EC**
  - **FTC will give priority to Safe Harbor complaints**
  - **FTC claims authority over most Safe Harbor participants**
  - **Consistent with FTC's role as *de facto* privacy regulatory agency**

SAFE HARBOR COMPLIANCE

- **Role of the State AGs**
  - **All 50 states have adopted mini-FTC acts**
  - **In 46 states, the mini-FTC acts provide for a private right of action by consumers**
  - **NAAG survey found 37 AGs will enforce Safe Harbor statements under mini-FTC acts**
  - **State AGs could also bring action under health information privacy statutes**

SAFE HARBOR COMPLIANCE

- **Role of HIPAA**
  - **Adherence to Safe Harbor is limited by statute, regulation or case law that creates conflicting obligations**
  - **Safe Harbor <u>never</u> provides authority to violate stricter state or federal privacy law**

SAFE HARBOR COMPLIANCE

- **Role of HIPAA**
  - **Personally identifiable health information electronically transmitted from EU to US will be covered by HIPAA privacy rules if it is "received" by a covered Entity**
  - **Compliance with HIPAA is likely to be deemed adequate for purposes of the EU Directive**

SAFE HARBOR COMPLIANCE

- **Role of HIPAA**
  - **HIPAA final rules are likely to be more privacy protective than Safe Harbor**
    - **Minimization requirement**
    - **De-identification requirement**
    - **Business partner requirement**
    - **Disclosures to non-health related divisions of a Covered Entity**
    - **Accounting of disclosures**
    - **Amendment and correction**
    - **Chief Privacy Officer**
    - **Employee training**

SAFE HARBOR COMPLIANCE

- **State health privacy law**
  - **State constitutions**
  - **Comprehensive state health information privacy statutes**
  - **Health care provider privacy statutes**
  - **State statutes governing types of health data -- genetic, HIV, mental health, pharmacy records**

SAFE HARBOR COMPLIANCE

- **State health privacy law**
  - **Confidentiality statutes and licensing standards**
  - **Doctor/patient privilege statutes**
  - **Consent statutes**

SAFE HARBOR COMPLIANCE

- **Common law claims**
  - **In most states, a false or deceptive Safe Harbor certification could create a common law tort claim for negligent or intentional misrepresentation**
  - **Both consumer and European data controller could bring action-seek damages**

SAFE HARBOR COMPLIANCE

- **Common law claims**
  - **In most states, there are also tort privacy claims that a breach of Safe Harbor may create or exacerbate**
    - **Intrusion**
    - **False light**
    - **Public disclosure of private facts**

SAFE HARBOR COMPLIANCE

- **Extra-legal pressures**
  - **Self-regulatory groups and peer relationships**
  - **Privacy advocacy organizations**
  - **The media**
  - **Boards of Directors and stockholders**

SAFE HARBOR COMPLIANCE

- **Compliance strategies and issues**
  - **When to enter Safe Harbor**
  - **Some organizations should never certify for Safe Harbor**
  - **Automated vs. manual data**
  - **Public statements and posture about Safe Harbor**
  - **Impact of Safe Harbor on U.S. generated health data**