U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

Remarks of John T. Bentivoglio
Special Counsel for Health Care Fraud and
Chief Privacy Officer
U.S. Department of Justice

Telemedicine: Evolving Legal and Regulatory Issues for the Health Professions

Friday, April 28, 2000 – Buffalo, New York

I want to thank the Schools of Law, Medicine and Pharmacy at the University at Buffalo for the invitation to present the Justice Department's views on the legal and regulatory issues surrounding telemedicine, particularly issues relating to fraud and privacy.

Why Is the Department of Justice Concerned About the Impact of Technologies – Particularly Information Technologies – in the Health Care Sector?

The Internet and other information technologies are revolutionizing the health care industry. Through these new technologies, we will be able to save billions of dollars in administrative and overhead costs – money that can be used to discover new drugs or expand coverage for the uninsured. These same technologies also promise to dramatically improve patient care. Nowhere is this more true than in the area of telemedicine. Although many commentators focus on the high-tech aspects of telemedicine – how a specialist in one location could provide real-time assistance in the treatment of a patient half-way around the world – the real benefits are going to be less eye-catching but far more important. I serve as a volunteer firefighter and EMT in the State of Maryland, and I am well aware of the dangers of transporting frail nursing home residents to the hospital. Telemedicine promises to reduce these dangers – allowing residents to receive high-quality treatment right in their rooms.

But the same factors that make information technology useful in the health care industry – low barriers to entry, relative anonymity, the elimination of geographic boundaries – also provide new opportunities for unscrupulous providers and new incentives to trample on the legitimate privacy rights of individuals. The online pharmacy industry is a case in point. There is no doubt that online pharmacies can benefit patients by reducing costs, providing targeted educational materials, and providing other services to patients, some online pharmacies are nothing more than scams – dispensing dangerous drugs to individuals without any meaningful evaluation of the

patient – indeed, sometimes providing drugs without the involvement of a doctor, pharmacist, or any health care professional whatsoever. The operation of these rogue Internet pharmacies is a serious public health and safety concern, and as I will discuss shortly, we are taking steps to address these issues.

Overview of Remarks

Today, I would like to discuss the Federal government's fraud, consumer protection, and privacy protection efforts as they relate to telemedicine and the emerging e-health industry, particularly the role of the U.S. Department of Justice and our counterparts in other law enforcement and regulatory agencies. My goal – in the next 25 minutes -- to is convince you of our commitment to safeguarding the health, safety and privacy of consumers in the health care system – online or off and to get you thinking about the need for developing effective compliance programs within your organization.

DOJ's Fraud Enforcement Program

Combating fraud and other white-collar crimes – particularly those that target elderly and other vulnerable consumers and those targeting taxpayer-funded health care programs – is one of the Justice Department's highest priorities. We have developed a sophisticated, nationwide -- and increasingly international -- program to combat all forms of fraud and white-collar crime.

In 1993, Attorney General Janet Reno announced that combating health care fraud would be the Department's number one white-collar crime priority. Last year, the Department of Justice obtained almost 400 convictions for health care fraud -- an increase of 21% over the prior year. In this same period, we were able to collect $524 million -- more than half a-billion dollars --- in criminal fines, civil settlements, and administrative penalties.

And our health care fraud enforcement efforts will increase significantly in the coming years. Under the "Kennedy-Kassebaum" or "HIPAA" legislation, the Departments of Justice and Health and Human Services receive dedicated – and increasing – funding for health care fraud enforcement. This year (FY 2000), the Justice Department and HHS received $158 million. This figure will increase to $240 million in FY 2003. Similarly, funding for the FBI will increase from $76 million this year to $ 114 million in FY 2003 – an increase of more than 50 percent.

These increased resources mean we have more investigators, auditors, and prosecutors focused on health care fraud than ever before – and our enforcement resources will increase for at least the next three years. These figures should convince even the skeptics that health care fraud will remain a high priority for the Justice Department and our federal law enforcement partners for the foreseeable future.

Legal and Regulatory Framework[1]

Fraud and false statements.

A number of federal criminal laws prohibit a wide range of fraudulent conduct, which can roughly be described as any scheme designed to obtain money or something of value under false pretenses.[2] Civil fraud remedies also are available where the federal government is the victim of fraud.[3] Federal law also prohibits making false statements to federal agencies, including statements made to obtain payment from the federal government or in connection with information provided to regulatory agencies, such as the Food and Drug Administration or the Health Care Financing Administration.[4] Thus, if your company submits information to the federal government, either in the course of compliance with a regulatory program or in order to obtain reimbursement, it is essential that you take steps to ensure the data is accurate.

Kickbacks and self-referral laws.

Health care companies providing services to federal health care programs also need to be mindful of federal laws that prohibit kickbacks and self-referrals. The federal anti-kickback statute makes it a crime, punishable by up to five years in prison, to provide any thing of value, money or otherwise, directly or indirectly, with the intent to induce a referral of a patient or a health care service.[5] Significantly, liability attaches to both parties to the transaction -- the entity or individual providing the prohibited remuneration and the entity or individual receiving it. Federal law also prohibits so-called physicians and other health care providers from referring beneficiaries in federal health care programs to clinics or other facilities in which the physician or

---

[1] This overview discusses a number of federal laws relevant to telemedicine and Internet-based health care providers. This is not meant to be an exhaustive list of the laws or regulations that might apply to specific businesses or practices.

[2] These statutes include, but are not limited to: 18 USC 669 (theft or embezzlement in connection with health care), 18 USC 1341 (mail fraud) ,18 USC 1343 (wire fraud), and 18 USC 1347 (fraud in public or private health care benefit programs).

[3] See 31 USC 3729-33 (False Claims Act).

[4] 18 USC 1001 (false statements to a federal agency); 18 USC 1035 (false statements relating to health care matters). A related statute, 18 USC 1518, prohibits efforts to obstruct a health investigation.

[5] 42 USC 1320a-7b(b). Various statutory and regulatory safe harbors have been established for beneficial arrangements that might otherwise violate the statute. See 42 USC 1320a-7b(b)(3) (statutory safe harbors); 42 CFR 1001.952 (regulatory safe harbors).

health care provider has an interest.[6] These practices – kickbacks and self-referrals – are prohibited under federal law because they tend to corrupt the exercise of a medical professional's independent judgment. The U.S. healthcare industry relies extensively on physicians, hospital discharge planners, and other health care providers to allocate scarce health care resources based on what's in the best interest of patients. Federal law contains broad prohibitions – backed up by stiff criminal and civil penalties – for arrangements that tend to corrupt that judgment and put the provider's bottom line ahead of the patient's well being.

Regulation of Drugs and Medical Devices.

The Federal Food, Drug and Cosmetic Act (FDCA) prohibits the unauthorized distribution of drugs or medical devices. Federal criminal penalties are available for knowing and intentional violations of the FDCA. The manufacture and distribution of controlled substances is governed by the Controlled Substances Act, which is enforced by the Drug Enforcement Administration, a component of the U.S. Department of Justice. The requirements of the FDCA and CSA apply to online as well as bricks-and-mortar pharmacies.

Federal Privacy Laws.

Although there are a number of federal laws that protect the privacy of individuals, I want to highlight two that are particularly important to the i-health industry. First, the Federal Trade Commission Act prohibits businesses engaged in interstate commerce from engaging in a broad range of unfair or deceptive trade practices. According to the FTC, collecting or disclosing personal information in violation of a Web site's written privacy policy may constitute an unfair or deceptive trade practice. The FTC has announced that it has launched an investigation into the privacy practices of a number of health care Web sites, prompted in part by the California Healthcare Foundation study that found several well-known sites were violating their own posted privacy policies.[7]

Potentially more important to the i-health industry are the new medical records privacy standards under development by the U.S. Department of Health and Human Services.[8] Because Congress failed to meet its own deadline for enacting comprehensive medical records privacy legislation, the 1996 Kennedy-Kassebaum law authorized and directed the HHS Secretary to develop privacy regulations for certain electronic health care transactions. These regulations

---

[6] 42 USC 1395nn (codifying "Stark I" and "Stark II" statutes).

[7] "FTC Reviews Privacy Issues at Health Web Sites," Wall Street Journal, Feb. 18, 2000, at B6.

[8] U.S. Department of Health and Human Services, Notice of Proposed Rule Making for Standards for Individually Identifiable Health Information, 64 Fed. Reg. 59917-60065 (Oct. 23, 1999). Also available at www.hhs.gov/hottopics/healthinfo/index.htm.

apply to health care providers, health care plans, and health care clearinghouses. Less noticed, but quite important, the Kennedy-Kassebaum legislation also required HHS to develop minimum standards for the security of electronic health information.[9] The recent cyberattacks on well-known e-commerce sites have served as a wakeup call to industry on the vulnerability of Internet-based computer networks – and the need to take steps to address information security issues.

Application to Telemedicine and the E-Health Industry

Earlier in the day, speakers addressed broadly the legal and regulatory framework for telemedicine providers and supplies. I want to dwell for a moment on the application of anti-fraud and consumer protection laws – particularly those enforced by U.S. Department of Justice.

Federal Food, Drug and Cosmetic Act.

Our most active enforcement efforts relating to the Internet and the e-health industry have focused on Internet pharmacies. The FDA's Office of Criminal Investigations has initiated 134 Internet-related investigations, including 88 open criminal investigations and 46 preliminary investigations. Of these 134 investigations, 54 involve sites selling prescription drugs, while 80 cases are related to various types of health fraud or unapproved drug products such as GHB. To date, 36 arrests and 17 convictions have resulted from FDA investigations into the illegal sale of drugs or medical products over the Internet.

In the near future, the Administration will present legislation to Congress to provide consumer protections for Internet drug sales. The underlying goal of the legislation will be to ensure that online pharmacies are licensed and operated under the same regulatory system that Congress and the States have put in place for traditional "brick and mortar" pharmacies. Therefore, the legislation will call for online pharmacies to post information on their Web sites about their ownership, state licensure, name of the pharmacist in charge, and a phone number where consumers can contact the pharmacist. Online pharmacies that fail to meet these requirements would be subject to federal civil and criminal penalties.

Anti-kickback Statute and Self-Referral Laws.

There has been far less enforcement activity under the anti-kickback and self-referral laws largely because the volume of federal reimbursement for telemedicine and Internet-based health care services is quite limited. The federal anti-kickback laws only apply to federal health care programs – Medicare, Medicaid, and a handful of other federal programs (although the kickback statutes in a number of states are not limited to government-funded health care programs). However, this situation is changing rapidly. Forrester Research estimates that the e-health care industry will reach $340 billion annually by 2004 – with more than online health care claims

---

[9] U.S. Department of Health and Human Services, Notice of Proposed Rule Making for Security and Electronic Signature Standards, 63 Fed. Reg. 43263-69 (Aug. 12, 1998).

accounting for more than $200 billion of this figure. In addition, there are advocates within Congress and the Administration who support expanding reimbursement for telemedicine. If these trends continue, the amount of federal dollars at risk – and the potential for fraudulent and abusive conduct increases – I believe we will see more enforcement activity.

Privacy.

I believe the Administration will release a final medical records privacy regulation this year. If the timetable under the current draft is retained, providers generally will have two years to come into compliance. While this may sound like a great deal of time, the privacy requirements are substantial, requiring new policies, procedures and practices among many different groups – clinical staff, IT professionals, medical records managers, public affairs staff, and others. While I do not expect a large volume of malicious or intentional violations, the value of information in healthcare databases is so valuable that I do anticipate some violations that will warrant criminal prosecution.

Compliance Tips

So, what can you do – individually within your companies and collectively through trade associations and other industry groups? You've taken the first step by attending this conference and learning more about the legal and regulatory framework for your industry. The next step should be a comprehensive assessment of your business practices, focusing on several key areas, including privacy practices, compliance with fraud and abuse laws, and compliance with regulations governing the sale and promotion of drugs and medical devices.

Do you collect and/or disclose personal information? If so, are you a health care provider, plan, or clearinghouse as defined in the new draft HHS privacy regulations? Have you taken steps to protect such data against cyberattacks?

Are you required to submit information to the federal government, such as information required by the FDA or other regulatory agency? If so, do you have systems in place to ensure the data is accurate?

Do you receive, directly or indirectly, reimbursement from the federal government for health care goods or services -- or are you contracting with an individual or entity that does? If so, have you examined your operations to ensure you are in compliance with all federal health care fraud laws, including the anti-kickback and self-referral statutes? Have you instituted steps to screen employees and contractors to ensure your company has not hired an individual who has been excluded from participation in federal health care programs?

Are you dispensing or promoting drugs or medical devices over the Internet in a manner that would subject you to regulation by the FDA, FTC, or state regulatory agencies?

For telemedicine or Internet-based health care businesses that rely, in whole or in part, on reimbursement from federal health care programs, I would encourage you to develop compliance programs that contain, at a minimum, the several components identified by the HHS Office of Inspector General in model compliance guides for various segments of the health care industry. These elements include: (1) written policies and procedures; (2) designation of a compliance officer and compliance committee; (3) education and training of management and employees; (4) establishment of lines of communication (including employee hotlines); (5) auditing and monitoring; (6) enforcing standards through disciplinary procedures and practices; and (7) responding to detected offenses and developing effective correction plans.

We realize that the health care industry is undergoing rapid change, and that the market favors businesses that are dynamic and embrace change rapidly. But it is just this type of environment – where critical management resources are stretched thin, and back-office operations like compliance rank far behind the need to obtain funding and get products out the door – where companies take short cuts that can result in criminal or civil investigations and punishment.

What Resources Are Available to Help?

There is a wealth of information available that describes the requirements of federal law and provides advice on how to comply. The Federal Trade Commission, which plays a critical role in safeguarding consumer privacy, provides very useful information on e-privacy and consumer fraud protection efforts on its Web site. Similarly, the Web site of the Department of Health and Human Services contains detailed information on the new draft medical records privacy regulations. For advice on compliance with federal health care fraud laws, I would encourage you to visit the Web site of the HHS Office of Inspector General. This site contains detailed compliance guides, advisory opinions, special fraud alerts, and other practical information.

Finally, the Justice Department just announced a new Web site – www.cybercrime.gov – which provides information on our computer and high-tech crime enforcement efforts. The site contains speeches, testimony, information on our investigative and prosecutorial efforts, among other things.

Conclusion

I hope that I have accomplished what I set out to do 25 minutes ago – to describe our health care fraud enforcement program, to provide a quick overview of the legal and regulatory framework for the telemedicine and Internet healthcare industry, to offer some personal predictions on the future of our enforcement efforts, and to provide some practical advice on how to comply with federal law. I hope this information has been helpful and I would be happy to answer any of your questions.