Global Information Assurance Certification Paper

HIPAA and compliance
John Rockwood

First, what is HIPAA? It is "Public Law 104-191, August. 21, 1996, Health Insurance Portability and Accountability Act of 1996. An Act: To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[1] From an information technology (IT) perspective it means that the health care industry has to get on the information and content security bandwagon and start protecting patient information and be held accountable for it. Why did this law come into existence? The health care industry has chosen profit over security and a patient's right to privacy. Even the Hippocratic Oath makes mention of the confidentiality of patient information by saying "Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."[2] Apparently the rest of the industry didn't subscribe to this radical concept! So now the industry finds itself behind the eight-ball, the law that is, and is scrambling to establish security policies and procedures to avoid government imposed penalties for non-compliance to the Act.

Who has to comply with HIPAA[2]:

- Health Care Plan consisting of: provider that serves more than 50 participants and is administered by someone other than the employer; health insurance issuer; health maintenance organization; and most all other types of health care plan providers. See public law 104-191 for complete details[2].
- Health Care Clearinghouses, public or private that processes health information.
- Health Care Provider of medical or other health services and any other person furnishing health care services or supplies.

After reading the Act I don't see much of a possibility for loopholes for health care organizations to not comply, other than to "not require disclosure of trade secrets or confidential commercial information" [2].

What data elements and transactions is HIPAA setting standards for[2]:

- Health claims.
- Health claims attachments.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health care payment and remittance advice.
- Health plan premium payments.
- First report of injury.
- Health claim status.

- Referral certification and authorization.

From a systems analysis and design perspective this seems straight forward and looks like common sense.

What safeguards have to be taken[2]:

- Ensure the integrity and confidentiality of the information.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information.
- Use electronic signatures for non-repudiation.

Now from a security perspective this is starting to look like a good thing except that it didn't cover availability of information and its being shoved down the throats of the health care industry because they didn't do it on there own. The availability portion is going to be covered by the certification and accreditation of your systems and sites. The cost of implementation will no doubt be past on to the patient! Although, Congress says that the Act will "…produce a net savings of approximately $12.3 billion for the health care delivery system."[3]

Refer to the Act for penalties[3]. To me they are a bit on the light side for compliance violations of this Act, but the penalties for wrongful disclosure of information are set to be classified as a felony offense.

What else does all this mean? Well for those of you who are familiar networks in the Federal Government this is going to look just like what you know as site based certification and accreditation of systems of computers. For you healthcare administrators and IT managers this is going to be a challenge if you're not prepared. The IT ramifications of the Act are new to the health care industry, but not to agency's like the Department of Defense. The stipulations in the Act look like a compilation of several public laws and defense directives. To get prepared for HIPAA you should take look and get familiar with the acts preceding HIPAA like:

- The Privacy Act of 1974, PL 93-579.[4]
- Computer Security Act of 1987, PL 100-235.[5]
- National Security Decision Directive Number 145, National Policy on Telecommunications and Automated Information Systems Security.[6]
- DoD Directive 5200.28, Security Requirements for Automated Information Systems.[7]
- Department of Defense Trusted Computer System Evaluation Criteria.[8]

For as many problems that HIPAA is going to create for you, there are just as many solutions and solution providers like:

- The Electronic Healthcare Network Accreditation Commission (EHNAC), Accredited Clearinghouses.[9]
- 3Com, HIPAA e-Source.[10]
- HIPAAcomply.[11]

- SAIC: Health Care: Our HIPAA Solutions.[12]
- Tivoli Security Solutions for Healthcare - Getting Ready for HIPAA Security Requirements.[13]

As with any new law somebody is going to make a lot of money. Just make sure that's it your organization and not the competition. It's not something that I would wish upon anyone, but in the end you're going to be very knowledgeable on accreditation's and certification of systems of computers. HIPAA is definitely a good thing! Don't let it run your organization, make it work for you.

[13] Public Law 104-191, AUG. 21, 1996, Health Insurance Portability and Accountability Act of 1996 URL: http://aspe.os.dhhs.gov/admnsimp/pl104191.htm

[2] The Hippocratic Oath, Hippocrates, *Works* trans., Francis Adams (New York; Loeb) vol. I, 299-301. URL: http://www.humanities.ccny.cuny.edu/history/reader/hippoath.htm

[3] HHS Announces Final Regulation Establishing First-Ever National Standards to Protect Patients' Personal Medical Records, URL: http://www.hhs.gov/news/press/2000pres/20001220.html

[4] The Privacy Act of 1974, PL 93-579, 5 USC § 552a -- As Amended, URL: http://www.usdoj.gov/04foia/privstat.htm

[5] Computer Security Act of 1987, PL 100-235, URL: http://www.fas.org/irp/offdocs/laws/pl100235.htm

[6] National Security Decision Directive Number 145 National Policy on Telecommunications and Automated Information Systems Security, The White House Washington, September 17, 1984, URL: http://www.fas.org/irp/offdocs/nsdd145.htm

[7] DoD Directive 5200.28 Security Requirements for Automated Information Systems, March 21, 1988, URL: http://atzhssweb.gordon.army.mil/otd/c2protect/isso/DOD/DOD520028/D520028a.htm

[8] Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985, URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[9] The Electronic Healthcare Network Accreditation Commission (EHNAC), Accredited Clearinghouses, URL: http://www.ehnac.org/Clearinghouses/Default.html

[10] 3Com, HIPAA e-Source, URL: http://www.3com.com/healthcare/securitynet/hipaa

[11] HIPAAcomply, URL: http://www.hipaacomply.com

[12] SAIC: Health Care: Our HIPAA Solutions, URL: http://www.saic.com/healthcare/hipaa/solutions.html

[13] Tivoli Security Solutions for Healthcare - Getting Ready for HIPAA Security Requirements, URL: http://www.tivoli.com/products/solutions/security/healthcare/hipaa.html

[1] Public Law 104-191, AUG. 21, 1996, Health Insurance Portability and Accountability Act of 1996 URL: http://aspe.os.dhhs.gov/admnsimp/pl104191.htm

[2] The Hippocratic Oath, Hippocrates, *Works* trans., Francis Adams (New York; Loeb) vol. I, 299-301. URL: http://www.humanities.ccny.cuny.edu/history/reader/hippoath.htm

[3] HHS Announces Final Regulation Establishing First-Ever National Standards to Protect Patients' Personal Medical Records, URL: http://www.hhs.gov/news/press/2000pres/20001220.html

[4] The Privacy Act of 1974, PL 93-579, 5 USC § 552a -- As Amended, URL: http://www.usdoj.gov/04foia/privstat.htm

[5] Computer Security Act of 1987, PL 100-235, URL: http://www.fas.org/irp/offdocs/laws/pl100235.htm

[6] National Security Decision Directive Number 145 National Policy on Telecommunications and Automated Information Systems Security, The White House Washington, September 17, 1984, URL: http://www.fas.org/irp/offdocs/nsdd145.htm

[7] DoD Directive 5200.28 Security Requirements for Automated Information Systems, March 21, 1988, URL: http://atzhssweb.gordon.army.mil/otd/c2protect/isso/DOD/DOD520028/D520028a.htm

[8] Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985, URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[9] The Electronic Healthcare Network Accreditation Commission (EHNAC), Accredited Clearinghouses, URL: http://www.ehnac.org/Clearinghouses/Default.html

[10] 3Com, HIPAA e-Source, URL: http://www.3com.com/healthcare/securitynet/hipaa

[11] HIPAAcomply, URL: http://www.hipaacomply.com

[12] SAIC: Health Care: Our HIPAA Solutions, URL: http://www.saic.com/healthcare/hipaa/solutions.html
[13] Tivoli Security Solutions for Healthcare - Getting Ready for HIPAA Security Requirements, URL: http://www.tivoli.com/products/solutions/security/healthcare/hipaa.html