WILMER, CUTLER & PICKERING

e-commerce news

april 23, 1999

With this edition of the E-Commerce News, we are initiating a regular update on e-commerce developments in broad areas of interest (financial services, privacy and

TELEMEDICINE

Telemedicine (electronic communication with patients or the use of electronic communications in diagnosing and consulting from a distance) holds great promise for timely, efficient, and expert delivery of health care. It also results in health care practitioners giving advice to patients living in other jurisdictions, often without opportunity for physical examination, and exchanging confidential patient data in electronic form with a number of parties. Like any professional relationship (including the lawyer-client relationship) conducted over the Internet, doctor-patient interactions may raise legal risks. In particular, Congress is likely to enact medical privacy legislation of which companies and practitioners will need to be aware.

Privacy concerns are the current focus of attention.

Congress is now considering wide-ranging medical privacy legislation that would apply to health care professionals, insurers, employers, laboratories, database outsourcers, and any other parties involved in the storage or transmission of individual medical data. It is likely that federal legislation adopted in 1999 will have a controlling effect on the development of telemedicine transmission and data storage techniques. Three comprehensive federal health privacy bills have been introduced in the 106th Congress. Of these, Sen. Patrick Leahy's (D-VT) bill (S. 573) and a companion House bill (H.R. 1057) sponsored by Rep. Ed Markey (D-MA) are the leading contenders for passage. In addition, patients' rights bills introduced in both the House and Senate include provisions related to confidentiality of identifiable health information and the right of individuals to access their personal health information.

Until this legislation is adopted, state legislation and common law govern the treatment of patient records and the disclosure of information to third parties. Unfortunately, the rules differ from one sector to another (hospitals, doctors, pharmacists, nurses, paramedics, insurers, and employers are subject to different standards and liabilities), as well as from one state to another. This phenomenon is especially pronounced across national borders. The European Data Protection Directive (Directive 95/46 EC) is being implemented this year in national legislation in the 15 EU member states and ultimately in most other European countries. It generally requires express prior consent to collect and store health-related information

about an individual, and it obliges any party with such data to so inform the individual and to give the individual access, on request, to the data. Moreover, medical data generally cannot be disclosed to any other party without consent. Canada, Australia, and other countries are considering similar legislation, with uncertain consequences for data transfers between the U.S. and those countries. Proposed federal legislation on medical privacy in the U.S. may or may not satisfy the test of "adequate protection" to justify cross-border data transfers under the laws of those countries.

Key issues for telemedicine applications include the following:

- What information is subject to confidentiality? How must the patient be notified of data practices and rights?
- May medical data be stored indefinitely?
- Under what circumstances may an individual waive privacy protection or consent to specific disclosures? How is informed consent established and recorded in purely electronic transactions?
- What exceptions are made for individual or public health emergencies, medical and scientific research, clinical trials and adverse events reporting, insurance and other payment systems, discovery in civil and disciplinary cases, internal use of health information by employers, etc.?
- Are the individual's rights to access data limited? How may the individual object to secondary uses of data (e.g., for marketing or employment) or correct inaccurate data?
- What standards apply to the secure processing and communication of sensitive personal data?
- In providing information electronically, how does a telemedicine provider ensure the identity of the person with whom it is communicating?

Some of these issues are common to other forms of electronic services and commerce (including, for example, the financial services industry), and the security and identification issues, in particular, will likely be resolved in increasingly standard ways.

What law governs?

The key jurisdictional issue for doctors practicing medicine over the Internet is which state's (or country's) laws govern the doctor-patient relationship. In other words, must a doctor be licensed to practice medicine in the state (or country) where his or her patient lives, or is licensure in his or her own state (or country) sufficient? Currently, there is no uniform answer to this question. Several states have adopted legislation stipulating that when the patient and doctor are in different states, the patient's jurisdiction prevails. This rule may not make much sense. Under current law, Florida's laws would govern the doctor-patient relationship between a patient who physically travels from Alaska for an appointment in a doctor's Florida office. If that patient returns to Alaska and calls her Florida doctor for advice, Florida law still governs their interaction. Why should doctor-patient communication over the Internet be treated differently?

Possible solutions to the jurisdictional problem include the establishment of a mutual recognition scheme, or reciprocity, among states. That is, Alaska and Florida could agree that the doctor's state will have jurisdiction over the relationship, and the doctor will be required to be licensed to practice medicine only in his or her home state. The drawback to this solution is that it requires coordination between states and would not be effective unless reciprocity is agreed to by a large number of states. The Federation of State Medical Boards is drafting a model statute recognizing a limited license for physicians licensed in another state to practice telemedicine. (There is a similar initiative in the European Union, for physicians licensed in another EU country.)

MONTHLY UPDATE

Privacy/Financial Services.

Rep. Ed Markey (D-MA) has introduced two privacy bills. HR 1339, the Depository Institution Customers Financial Privacy Enhancement Act of 1999, would require insured depository institutions, depository institution holding companies, and insured credit unions to protect the confidentiality of financial information obtained concerning their customers. HR 1340, the Securities Investors Privacy Enhancement Act of 1999, would require brokers, dealers, investment companies, and investment advisers to protect the confidentiality of financial information obtained concerning their customers. Rep. Markey has indicated that he will introduce both of these bills as amendments to HR 10, the Financial Services Act of 1999, when it is marked up by the House Commerce Committee. (Consideration of HR 10 by the Commerce Committee will begin later this month with a markup likely in May.)

Privacy/General.

Sen. Conrad Burns (R-MT), along with Sen. Ron Wyden (D-OR), introduced the Online Privacy Protection Act, legislation aimed at ensuring the security of personal information on the Internet. The bill requires commercial web sites to notify visitors if any information is collected and gives visitors the ability to "opt-out" of having their information collected.

Sen. Patrick Leahy introduced S. 854, the Electronic Rights for the 21st Century (ERIGHTS) Act, aimed at encouraging Americans to develop and use encryption technology.

Securities Fraud.

Sen. Susan Collins (R-Maine) has announced that she will introduce this spring a bill (1) prohibiting broker-dealers accused of violating federal securities laws from acting as microcap stock promoters, and (2) broadening the Securities and Exchange Commission's ability to use information gathered by state regulators to bring enforcement actions.

Communications.

Sen. Conrad Burns is expected to introduce a bill clarifying that the FCC has substantial deregulatory authority to encourage the building of broadband data networks under section 706 of the Telecom Act.

AOL's Steve Case testified in front of the Senate Commerce Committee last week. Case pushed for FCC intervention to make cable operators provide ISPs with access to cable networks. Panelists and other members signaled that they need more information before acting on the problem.

Sen. John McCain (R-AZ) is expected to introduce legislation to require NTIA and the FCC to collaborate on a study of broadband service deployment, with emphasis on access for low-income rural consumers. Sen. Fritz Hollings (D-SC) and Sen. Conrad Burns will be co-sponsors.

FCC Chairman Kennard has indicated that he does not want to take up the Internet/cable access issue in the near future.

* * *

For further information, contact:

David R. Johnson 202/663-6868
djohnson@wilmer.com
W. Scott Blackmer 202/663-6167
sblackmer@wilmer.com
Susan P. Crawford 202/663-6479
scrawford@wilmer.com
Jennifer E. Grishkin 202/663-6048
jgrishkin@wilmer.com

E-Commerce News also available at http://www.wilmer.com