Davis Wright Tremaine
LLP

Legal and Ethical Issues in the Healthcare Internet and E-Commerce

Keith M. Korenchuk, Charlotte, NC

August 24, 2000

Part I

Online Pharmacies

Davis Wright Tremaine LLP

Regulating E-Health

- Healthcare is among the most regulated of American industries — expecting E-Health to escape regulatory scrutiny is unrealistic.
- The explosion of healthcare-related activity on the Internet is too great to be ignored by state and federal regulators.

Davis Wright Tremaine LLP

E-Health — Market Considerations

- This represents 68% of approx. 88 million adults accessing the Web (Harris Poll).
- By 2003, 156.7 million persons will be online (Jupiter Communications).
- Web content related to healthcare is proliferating rapidly — the Alta Vista search engine identified 5,000 pages indexed by "health" in December 1996; 18,000 in October 1998; 13,749,000 in January 2000; 23,551,210 in May, 2000.
- By 2003, 19% of the online population, or 27.3 million users, will be 50 or older.

Davis Wright Tremaine LLP

Internet Use for Health Care

- Pharmaceuticals at the center of complex legal issues
- The initial cutting edge for legal issues
- Pharmacies expand role online.

Davis Wright Tremaine LLP

History of Regulation

- Regulation of Pharmaceuticals
- State Regulation
  - Practice of Pharmacy
  - Practice of Medicine
- Mail Order Pharmacies
- State and Federal Enforcement Efforts

Davis Wright Tremaine LLP

E-Health Frontier — Regulatory Challenges

- Three types of business activity
  - Traditional pharmacy business
  - Business combining pharmacy activity with prescribing regimen
  - Offshore pharmacy.

Business #1

The Traditional Pharmacy Goes Online

Davis Wright Tremaine LLP

State Licensure Issues

- Licensed in the state in which they operate.
- Compliance with state laws where patients located.
- Licensure or regulatory approval required in each of the states in order to maintain compliance.

Davis Wright Tremaine LLP

Protection of Patient Confidentiality

- Potential liability for damages caused by inappropriate disclosure of patient information.
- Pharmacies must use latest technology available for data encryption.
- Must take other appropriate electronic security measures.

Davis Wright Tremaine LLP

Other Legal Issues

- Risk management and professional liability
  - Prescription appropriately written.
- Verification Activities
  - Ensuring prescription is valid
  - Physician is authorized to write prescription
  - Physician has appropriate licensure.

Davis Wright Tremaine LLP

Health and Product Information

- Must be accurate and not misleading.
- Inappropriate information could result in potential liability.
- State consumer protection or Federal Trade Commission action.

Business #2

Pharmacies that Prescribe

Pharmacies That Prescribe

- Combines the pharmacy function with a prescribing function.
- Online user to access pharmaceutical information, fills out patient encounter forms, and orders pharmaceuticals .
- Patient does not independently seek medical advice nor have an independently obtained prescription.
- Online process includes a physician “consultation.”

Legal Issues and Risks

- Internet development will challenge traditional boundaries.
- A licensed physician or authorized health care professional is required to make prescription decision.
- Without valid prescription, pharmacy could violate the practice of medicine prohibitions.

Reducing the Legal Risk

- Organizations should retain licensed physicians to provide appropriate patient review and prescriptive authority.
- Physicians face the risk of violating the practice of medicine laws in various states.
- Attorney General and state enforcement initiatives.

Site Design Challenges

- Sufficient patient information must be obtained.
- Role of the physician in the review.
- Physicians who prescribe without sufficient patient contact risk ethical, regulatory, and legal challenges.

Davis Wright Tremaine LLP

Pharmacy — Patient Relationship

- Increased exposure to liability actions if patient injury occurs.
- Establishment of physician-patient relationship.
- Corporate practice of medicine prohibitions, aiding and abetting in the unlicensed practice of medicine.
- Chat Rooms and Message Boards.

Davis Wright Tremaine LLP

Health Care–Specific Regulatory Issues

- Fraud & Abuse .
- Stark and State Anti-referral statutes.

Business #3

Offshore Pharmacies

Davis Wright Tremaine LLP

Offshore Pharmacies

- Most problematic from a regulatory and enforcement perspective.
- Allows consumers on the Internet to obtain pharmaceuticals without prescription from a physician.
- Allows consumers to obtain pharmaceuticals without quality control standards.

Davis Wright Tremaine LLP

Legal Issues

- Most of these companies are designed not to comply with applicable federal and state laws.
- Ability to track down and enforce American legal standards on these organizations is difficult to achieve.

Davis Wright Tremaine LLP

Policy Issues, Enforcement and Certification

The Future of E-Pharmacy (and E-Health)

- Legal and regulatory environment struggles to respond.
- A model act for the development of the pharmacy/internet interface and practice of medicine over the Internet will be developed.
- Federal legislation has been proposed.

National Association of Boards of Pharmacy

- Established a self-regulating seal of approval for companies that operate on the Internet in the pharmaceutical area.
- Organizations that comply with the criteria of NABP may display its "seal of approval."
- Require online pharmacies be licensed in every state they ship drugs.
- Sites must meet standards for patient privacy, quality assurance, authentication and security of prescriptions and communications between patient and pharmacist.

Davis Wright Tremaine LLP

Regulatory and Enforcement Context

States

- Regulation: Licensure of Providers & Pharmacies
- Enforcement: Consumer Protection & Provider Issues.

Federal

- Regulation: Pharmaceuticals
- Enforcement: Consumer Protection.

Davis Wright Tremaine LLP

The E-Health Policy Issues for Licensure

Considerations for Regulation/Licensure/ Enforcement

- Consumer Protection (Education, Fraud, Privacy)
- Quality Oversight
- Support Clinical/Business Innovation
- Unburdensome Regulation with clear guidance.

Davis Wright Tremaine LLP

State Approaches

- Coordinated State Initiatives
- Model UCC, Uniform Acts (Limited Partnership, LLC)
- Coordinating Approach — FSMB/NAPB
- Challenges — Coordination, Multiple Parties, Turf.

Davis Wright Tremaine LLP

Federal Licensure

- FDA proposed regulation
- Model — ERISA
- Challenges — Regulatory expertise, against historical approach and state interests
- US Jurisdiction/International.

Davis Wright Tremaine LLP

A Possible Legislative Approach for Pharmacy/Prescribing

- FSMB/NAPB collaborative effort
- Model legislation
- State member support
- Need for prompt/uniform action
- Challenges
- Opportunities
- FDA ALTERNATIVE

Davis Wright Tremaine LLP

Enforcement Initiatives

- State
- Federal
- International
- Tailor Effort to Evolving E-Commerce Market

Part II

Overview of E-Health Legal Issues

Davis Wright Tremaine LLP

What Is E-Health Law?

- Healthcare Law
- Copyright Law
- Commercial Law
- Internet Law
- Much More

The Regulatory Landscape

- Attorney General's working group to review unlawful conduct on the Internet.
- Conclusion — significant new substantive legislation not necessary.
- OIG, DOJ, DOC, FTC and FBI all have jurisdiction.

Cybermedicine Liability Issues

- When does providing medical information through a website become the practice of medicine?
- States laws determine what constitutes the practice of medicine.
- Generally, a physician-patient relationship is formed when a physician exercises independent medical judgment on behalf of a patient.
- Telephone or online diagnosis appears to qualify as the practice of medicine in many states.

Cybermedicine Liability Issues (cont'd)

- Physicians providing online medical advice may subject themselves to the jurisdictions of many states, each with its own definition of the practice of medicine.
- Corporate practice of medicine issues — medical information sites that use physicians to provide advice or information directly to individual patients may be at risk.

Cybermedicine Liability Issues (cont'd)

- The Internet creates the potential for greater confusion regarding who is the provider of care.
- Linking arrangements create the possibility of creating the appearance of integration or affiliation among healthcare providers that may not exist.

Information Torts

- Healthcare provider liability actions will most likely involve information torts.
- An information tort arises from the quality of information interchange between provider and patient, rather than interpersonal acts or quality of care.
- Examples: informed consent and failure to warn.

Information Torts (cont'd)

- Courts will have to decide how to allocate the risk for erroneous medical information disseminated online: it's becoming cheaper and easier for physicians to give advice and for patients to access advice and information.
- Is it reasonable to hold a single physician responsible to a hundred recipients of medical "advice"?

Telemedicine Laws

- State telemedicine statutes generally do not permit physicians to directly provide care to patients in other states via the Internet without appropriate state licensure.
- Exceptions are often permitted for emergencies, consultations and educational purposes.
- State legislatures are seeking to continue to control the practice of medicine in their states.
- It's unlikely that telemedicine laws will be loosened to make the practice of medicine in multiple states through the Internet any easier.

Davis Wright Tremaine LLP

Chat Room Liability

- Erroneous medical information may be spread by users or patients through a chat room or message board sponsored by a provider.
- Should the chat room content be monitored or moderated?
- For providers, ethical considerations may control.
- For non-providers, monitoring content may increase responsibility (and liability).
- *Zeran v. America Online*: how much protection does this case offer to providers?

Davis Wright Tremaine LLP

False Advertising Issues

- Every web site is essentially an advertisement.
- Providers should take the same care with web site content as they do with advertising.
- California Business & Professions Code Section 651 prohibits false, fraudulent, misleading or deceptive advertising by physicians.

Davis Wright Tremaine LLP

California Business & Professions Code Section 17508

- Specifically applies to Internet advertising.
- Advertisements may not make false claims that purport to be based upon factual or clinical evidence.
- The California Attorney General, city attorney or district attorney may require an advertiser to produce evidence of facts supporting the claims.
- Providers should carefully review any factual statements made on web sites regarding response times or success rates.

Davis Wright Tremaine LLP

Federal Trade Commission Enforcement

- Jodie Bernstein, director of the FTC's Bureau of Consumer Affairs, is targeting fraud, violations of consumer privacy an deceptive marketing practices on the Web.
- FTC now conducts "surf days" to scan the Internet for fraud.
- Areas of focus: online pharmacies and healthcare products making deceptive claims.

Davis Wright Tremaine LLP

Provider–Patient E–Mail

- Whether providers realize it or not, patient e-mails are part of the medical record and should be treated as such.
- Security of patient e-mails must be guarded — a patient sending an e-mail to drsmith.com may have an expectation that it is being read solely by Dr. Smith, when it may be printed out and left on a desk where the entire office staff and other patients may read it.
- Encryption of provider-patient e-mail will be required by HIPAA — it is advisable today.
- Handling of e-mail communications should be consistent with the provider's general standard of practice.

Provider–Patient E–Mail (cont'd)

- One of the appeals of e-mail is that you can answer whenever you like.
- Court cases have established that a physician may be negligent for failing to return a patient's phone call within a reasonable period.
- Providers should establish specific expectations for e-mail response time.
- Providers should consider whether certain types of communications (like test results) should be communicated by e-mail in the absence of appropriate encryption.

Privacy Issues — Overview

- A maze of contradictory and competing laws, both within and outside the U.S., may apply to sites that collect personal data about users.
- Electronic Funds Transfer Act.
- The Fair Credit Reporting Act.

Privacy Issues — Overview (cont'd)

- European Union Privacy Directive.
- The Children's Online Privacy Protection Act.
- FDA electronic submission regulations.
- Health Insurance Portability and Accountability Act of 1996.

Davis Wright Tremaine LLP

HCFA Internet Security Policy

- Unlike HIPAA, the November 1998 HCFA Internet Security Policy is being enforced today.
- Serves as a stop-gap until HIPAA becomes effective.
- Applicable to entities that contract with HCFA and handle Medicare beneficiary information (carriers, intermediaries, state Medicaid programs, Medicare+Choice plans).

HCFA Internet Security Policy (cont'd)

- A covered entity transmitting Medicare beneficiary information over the Internet must have the following measures in place:
  - encryption
  - authentication or identification of users
  - use of an effective password/key management system.

Davis Wright Tremaine LLP

The DoubleClick Controversy

- DoubleClick's use of "cookies."
- What is a cookie?
- California Healthcare Foundation's report on e-health privacy practices (January 2000).

Davis Wright Tremaine LLP

The DoubleClick Controversy (cont'd)

- FTC investigation of Health Central.com, iVillage.com and other e-health sites (February 2000).
- Michigan Attorney General commences legal proceedings against DoubleClick.
- Critics charge that e-health sites under examination were not properly disclosing in their online privacy policy the user information being gathered by DoubleClick.
- DoubleClick announces that it will not use the Abacus database to link personally identifiable information to information obtained through cookies (March 2000).

Privacy Policies

- A web site privacy policy should not be a generic document — it must reflect your actual privacy practices.
- Deceptive or incomplete privacy policies may violate state consumer protection or false advertising laws.
- Possibility of FTC scrutiny.

Common Privacy Policy Mistakes

- Failure to discuss use of cookies.
- "Puffing" regarding level of security protections — there's no such thing as "100% secure."
- Failure to address Children's Online Privacy Protection Act (when applicable).

Common Privacy Policy Mistakes (cont'd)

- Clearly and accurately describe use of aggregate or de-identified user data.
- Discuss employee training and discipline.
- Consent to policy updates through continued use of site.

New Theories of Liability

- Failure to comply with a site's posted privacy policies may violate state unfair and deceptive acts and practices statutes, as enforced by state Attorneys General.
- Possibility of negligence actions against sites for security breaches, including acting as a host for hacker attacks.
- A class action lawsuit has even been filed in Texas seeking to apply the Texas anti-stalking law to Yahoo's use of cookies.

Terms of Use Disclaimers

- No medical advice.
- No warranty regarding goods or services.
- Limitation of liability, including consequential damages.

Davis Wright Tremaine LLP

Terms of Use Disclaimers (cont'd)

- Not responsible for chat room and message board postings.
- Not responsible for privacy practices of linked sites.

Davis Wright Tremaine LLP

Terms of Use

- Remember to adapt the Terms of Use for new functionalities that may give rise to liability, such as a drug interaction checker or medication reminder.
- Clarify any ambiguities regarding corporate entities and affiliations.

Terms of Use (cont'd)

- For content licensing or co-branding arrangements, make sure it's clear whose Terms of Use and Privacy Policy apply.
- Do the terms of use create a binding contract with users?
- *Ticketmaster Corp. v. Tickets.com, Inc.*

Regulatory Issues in Cyberspace

- Example: a medical information site charges pharmacies each time someone visiting the site clicks a link to the pharmacy to have prescriptions filled.
- The medical information site may be viewed as violating the federal anti-kickback statute if payments are being made to induce the referral of services (like pharmaceuticals) reimbursed by the Medicare program.
- Office of Inspector has not demonstrated an interest in cyberspace fraud and abuse — yet.

Hospital–Physician Networks

- Hospitals and health systems may wish to place hardware and software in the hands of affiliated physicians.
- These arrangements raise difficult issues under the federal anti-kickback statute, the Stark statute and state analogs.
- Network arrangements may also raise private inurement and private benefit issues for tax-exempt hospitals.

Hospital–Physician Networks (cont'd)

- Personal uses of the equipment should be limited.
- Turning a blind eye to personal uses and add-on of personal hardware and software is problematic.
- Unfortunately, good intentions are not an excuse.

E-Health Ethics Initiatives

- Health on the Net Foundation's Code of Conduct for Medical Web Sites.
- Hi-Ethics Alliance.
- Internet Healthcare Coalition draft "International e-Health Code of Ethics."

E-Health Ethical Issues

- Disclosure of financial relationships.
- Distinguishing content from advertising.
- Utilizing credible sources of medical information and providing authoritative attribution of sources.

Provider-Sponsored Sites

- Web sites intended to operate as a business may become entwined with healthcare regulatory issues when providers are involved.
- For this reason, many providers operate web sites through separate legal entities that do not directly provide healthcare services.

Davis Wright Tremaine LLP

It May Be Legal, But Is It Ethical?

- A theme that will probably be repeated in the e-health arena: entrepreneurial providers whose actions are called into question based upon the "white coat syndrome."
- Healthcare providers are not judged by the same ethical (and legal) standards as other business people — particularly when they are engaged in activities related to the healthcare profession.

Davis Wright Tremaine LLP

Part III

HIPAA Electronic Data Security and Privacy Standards

Background

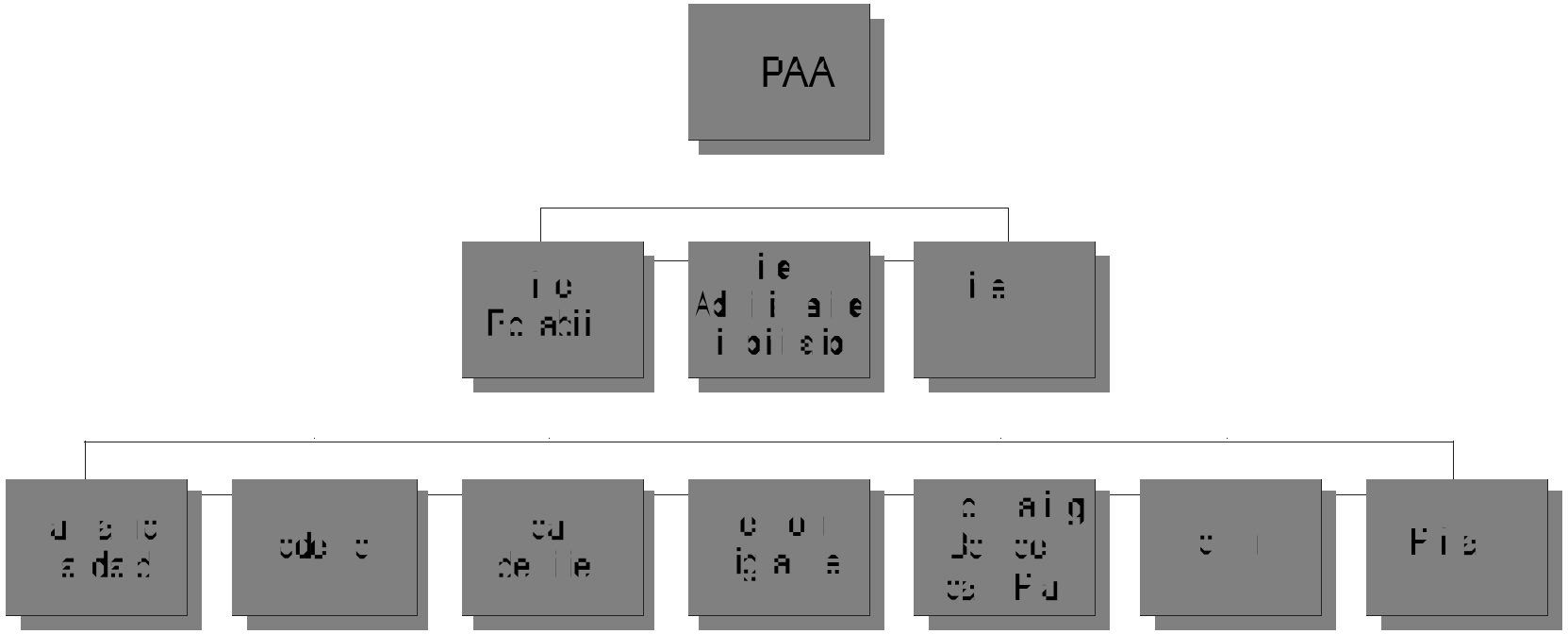
- High administrative costs
- Administrative costs summit
  - Stakeholder buy-in
  - Workgroup on electronic data interchange.
- Health care reform
  - Failure of Clinton plan
  - Kassebaum-Kennedy incremental reforms bill.

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

- Public Law 104-191 (August 21, 1996)
- Goals:
  - Assure health insurance portability
  - Reduce fraud and abuse
  - Establish uniform standards for health information transmission and use
  - Security and privacy of health information.

Davis Wright Tremaine LLP

HIPAA — Not Just One Issue



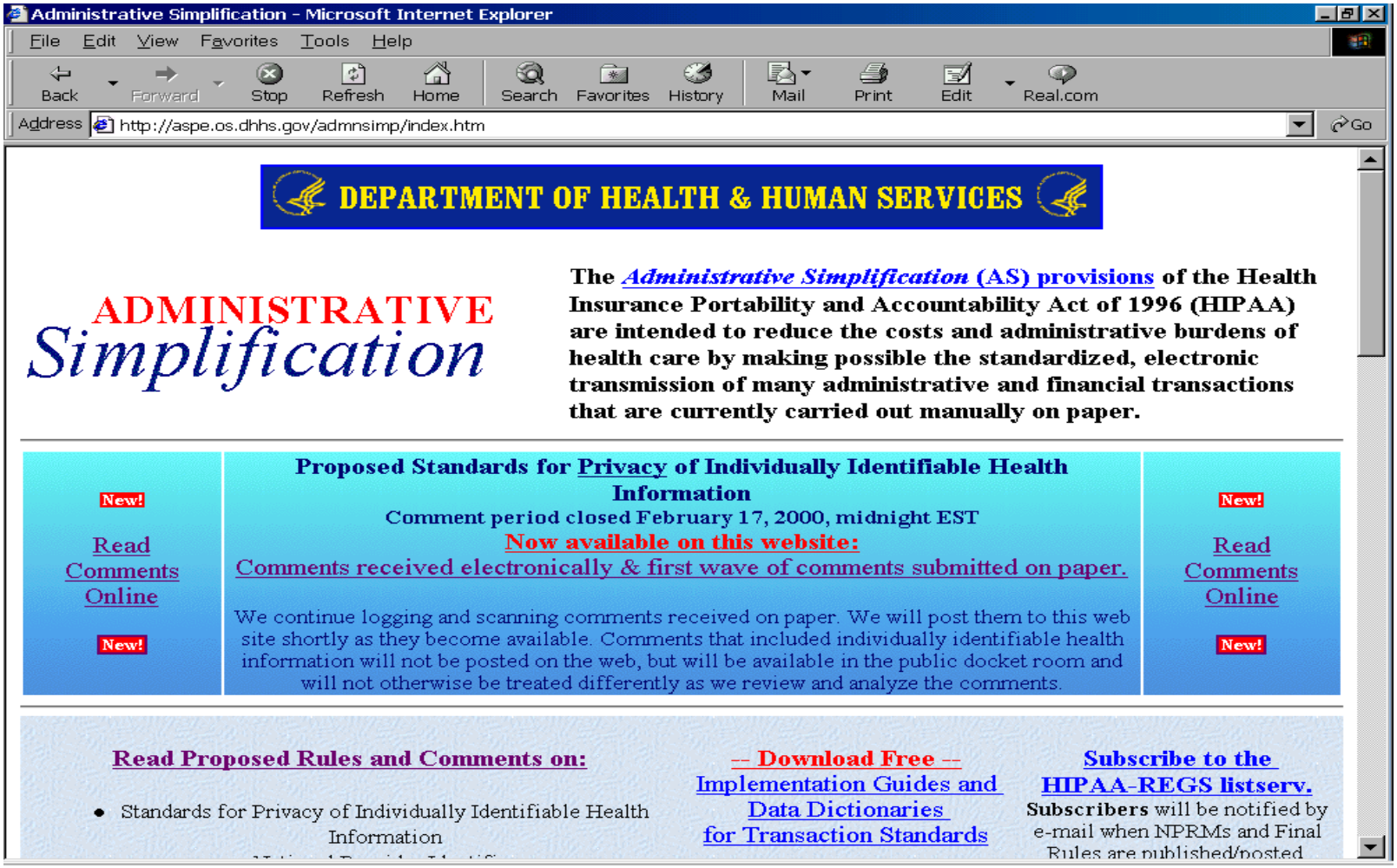
Administrative Simplification

- Streamline costs through standardization —
  - Transaction standards
  - Code sets
  - Unique health identifiers
  - Information sharing between health plans
  - Electronic signature standards
  - Security standards
  - Privacy legislation.

Davis Wright Tremaine LLP

Administrative Simplification

http://aspe.os.dhhs.gov/admnsimp/index.htm



Davis Wright Tremaine LLP

Goal

"Any standard adopted . . . shall be consistent with the objective of reducing the administrative costs of providing and paying for health care."

—Public Law 104-191

Applicability

- Health Plans
  - Plans that provide or pay for medical care
  - Self-insured employers.
- Providers
  - Providers of medical health services
  - Any other person furnishing health care services or supplies.
- Health Care Clearinghouses
  - Entities that process or facilitate processing non-standard data elements into standard data elements.

Implementation

- Consultation
- Proposed rules
  - Issued for public comment
  - Some proposed rules already published.
- Final rules
  - Consideration of pubic comments
  - No final rules published yet
  - Awaiting revised publication dates.
- Mandatory compliance 24 months after publication of final rules.

Timetable — Information System Regulations

Standard	Proposed Rule Publication Date	Expected Final Rule Publication Date	Expected Compliance Date
Transactions and Code Sets	5/07/1998	6/2000	8/2002
National Provider Identifier	5/07/1998		
National Employer Identifier	6/16/1998		
Security	8/12/1998		
Privacy	11/3/1999		
National Health Plan Identifier			
Claims Attachments			
National Individual Identifier	On hold	On hold	On hold

What's Covered?

- Individually identifiable health information that is — *or was* — in electronic format.
- Not purely paper transactions (i.e., never in electronic format).

Transaction Standards

Health plans must be able to handle the following transactions electronically (providers *may*):

- Claims or encounter information
- Claims attachments
- Payments and remittances
- Eligibility
- Enrollment/disenrollment
- Premium payments
- First report of injury (deferred)
- Health claim status
- Referral certification and authorization

Transaction Standards: Requirements

- Health Plans must have capability to send electronic transactions via designated standard transaction using standard code sets and unique identifiers.
- Providers must use designated standard transaction using standard code sets and unique identifiers, ***if*** they choose to use electronic transactions.

Code Sets

Define data element values (both content and format) values in std transactions (can't ask for additional info or different format). Includes:

- ICD-9-CM (not ICD-10)
- HCPCS
- CPT-4 (not CPT-5)
- Claim Adjustment Reason Code
- Diagnosis Related Group Number (DRG)
- Admission Source Code
- Admission Type code
- Claim Frequency Code
- National Drug Code by Format
- HCFA Claim Payment Remark Codes

Unique Health Identifiers

- Identifiers to be created:
  - Providers
  - Employers
  - Payers
  - Individuals (on hold).
- Identifiers will be "intelligence-free."

Electronic Signature Standards

- Standards for electronic transmission and authentication of health information.
- Applies when HIPAA-specified transaction requires electronic signature.
- Not required by any of the current transaction standards.

Security Standards

- Applies to health information whether or not identifiable:
- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security for network communications.

Davis Wright Tremaine LLP

Administrative Procedures

- Sets standards for:
  - Certification
  - Chain of Trust Agreements
  - Contingency Planning
  - Record Processing
  - Info Access control
  - Internal Audit
  - Personal Security
  - Security Config.
  - Security Incident
  - Security Mgmt
  - Termination Procedures
  - Training!

Physical Safeguards

- Governs physical security and organization issues:
  - Assigned Security Responsibility
  - Media controls
  - Physical access controls
  - Policy/guideline on workstation use
  - Security workstation location
  - Security awareness training.

Technical Security Services

- General security safeguards
- Standards covered:
  - Access Control
  - Authorization Control
  - Data Authentication (Integrity)
  - Entity Authentication.

Davis Wright Tremaine LLP

Technical Security for Network Communications

- Basic networking safeguards
- Addresses two network security issues:
  - Integrity (corruption) and confidentiality (interception)
  - Protect from unauthorized access.

Davis Wright Tremaine LLP

Electronic Data Security Compliance Plans

- Not one-size-fits-all — some measures not required
  - Conduct systems audit to identify risks
  - Develop security policies, confidentiality standards and access controls
  - Review and update policies periodically.
- If contract with a vendor or partner to handle health information through electronic transactions?
  - Enter into a security agreement disclosing electronic data security standards and requiring compliance.

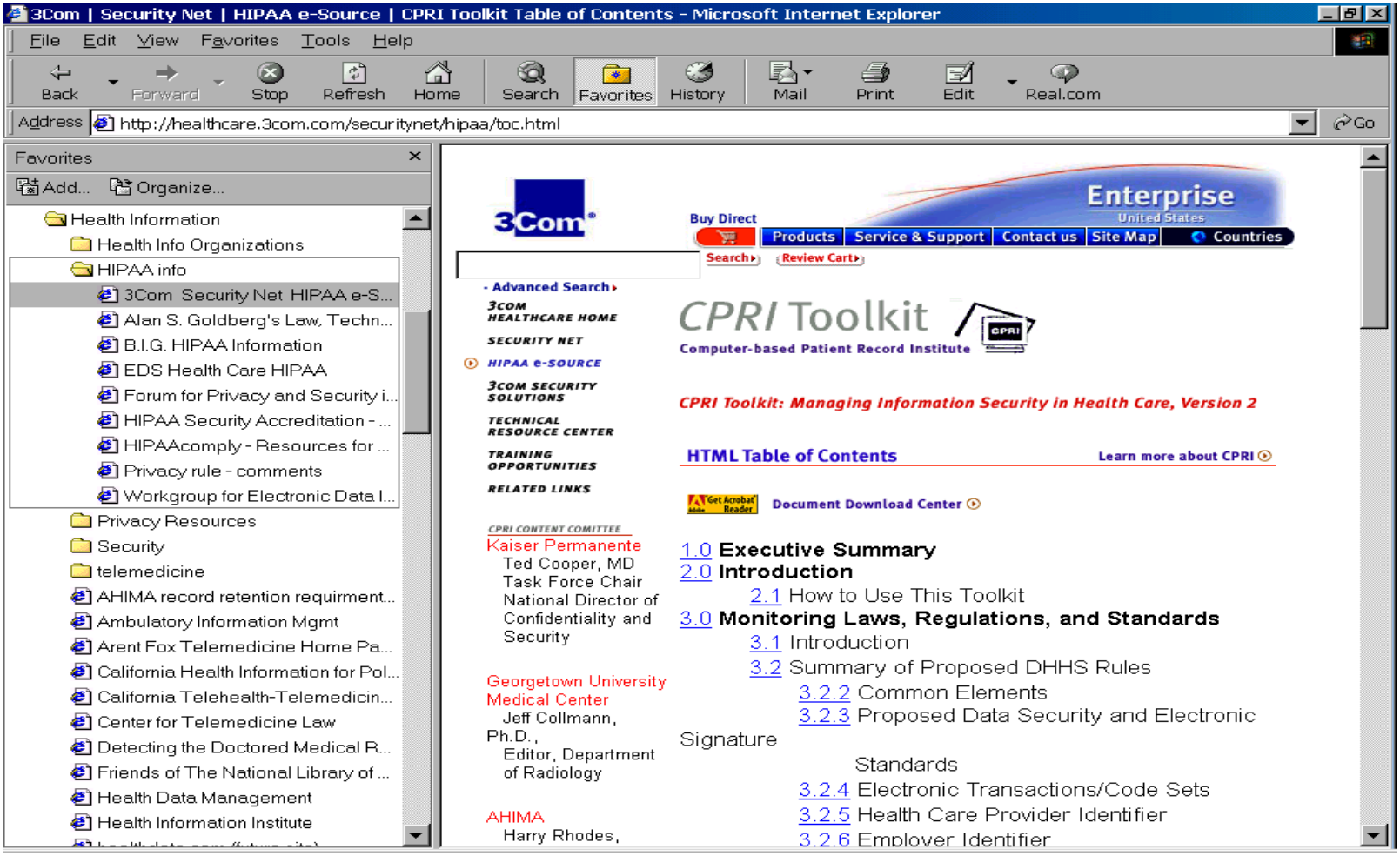
Electronic Data Security Compliance Plans (cont'd)

- Adopt security management practices and procedures:
  - Inventory of computer assets
  - Policies for installing/maintaining hardware & software
  - Locks and keys on computer systems
  - Access controls
  - Callback procedures to verify user identity
  - Passwords
  - Authentication procedures to verify user identity
  - Automatic logoff after periods of inactivity
  - Recording audit trails.

Davis Wright Tremaine LLP

Security Toolkit

http://healthcare.3com.com/securitynet/hipaa/toc.html



Privacy Standards

- Secretary of DHHS required to promulgate regulations if Congress did not act by Aug '99
- Proposed rules published November 3, 1999
- Comment period closed February 17, 2000
  - Record # of comments received
- Final rule by ???

Davis Wright Tremaine LLP

Privacy Standards

- Privacy standards cover:
  - Individually identifiable health information that is — *or was* — in electronic format.
  - Maintained by "covered entities"
    - Health care providers
    - Health plans
    - Health care clearinghouses.

Davis Wright Tremaine LLP

What Information Is Covered?

- New: Protected Health Information ("PHI"):
  - Created or received by a covered entity
  - Relating to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or future payment for such care.
  - At some point has been in electronic format
    - Key: look for computer
    - Fax? Telephone calls?

Privacy — General Rules

- May not use or disclose PHI except:
  - as authorized by patient
  - as permitted or required by regulation.
- PHI may be used within entity for treatment and payment.
- PHI may be disclosed for "national priority" purposes.
- Written authorization required for most other disclosures of PHI.

General Rules (cont'd)

- New Concepts:
  - Disclosure restricted to "minimum necessary" to accomplish purpose
  - "Business partners"
  - Notice of information practices
  - Creation of patient information rights
  - Accounting of disclosures
  - Authorization form specifications
  - Standards for "de-identification."

Minimum Necessary

- CE must make "all reasonable efforts" not to use or disclose more than the minimum PHI necessary.
- Exceptions:
  - Release authorized or for individual's own review
  - Compliance with other HIPAA requirements
  - Required by law and may disclose w/o authorization
  - Release to health plan for audit purposes.
- Determination made on individual basis (within entity's technological capabilities).

Davis Wright Tremaine LLP

National Priority Activities

- PHI may/must be disclosed without authorization for specified national priority activities:
  - Health care system oversight
  - Public health
  - Judicial/administrative proceedings
  - Law enforcement
  - Next-of-kin
  - ID of deceased person
  - Gov't health data systems
  - Facility directories
  - Financial institutions.

Business Partners

- Business Partners: Individuals and entities that perform or assist covered entities with a function or activity and receive PHI.
  - E.g.: lawyers, auditors, consultants, TPAs, clearinghouses, and data processing and billing firms.
- Written assurance (chain of trust agreement)
  - Specified confidentiality assurances
  - Breach of agreement imputed to the covered entity
  - Individuals as third party beneficiaries.

Chain of Trust Agreements

- Covered entity is liable for business partner's breach if —
  - covered entity "knew or reasonably should have known" and
  - failed to take reasonable steps to cure
- How much diligence and monitoring required?

Davis Wright Tremaine LLP

Chain of Trust Agreement Terms

- No use or disclosure of PHI not permitted for CE.
- Appropriate privacy and security safeguards.
- Report unauthorized disclosures to CE.
- Ensure subcontractors comply.
- Make PHI available to CE as necessary to allow individuals to exercise their right of access.
- Return or destroy all PHI upon termination.

Notice of Information Practices

- CE must provide patients with written notice of information practices
  - Plain language
  - Practices for handling/using PHI
  - Sufficient detail to put the patient on notice of the uses and disclosures to be made PHI
  - Patients' rights with respect to PHI.

Patient Rights

- Right to written notice of information practices.
- Right to access, inspect, and obtain copies.
- Right to request non-disclosure.
- Right to request corrections and amendments.
- Right to accounting of disclosures.

Accounting of Disclosures

- Accounting includes:
  - Date of disclosure
  - Recipient name and address
  - Description of information disclosed
  - Purpose of disclosure
  - Copies of all disclosure requests.
- Exceptions:
  - Treatment, payment and healthcare operations
  - Health oversight or law enforcement agencies (sometimes).

Authorization Forms

- Detailed requirements for forms authorizing the release of PHI.
- Requirements differ depending upon —
  - Authorization initiated by covered entity
  - Authorization initiated by individual
- Sample forms in the regulations.

Davis Wright Tremaine LLP

De-Identification

- Confidentiality requirements do not apply to health information that has been "de-identified."
- Must remove, by removing, coding, encrypting, or otherwise eliminating or concealing, all individually identifiable information.

De-Identification

- Presumption that information is not individually identifiable if certain information is removed or otherwise concealed:

Name	Address & zip	Relatives
Employer	DOB	Tel/Fax
E-mail	SSN	MR#
Health Plan ID	Account #	Vehicle ID
Certificate or license #	URL or IP address	Finger or voice print
Photo	Other	

Administrative Procedures

- CEs must have policies, procedures, and systems to protect health information and individual rights.
  - Designation of a privacy officer
  - Privacy training for employees
  - Safeguards to prevent intentional or accidental misuse of PHI
  - Means for individuals to lodge complaints
  - Sanctions for employee violations.

Preemption of State Law

- HIPAA preempts all "contrary" state laws unless a state law is "more stringent."
- Contrary —
  - State law is "contrary" when an entity cannot comply with both it and HIPAA requirements or when state law is an obstacle to the purposes and objectives of HIPAA.
  - States may apply to DHHS for time-limited exceptions if laws promote impt state interests.

Preemption (cont'd)

- State law is "more stringent" if —
  - Stricter limits on use or disclosure
  - Gives individuals greater rights of access (except for minors)
  - Harsher penalties for unauthorized disclosure
  - Greater information or rights to individuals regarding use or disclosure
  - Stricter terms for authorizing disclosure
  - Stricter standards of record-keeping or accounting.

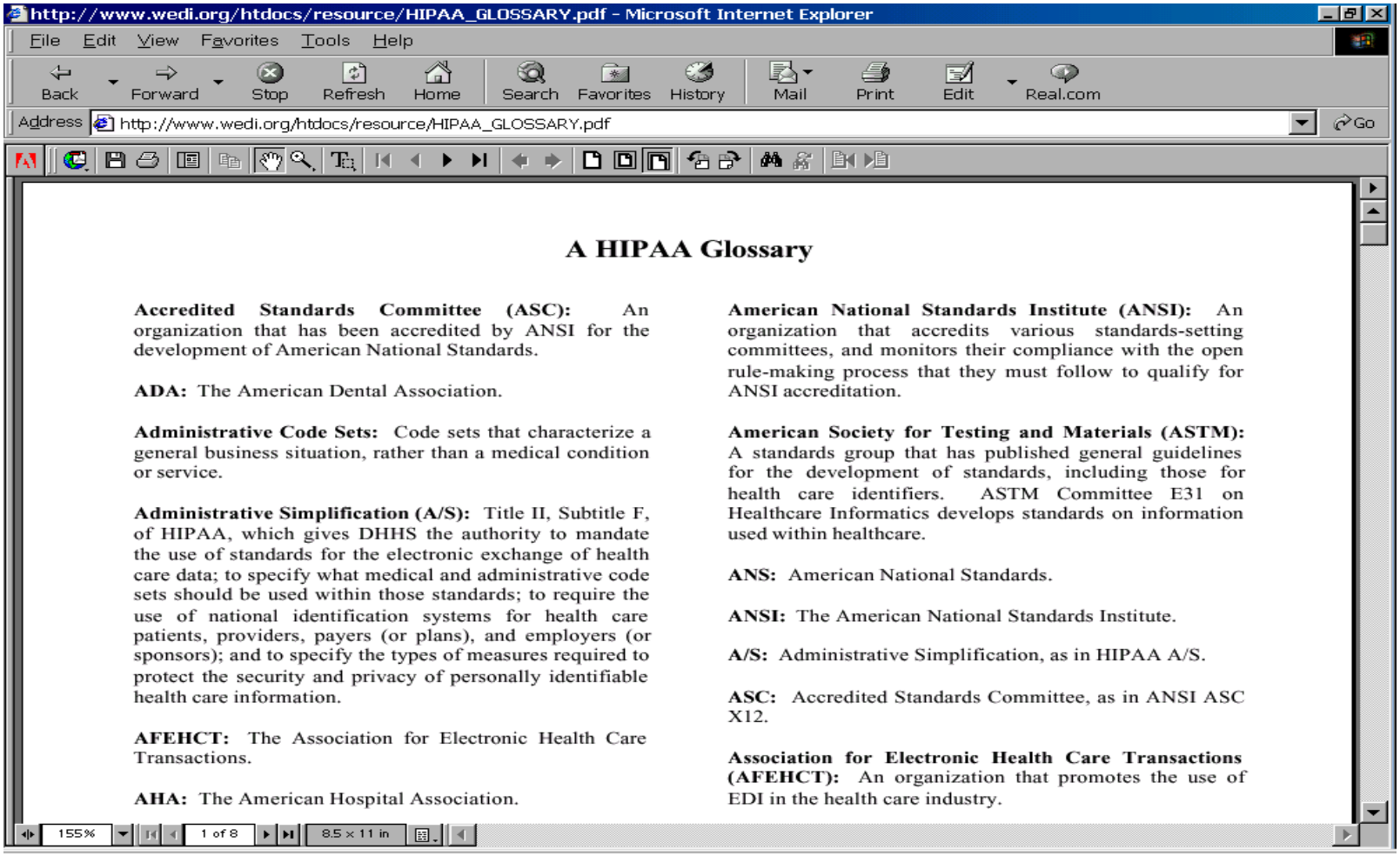
Davis Wright Tremaine LLP

Enforcement

- CMPs against covered entities that fail to comply
  - $100 per violation — not to exceed $25,000/year.
- Criminal penalties for knowingly disclosing health information in violation of HIPAA:
  - Wrongful disclosure: fine $\leq$ $50,000, prison $\leq$ 1 yr
  - False pretenses: fine $\leq$ $100,000, prison $\leq$ 5 yrs
  - Use for commercial or personal gain or malicious harm: fine < $250,000, prison $\leq$ 10 yrs.

HIPAA Glossary

www.wedi.org/htdocs/resource/hipaa_glossary.pdf



A HIPAA Glossary

Accredited Standards Committee (ASC): An organization that has been accredited by ANSI for the development of American National Standards.

ADA: The American Dental Association.

Administrative Code Sets: Code sets that characterize a general business situation, rather than a medical condition or service.

Administrative Simplification (A/S): Title II, Subtitle F, of HIPAA, which gives DHHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.

AFEHCT: The Association for Electronic Health Care Transactions.

AHA: The American Hospital Association.

American National Standards Institute (ANSI): An organization that accredits various standards-setting committees, and monitors their compliance with the open rule-making process that they must follow to qualify for ANSI accreditation.

American Society for Testing and Materials (ASTM): A standards group that has published general guidelines for the development of standards, including those for health care identifiers. ASTM Committee E31 on Healthcare Informatics develops standards on information used within healthcare.

ANS: American National Standards.

ANSI: The American National Standards Institute.

A/S: Administrative Simplification, as in HIPAA A/S.

ASC: Accredited Standards Committee, as in ANSI ASC X12.

Association for Electronic Health Care Transactions (AFEHCT): An organization that promotes the use of EDI in the health care industry.

HIPAA Resources

- DHHS — Administrative Simplification
  - http://aspe.os.dhhs.gov/admnsimp/index.htm
- Workgroup for Electronic Data Interchange
  - http://www.wedi.org/
- Health Privacy Project
  - http://www.healthprivacy.org/

Part IV

Website Legal Audit

Legal Audit of Provider Websites

- The law of the Internet changes rapidly — so do the content and functions of most sites.
- Compliance is a moving target.
- Periodic legal audits, including updates to privacy policies and terms of use, are a virtual necessity.

Internet Legal Audit

1. Do you have a written agreement with your web site developer that addresses these issues?

- Protection of your ownership of all intellectual property developed in connection with the site, including all code and graphics developed specifically for your site.
- Your license to use (without payment of royalties) any prior intellectual property the developer owns that is it is bundling or using in your site.
- The developer's duty to fix any bugs or faulty links, including the time frame for necessary corrections.

Internet Legal Audit (cont'd)

2. Do you collect personal data regarding users?

- If so, you should be aware of current and proposed laws governing use of personal data, including the European Union Privacy Directive, The Electronic Funds Transfer Act, The Fair Credit Reporting Act and The Children's Online Privacy Protection Act.

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

3. Do you have a policy regarding maintaining privacy of personal data? Is it sufficiently accessible to users?

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

4. Are you sure that you own the intellectual property or other content offered on your site?

- Was the content developed by your employees as a work-for-hire?
- Was the content developed by independent contractors who have assigned their rights to you?
- If the content was created by third parties, do you have a procedure for obtaining necessary clearances? Do you need to retain a clearance service to perform this function?

Internet Legal Audit (cont'd)

5. Have you placed a copyright notice on your site? Have you considered periodically registering the evolving content of your site with the U.S. Copyright Office?

Internet Legal Audit (cont'd)

6. Have you considered registering an agent for notice of claimed infringements with the U.S. Copyright Office under the Digital Millennium Copyright Act?

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

7. Have you patented any technology that is made available through your site?

- Do you qualify for a business process patent?

Internet Legal Audit (cont'd)

8. Have you considered registering your domain name as a trademark?

Internet Legal Audit (cont'd)

9. Do you send unsolicited commercial email ("spam")? If so, you should be aware of the growing body of case law, Federal Trade Commission regulations and state statutes applicable to spamming.

Internet Legal Audit (cont'd)

10. Have you considered in which jurisdictions your business may be sued? Have you taken appropriate measures to limit those jurisdictions through disclaimers or other measures?

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

11. Have you considered in which jurisdictions you may be subject to state and local taxation? Have you take measures to limit those jurisdictions through properly structuring your sales operations?

Internet Legal Audit (cont'd)

12. If your site contains hypertext links or frames, have the links or frames been constructed in a manner that minimizes your potential liability with respect to trademark infringement, trademark dilution and unfair competition claims?

Internet Legal Audit (cont'd)

13. Does your site include appropriate disclaimers with respect to:

- Liability arising from inaccurate information provided through the site?
- Warranties of merchantability and fitness for a particular purpose for goods offered through the site?
- Liability arising from content made available through hyperlinks to other sites?

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

14. Have you taken appropriate measures to ensure that any online contracts are binding and enforceable?

- Does the online contract include all key terms and conditions for the provision of your goods or services?
- Is the online contract conspicuously displayed and available to customers?
- Do you maintain records of each customer's assent to the online contract?
- Does the online contract limit the remedies and damages available to a disgruntled customer?

Internet Legal Audit (cont'd)

15. If you engage in e-commerce, are your refund and return policies appropriately disclosed to customers? Have you considered whether you must comply with state laws regarding Internet refund and return policies, such as California Business and Professions Code Section 17538?

Internet Legal Audit (cont'd)

16. Have you reviewed your Internet advertising for compliance with state and federal laws regarding false and deceptive advertising?

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

17. Have you implemented reasonable security and encryption measures to protect your company's client information and other confidential and proprietary information?

Internet Legal Audit (cont'd)

18. Do you have actual knowledge that you receive personal information from children under age 13? If so, you may be required to comply with the Children's Online Privacy Protection Act ("COPPA").

Davis Wright Tremaine LLP

Internet Legal Audit (cont'd)

19. Do you collect or transmit patient identifiable information? If so, you should develop policies and procedures for compliance with the proposed Health Insurance Portability and Accountability Act of 1996 electronic data security and privacy standards, the HCFA Internet Security Policy and applicable state medical records privacy laws.

Internet Legal Audit (cont'd)

20. Is medical information or advice provided through your site? If so, you should consider whether such activities may constitute the practice of medicine or another licensed profession.

Internet Legal Audit (cont'd)

21. Do you operate a medical chat room or message board? If so, you should assess the potential liabilities arising from erroneous medical information provided by users, consider appropriate disclaimers and evaluate whether chat room or message board communications should be monitored or moderated.

Internet Legal Audit (cont'd)

22. Do you provide a product, such as clinical diagnostic software, that may constitute a medical device subject to FDA regulation?

Internet Legal Audit (cont'd)

23. Should your site consider compliance with the Americans with Disabilities Act?

Internet Legal Audit (cont'd)

24. Does your site involve transactions between healthcare providers, whether through e-commerce, advertising or in-kind exchanges? If so, you should consider whether your site complies with the federal Stark II statute and applicable state laws prohibiting self-referrals.

Internet Legal Audit (cont'd)

25. Does your site directly or indirectly relate to the referral of patients? If so, you should consider whether your site complies with the federal anti-kickback statute and applicable state laws prohibiting payments for patient referrals.

Internet Legal Audit (cont'd)

26. Do you have an insurance policy that addresses liabilities arising from web site operations?