VLANs, Authenticted VLANs and Firewalls:

Tools for Complying with HIPAA's Security and Confidentiality Requirements

Joint White Paper By:

Alan Amrod
Executive Director
North America Field Marketing

and

John A. Knapp, Esq.
Shahram M. Siddiqui, Esq.

> Americans treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the Global Information Infrastructure's great promise -- that it facilitates the collection, re-use and instantaneous transmission of information -- can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

— Joint statement by President William Clinton and Vice-President Al Gore.

The Unites States Supreme Court has interpreted the Constitution to include a right to privacy for every American.[i] Our belief in this right is deeply rooted in both our traditions and our laws. In no area is this right more cherished than in the area of an individual's private health information.[ii]

Today, the health information of most Americans is electronically stored, maintained and transmitted by doctors, hospitals, laboratories, clinics, insurance companies and managed care organizations for diagnosis, billing and other purposes. In many cases these same organizations also share this information with universities and drug manufacturers for use in medical research. As a result of these proliferating uses for health information, it is becoming increasingly difficult for a modern-day healthcare organization to guaranty the information's security and confidentiality.

As many healthcare organizations drive towards openly sharing health information across an enterprise, the number and scope of breaches in the security and confidentiality of health information will only increase. Thus, it is imperative for any healthcare organization to temper its use of the health information in its possession with assurances that the information is being stored, shared and accessed in a policy-based and secure manner.

Historically, the legal controls over health information have been the purview of state law. Every state has legal controls on the use and disclosure of health information. Many states have laws which protect special classes of health information, such as HIV infection and mental health information.[iii] Some states impose confidentiality duties upon those individuals or organizations who maintain or control private health care information.[iv] And a few states have established additional or different security standards for the electronic storage and transmission of health information.[v] However, the scope and strength of these state laws vary greatly.

In 1996, Congress enacted the Health Care Insurance Portability and Accountability Act ("HIPAA").[vi] Originally dubbed the Kennedy-Kassebaum legislation, HIPAA is widely-known for its provisions which permit the portability of health insurance. However, HIPAA's other less well known provisions address issues of administrative simplification and the privacy and confidentiality of electronically stored and transmitted health information.

When it enacted HIPAA's portability provisions, Congress recognized that the procedures for filing and paying health insurance claims were too cumbersome. Therefore, Congress delegated to the Department of Health and Human Services ("DHHS") the authority to issue administrative regulations simplifying the claims procedures and encouraging the use of electronic claims.

A by-product of this encouragement, however, is the need to establish security guidelines for the electronic storage and transmission of health information and for ensuring its privacy and confidentiality. HIPAA attempts to accomplish this by replacing the patchwork of state laws which currently govern the security of heath information with uniform federal administrative regulations. Moreover, HIPAA begins to addresses the concerns surrounding the privacy of health information by requiring DHHS to make recommendations for federal privacy legislation regulating its confidentiality and disclosure.

In September of 1997, DHHS presented its federal privacy legislation recommendations to Congress and in August of 1998, it issued its proposed security standard regulations.

Now, before these administrative regulations become effective and before the legislative process reaches its conclusion, is the time for every healthcare organization to begin the process of integrating the concepts of security and privacy into their daily routines. The first step towards creating such a security-conscious healthcare organization is a "buy-in" from management, which is subsequently driven down to the level of individual accountability. HIPAA requires management to devise, implement and monitor security and privacy polices, procedures and systems to protect all health information in that organization's possession from exposure, disclosure or inappropriate use.

The next step toward implementing security awareness must occur on a daily basis at a very basic level throughout the healthcare organization. The level must be so basic that neither healthcare providers nor healthcare support staff can start a shift without physically and visually becoming security-aware at a hands-on level. A technology called "authenticated virtual local area networks," more commonly referred to as authenticated VLANs, can help develop this basic level of security awareness. Coupled with firewall technology, authenticated VLANs can provide a comprehensive mechanism for securing health information while still promoting the level of information exchange necessary for comprehensive patient care.

The legislative impact of HIPAA and the policies, processes, and systems that it requires healthcare organizations to implement could significantly dwarf the expenses currently associated with the Year 2000 problem ("Y2K"). Y2K expenses are consuming nearly 25 cents of every health care information technology dollar spent in Fiscal Years 1997, 1998 and 1999.[vii] In the future, expenditures on security and confidentiality of health information will become an annual healthcare industry budgetary line item. This line item will include the continuing costs of training, evaluating, inspecting, and upgrading the healthcare organization's security and confidentiality polices and systems.

This paper only addresses HIPAA's security and privacy provisions. Part I of this paper reviews the proposed administrative regulations which establish the security standards for the electronic storage and transmission of health information. Part II summarizes DHHS' privacy recommendations and reviews their current legislative status. Part III provides an in-depth discussion of authenticated VLANs and firewall technology and their potential applicability to a healthcare organization's HIPAA compliance strategies.

Part I
Security of Health Information

HIPAA's security standard requires every healthcare organization which electronically stores or transmits health information to maintain reasonable and appropriate security standards which (a) ensures the integrity and confidentiality of the information, (b) protects against any reasonably anticipated threats and hazards to the security or integrity of the information, and (c) prevents unauthorized access to and disclosure of the information. No distinction is made between internal and external communications.

The proposed regulations define the required security standard as a series of administrative, physical and technical objectives which every healthcare organization must achieve in their daily operations. By achieving these objectives, the healthcare organization will have provided the minimum level of security and confidentiality required by HIPAA. The means of achieving these objectives are, however, left to the discretion of the individual healthcare organization.

The security standard proposed by the regulations does not reference or advocate a specific technology. By omitting references to specific technologies, the regulations have created a security standard which appears to be flexible enough to take advantage of future technological advancements. Moreover, the standard does not address the extent to which a particular healthcare organization must implement any of the security standards. Instead, the proposed regulations require each affected entity to assess its own security needs and risks, and to devise, implement, and maintain those security standards appropriate to that healthcare organization's needs.

Satisfying HIPAA's security standard and deciding on the appropriate technology to meet this standard is a business decision which each healthcare organization will have to make. Inherent in this process is a critical need to strike a balance between the need to secure health information against the risks and the economic costs of doing so.

Each healthcare organization must utilize a combination of the security standard objectives as a means to safeguard the integrity, confidently, and availability of its health information. A healthcare organization must document and keep current whichever security objectives it may chose to implement. The proposed security objectives are:

(A) **Administrative Procedures**. These are documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of this data;

(B) **Physical Safeguards**. These relate to the protection of the physical computer systems and related buildings and equipment from fire and other natural and environmental hazards. This also includes the use of locks, keys and administrative measures used to control access to computer systems and facilities;

(C) **Technical Security Services**. These include the processes that are put in place to protect, control and monitor information access; and

(D) **Technical Security Mechanisms**. These include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

The relative importance of each objective depends on the individual characteristics and needs of each healthcare organization. Therefore, a small healthcare organization's implementation of only the administrative and physical objectives may be appropriate, whereas a large healthcare organization's implementation of only these two could be insufficient.

The proposed regulations do not impose any accountability or responsibility upon vendors of hardware or software to provide the functionality to enable healthcare organizations to comply with HIPAA. Their products are not required to be designed to meet any of HIPAA's security objectives. Therefore, virtually the entire expense and responsibility for compliance will fall on the healthcare industry.

The proposed security standard would also supersede contrary provisions of State law, including any State law which requires health information to be maintained or transmitted in other electronic formats.[viii] Healthcare organizations would only be required to meet one set of security standards rather than two potentially competing standards. There are certain exceptions to this preemption; however, these exceptions require specific determinations by the Secretary of the DHHS (the "Secretary").

The failure of any healthcare organization to comply with the security standards could result in the assessment of civil penalties. HIPAA provides for penalties of not more than $100 per violation, with the total assessment imposed in each calendar year not exceeding $25,000 for any one violation.[ix] DHHS has, at this time, not proposed any enforcement procedures for HIPAA's security standard. It has, however, stated that it envisions the "monitoring and enforcement process as a partnership between the Federal government and the private sector."[x]

Any security standard which is ultimately adopted would become law 24 months after its effective date, with small health plans[xi] being required to comply within 36 months.[xii] The security standards contained in the proposed regulations were first published in August of 1998 and the comment period for the standards closed in October of 1998. Therefore, these regulations, as modified by comments, should become effective in the near future.

Part II
Confidentiality of Health Information

> The fears of invasion of privacy, as a consequence of inexorable forces seemingly out of the control of the average American, has risen to a major public policy issue.
>
> — Alan Greenspan, March 7, 1997.

HIPAA requires the Secretary to provide Congress with recommendations for Federal legislation regulating the confidentiality of health information. These recommendations must address the rights of individuals, the procedures that should be established for the exercise of individual rights, and the uses and disclosures of such information that should be authorized or required.

The Secretary reported her recommendations to Congress in September of 1997.[xiii] The Secretary's findings state that establishing a basic national standard of confidentiality is necessary to provide rights for patients and to define the responsibilities for record keepers. The blanket authorizations often used today do not protect Americans, in part because these releases do not provide useful information about how the health information will be used, who will see it, or how the individual can get access to the information. The Secretary's report encourages Congress to replace the ineffective use of authorizations with a system of Federal legislative controls.

The Secretary recommended that Congress enact a broad Federal privacy law which prohibits the disclosure of identifiable health information except as authorized by the individual or as explicitly permitted or required by law. The disclosure of health information would be limited to the minimum amount necessary to accomplish the purpose of the disclosure, and the information would be used only for the purposes for which it was collected or disseminated.

The Secretary's recommendations are founded on five key principles:

(1) **Boundaries**. An individual's health information should be used only for health purposes. Any federal legislation should impose a legal duty of confidentiality on healthcare organizations that receive health information.

(2) **Security**. Organizations to which health information is entrusted ought to protect it against deliberate or inadvertent misuse or disclosure.

(3) **Consumer Control**. Individuals should be able to see their health information, get copies of any health records, correct errors, and find out who else has seen the information.

(4) **Accountability**. Those who misuse health information should be punished, and those who are harmed by its misuse should have legal recourse.

(5) **Public Responsibility**. An individual's claims to privacy must be balanced against their public responsibility to contribute to the common good, through the use of their information for important, socially useful programs, with the understanding that their information will be used with respect and care and will be legally protected. Federal law should identify those limited arenas in which the individuals public responsibilities warrant authorization of access to health information, and should sharply limit the uses and disclosures of information in those contexts.

The Federal privacy legislation recommended by the Secretary does not require the disclosure of any information, except to the individual who asks to see his or her own health information. The recommended allowable disclosures are just that -- allowable. For disclosures that are not compelled by other law, healthcare organizations would be free to deny disclosure according to their own policies.

If a healthcare organization were to receive health information without an individual's authorization, that organization would be permitted to use the information only for purposes compatible with and directly related to the purposes for which the information was collected or received. These same healthcare organizations would be required to maintain reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity and confidentiality of the health information in their possession.

The Secretary also recommended both civil and criminal penalties. If any individual's confidentiality rights are knowingly or negligently violated, that individual would be permitted to bring an action in federal court, or any other court of competent jurisdiction, for damages and equitable relief. Damages would encompasses non-pecuniary losses, such as physical or mental injury, as well as pecuniary losses. In the case of a knowing violation, attorneys' fees and punitive damages would also be available.

Criminal penalties (including a fine and imprisonment) would be available, at a felony level, for anyone obtaining health information under false pretense, for knowingly and unlawfully obtaining health information, and for knowingly and unlawfully using or disclosing health information. Penalties would also be higher for any of these acts performed for profit or monetary gain.

HIPAA requires Congress to enact Federal privacy legislation before August of 1999.[xiv] This legislation may, but is not required to be, based upon the Secretary's recommendations. Congress' failure to enact legislation by this deadline would allow DHHS to impose privacy and confidentiality rules by administrative regulations.[xv] Though DHHS has not yet proposed any administrative regulations because there are a number of bills presently pending in Congress, it recently established an interagency working group to begin drafting such regulations.

Shortly after the Secretary's report, a series of Congressional bills were introduced to implement the recommendations. The authors of this article have attempted to summarize the pending legislation below. However, given the fluid nature of the legislative process, it is very likely that this summary will be out-of-date prior to the publication of this article. The summary is accurate only as the date this piece was prepared. Current versions of these legislative initiatives may be obtained from the Congressional Web Site[xvi] or from the authors of this article.

Senate Bill 573[xvii] was introduced by Senator Patrick Leahy (D-Vermont), and an identical bill, House Resolution 1057,[xviii] was introduced by Representative Edward Markey (D-Mass.). These bills, entitled the Medical Information Privacy and Security Act of 1999, would (a) provide individuals with access to health information to which they are a subject; (b) ensure personal privacy with respect to healthcare-related information; (c) impose criminal and civil penalties for unauthorized use of health information; (d) provide for strong enforcement of such rights; and (e) protect State rights.

Additional legislation was also introduced in the Senate. These were Senate Bill 587,[xix] sponsored by Senator James Jeffords (R-Vermont), and Senate Bill 881,[xx] sponsored by Senator Robert Bennett (R-Utah). Both of these legislative initiatives either modify the Secretary's recommendations or added additional requirements. Subsequently, Senate Bills 573, 587 and 881

were combined into one new bill, entitled the Health Information Confidentiality Act of 1999.

As of May 25, 1999, the Senate Health, Education, Labor and Pensions Committee had postponed any additional consideration of the Health Information Confidentiality Act of 1999 in order to resolve issues that threatened to end the bill's bipartisan support.[xxi] As written, the Health Information Confidentiality Act of 1999 gives individuals the right to bring a civil action against whoever violated the confidentiality of their health information and to recover damages, punitive damages and attorneys' fees.[xxii] Republican senators hope to introduce a legislative amendment to eliminate this right[xxiii]

The Health Information Confidentiality Act of 1999 also provides for both criminal and civil penalties. Criminal penalties would range from fines of $50,000 to $500,000, with prison sentences ranging from one year to 10 years.[xxiv] Civil penalties would range from $500 to $100,000 per violation for actions brought by the Secretary or the Attorney General of the United States, and the greater of compensatory damages or $5,000 for actions brought by individuals..[xxv]

Since its introduction, no action has been taken by the House of Representatives with respect to House Resolution 1057. With only a few weeks left in which to enact privacy legislation, and in an effort to break the logjam with respect to this legislation, yet another bill was introduced in the House. This bill, House Resolution 1941[xxvi] and entitled the Health Information Privacy Act, was introduced by Representative Gary Condit (D-Calif.). On May 27, 1999, the House Commerce Committee's health and environmental subcommittee heard testimony from a wide range of parties interested in the resolution, including researchers and representatives from various segments of the healthcare industry. These interested parities have been unable to agree on the proper balance among the rights of patients to privacy, the interests of society in having access to the information and businesses such as insurance companies that rely on the data for efficient operation.

The Health Information Privacy Act would bar the use or disclosure of medical information without the subjects knowledge and consent, and it would give the individual the right to inspect, copy and amend the information.[xxvii] This resolution would also avoid preempting stronger state laws.[xxviii]

The civil and criminal penalties provided by this resolution differ from those proposed by the various Senate bills. In this resolution, the maximum civil penalty which could be assessed in any action brought by the Secretary would be $10,000 per violation.[xxix] In private civil actions, the claimant would be entitled to the lesser of actual damages of $5,000, plus punitive damages and attorneys' fees when the disclosure was knowingly made.[xxx] Criminal penalties would range from a maximum of 5 years for the knowing disclosure of private health information, to a maximum of 10 years for a disclosure made for profit or monetary gain.[xxxi]

Part III
Virtual Local Area Networks and Firewalls

As the implementation of HIPAA's security and confidentiality requirements looms in the not-to-distant future, no healthcare organization

can afford to have its health information network compromised. Historically, healthcare organizations have made limited use of either firewall technology to protect their information from external threats, or passwords and personal identification numbers to control and protect access to, and to authenticate internal users of, health information.

However, if HIPAA's proposed technical security standards are adopted without change, then many healthcare organizations will be required to deploy these, and other technical security measures, across their enterprises. The proposed regulations specifically note that the use of authentication technology may be utilized in complying with many of the technical security objectives. In particular, HIPAA addresses the use of user, role and context-based authentication, all of which utilize passwords, personal identification numbers, or both, along with several other options to secure health information.

A. About Authenticated VLANs

Virtual LANs in a switched network are a logical collection of network devices that are grouped into a common broadcast domain. VLANs ultimately appear as a subnet and can easily switch traffic around at wirespeed within the same broadcast domain or subnet. However, information will have to be routed if there is a requirement to send data between devices in different VLANs. Effectively, VLANs provide a cost-effective way of collapsing devices down into a broadcast domain or subnet without the use of an expensive router or even the use of complicated subnet masks, in many cases.

Authenticated VLANs are a flexible and powerful way to control the traffic that enters a switched network while also significantly improving the security of the network. Switched networks are increasing in popularity in healthcare because of bandwidth hungry applications and services that older shared and router-centric networks are incapable of delivering. Authenticated VLANs are a secure deterministic mechanism for adding and removing users from a mobile VLAN. Instead of grouping a user by data sent by an end-system, in an authenticated VLAN membership is based upon a user's identity and a set of policies defined by the network administrator, per the healthcare organization's guidelines. When a user is authenticated into a VLAN, he can only intercommunicate with other users and devices that have been similarly authenticated and joined into the VLAN. This is different from non-authenticated VLANs that rely on easily spoofed (counterfeited) layer-two and layer-three information to determine membership.

When a user that is connected to a port on a network first attempts communication, he or she must be successfully authenticated. After authentication, the user is placed in his or her predefined policy-based VLAN. At that point, the user is free to use his or her approved network resources.

Authenticated VLANs can extend network security to the wall plate. When authenticated VLANs are defined on switched networks, end-systems within those VLANs cannot send or receive traffic until they have been successfully authenticated. Authentication functionality can make network access completely deterministic; access can be limited by time of day and week rules and by any other means available by an authentication server. Static devices such as printers and image acquisition systems can be configured to operate

in a specific VLAN and only users who enter the proper identification and password would be allowed inside a VLAN with them.

Well-engineered authenticated VLANs will have event logging capabilities that provide useful information, such as where on the network users are connecting, or where someone is trying to break into the network. When an event occurs, the administrator can quickly determine where it is logically, and more importantly, where it is physically, on the network. The event log should also be used to track mobile users as they move around the network to see where people are logging in and doing their work.

Healthcare organizations will require the most feature-rich authenticated VLANs of any industry. Healthcare information technology organizations faces the monumental task of linking and securing a highly diverse and disparate set of applications and information systems to achieve HIPAA compliance and limit their organizations' liability. It is not uncommon for a healthcare information technology organization to support over a dozen different applications and their associated information systems; often, with limited or overburdened resources. Authentication and, subsequently, authenticated VLANs, can provide a flexible, highly manageable, and secure method of segmenting and protecting internal assets.

By placing high profile targets like pharmacy, laboratory, pathology, radiology, billing, etc., in their own VLANs and then applying an authentication scheme to them, network managers can effectively segment the network and limit potential internal breaches. Remember that routing must occur between VLANs, and therefore could lock-down the network not only by applying an authentication scheme, but also by limiting the routes between departments. Pharmacy and laboratory may have no need to directly communicate, but they may upload their information to a common clinical data repository gateway for use by providers across the enterprise.

B. About Firewalls

Firewall technology is a mature offering and is currently installed in many healthcare organizations around the world. It is most often associated with the need to protect internal resources from intrusion by way of the Internet or a dial-in link. However, firewall technology is equally effective for protecting highly sensitive or critical internal resources within a healthcare organization. It is prudent to protect your organization from external intrusion, but statistically a healthcare organization is far more likely to breach patient confidentiality by way of internal breaches. Statistically, a disgruntled employee, careless handling, or lack of awareness of security guidelines and procedures is far more likely to be an issue than a deliberate external attack on a healthcare organization's data.

In a switched network authenticated VLANs work on the principle of dynamically querying the user to obtain a password or personal identification number and matching it against an authentication server. When successfully matched with the server, network access is granted and the user will have access to high-speed network services for the entire session.

Firewall technology on the other hand validates the content of every packet using a sophisticated inspection process. This process is called packet filtering, which has the ability to inspect every packet against a set of configurable filters and policies before passing or denying transport to

the next device. However, because of the inspection process, firewalls are commonly termed “rate-limited”, in that the packet throughput is substantially less than wirespeed. Firewall technology is, however, a highly secure and proven method of protecting information and resources.

Coupling firewall technology, with its ability to validate content via an inspection process, and authenticated VLANs, with their ability to authenticate user identification with policy-based permission sets, provides a powerful combination to address HIPAA requirements.

Summary

Ultimately, there is no perfect security system or policy. The United States government is as painfully aware of this as any organization. The HIPAA security and confidentiality regulations are purposefully vendor and technology neutral. Although there is no perfect solution, there is also very little room for a healthcare organization to evade or escape the requirement to implement security in their organization. HIPAA only lays out the framework and guidelines and offers suggestions.

HIPAA uses the term “best effort” when describing the intent expected of a healthcare organization when addressing security. Each healthcare organization must rely upon their own devices to develop and implement a comprehensive security policy. As is often the case, seeking outside advice is highly recommended, but the healthcare organizations are ultimately responsible and liable for security failings, not the outsourced vendor. Security is a nebulous term and a difficult science in which to offer absolutes. Therefore, those purporting an expertise and offering guarantees should be closely scrutinized, as the healthcare organization will bear the burden of any failures.

Good security, because there is no great security, often starts with good preventive measures and a high degree of awareness. Implementing administrative and physical preventive measures to hinder or deter an attack or breach should be the first step towards creating a secure environment. Installing physical and technological mechanisms to provide access to only those persons authorized access or usage, and providing technological mechanisms which can rapidly alert and pinpoint the location of an attack or insecure event are some other options. Finally, promotion of extensive training and constant reinforcement of security guidelines and systems will result in a high degree of security awareness.

Switching technology is far more secure than a shared networking environment. In a shared Ethernet environment for example all the data is distributed along a common backplane where everyone can service or monitor the data, and the address it is intended to reach must grab it off the common backplane. However, in a switching architecture, data is switched from port to port. In other words, it is inherently a point-to-point transport where other users can not view data as easily as they can if connected to a shared Ethernet backplane. The target address does not have to pull it off a shared environment because the data is delivered directly to its port.

Designing and implementing VLANs across a network based upon structure, function, or activity would effectively segment and compartmentalize an organization, providing the framework for role-based authentication. This would effectively create the first level of network security in that without

the proper routes setup between VLANs intercommunication would be difficult and require deliberate intervention.

Designing and implementing authenticated VLANs in high-profile departments that characteristically contain sensitive patient information, such as pharmacy, laboratory, pathology, radiology, cardiology and others will add a much higher degree of security. Using a password and personal identification number scheme to gain access to an authenticated VLAN would meet the user-based and role-based criteria in HIPAA. By applying policies such as time of day, location, and specialized applications, the criteria for context-based authentication could also be achieved.

Implementing firewalls at critical network access points, or the backbone access point of high-profile departments, will achieve an even higher degree of security when coupled with authenticated VLANs. Firewalls will provide the packet filtering inspection of content and authenticated VLANs will ensure that only authorized users can access a particular VLAN and its resources and users.

Conclusion

Healthcare information technology will be expected to implement security policies, procedures, and systems to protect the security and confidentiality of health information. It will be expected to do so in a very short period of time and probably with few resources and a limited budget. Under these circumstances, technology and awareness are the most effective tools. VLANs, authenticated VLANs, and firewall technology provide an excellent first step towards compliance with the proposed HIPAA regulations.

[i] *See Roe v. Wade*, 410 U.S. 113, 93 S. Ct. 704 (1973); *see also* Joseph L. Bierworth, Jr., *A Constitutional Right to Privacy in Confidential Information: Does it Exist in the Circuit Court?*, 41 BOSTON BAR J.4, 7 (Sept./Oct. 1997).

[ii] "Healthcare information" means any information, whether oral or recorded in any form or medium, that is created or received by a healthcare organization or provider and that relates to the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of healthcare to an individual. *See* Security and Electronic Signature Standards, 63 Fed. Reg. 43,242, 43,264 (to be codified at 45 C.F.R. pt. 142) (proposed Aug. 12, 1998).

[iii] *See, e.g.*, 35 PA. CONS. STAT. § 7607 (1998), ARK. CODE ANN. § 36-664 (Michie 1999), CONN. GEN. STAT. § 19a-583 (1997).

[iv] *See, e.g.*, CAL. CIV. CODE § 56.10 (Deering 1999).

[v] *See, e.g.*, LA. REV. STAT. ANN. § 40:2144 (West 1998).

[vi] *See* Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191, H.R. 3103, 110 Stat. 1936 (1996).

[vii] *See* Howard A. Rubin, *Information Week 500: IT Dollars and Cents*, INFORMATION WEEK (Sept. 14, 1998).

[viii] *See* Security and Electronic Signature Standards, 63 Fed. Reg. at 43,259.

[ix] *See id.*

[x] *See id.*

[xi] "Small health plan" means a group health plan that provides, or pays the cost of, medical care to fewer than 50 participants. *See id*. at 43,248.

[xii] *See id.* at 43,249.

[xiii] *See* Secretary of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information* (Sept. 11, 1997).

[xiv] *See* 42 U.S.C.S. § 1320d-2 (Law. Co-op. 1998).

[xv] *See id.*

[xvi] *See* www.thomas.loc.gov

[xvii] *See* S. 573, 106th Cong. (1999).

[xviii] *See* H.R. 1057, 106th Cong. (1999).

[xix] *See* S. 587, 106th Cong. (1999).

[xx] *See* S. 881, 106th Cong. (1999).

[xxi] *See Congressional Roundup*, 8 Health L. Rep. (BNA) 860 (May 27, 1999).

[xxii] *See* S. 573, § 323.

[xxiii] *See* 8 Health L. Rep. (BNA) at 860.

[xxiv] *See* S. 573, § 311.

[xxv] *See* S. 573, § 321.

[xxvi] *See* H.R. 1941, 106th Cong. (1999).

[xxvii] *See* H.R. 1941, §§ 101-103.

[xxviii] *See* H.R. 1941, § 503.

[xxix] *See* H.R. 1941, § 502(b).

[xxx] *See* H.R. 1941, § 502(d).

[xxxi] *See* H.R. 1941, § 502(c).