

HIPAA PRIVACY and SECURITY

Risk - Assessment - Compliance

Privacy issues have been moved to the front burner by most financial services organizations, but insurers are especially finding themselves doubly exposed when it comes to this subject. Insurers are not only in the spotlight because of Gramm-Leach-Bliley Act (GLBA) regulations concerning the privacy of financial information, but also because of the **Health Insurance Portability and Accountability Act (HIPAA)** regulations concerning medical information. Adding to the mix are separate financial and medical privacy regulations stipulated by the National Association of Insurance Commissioners (NAIC) – which have undergone significant debate among the NAIC subcommittee on model regulations (chaired by Kathleen Sebelius, Kansas) and insurance industry association groups. Although these factions (so far) tend to see more eye-to-eye on financial privacy than they do on medical privacy, the debate is far from over. Certain passages below relating to HIPAA standards are courtesy of Elizabeth N. Rogers, Vinson & Elkins LLP, “HIPAA Privacy and Security Standards.” Nick Mallouf reports.

What’s it all about?

HIPAA concerns the confidentiality, integrity, and availability of individually identifiable health information – commonly referred to as protected health information (PHI). Original 1996 federal HIPAA regulations dealt with insurance portability, fraud and abuse accountability, and simplification of health plan administration. The year-2000 update specifically addresses administrative simplification. This update dictates a set of codes and data transmission standards for consistently communicating health information among health entities and the government. Upon closer examination, however, it imposes a set of privacy and security regulations that are anything but simplifying.

Some HIPAA specialists have said that insurers should be in pretty good shape to deal with these new regulations, *if* they adequately went through the Y2K assessment and implementation processes. Nonetheless, companies characterized as leading edge in their preparation for new regulations have found that combining privacy and security issues present some unique risks, and legal exposures.

The first of five new sets of standards was issued in August 2000. It’s unclear whether or not additional standards will come out before year-end, but it’s not unlikely to expect them sometime first quarter 2001. Most “covered entities” will have 24 months from the date a new standard is issued to implement it.

Like GLBA, HIPAA breaks new ground. It is extraordinarily comprehensive, covers complex issues, and requires collaborative effort to implement. Given the added federal, state, and NAIC coordination issues, along with specific implementation deadlines, it’s no wonder companies are scrambling to figure out what to do about it.

What to do about it?

How do companies address compliance with regulations as complicated and onerous as HIPAA? Much the way they did with Y2K. Likewise, how sophisticated the approach or remedy will depend upon availability of resources. But when a covered entity understands the rules and recognizes that risks are clearly present, the following steps offer a good way to begin.

Build Teams Get an executive sponsor – it’s a must. Without one, projects such as this are doomed for failure. Create a steering committee, assign a project director and/or establish a project management office. Build separate project teams for privacy, security, standards, and certification.

Assess Baseline Understand and document existing privacy and security standards, policies, and procedures. Engage a formal methodology or retain a top-quality project manager. Map the flow of information.

Analyze Risk Analyze your findings. Determine where you are, where you want to be, and what it's going to take to get there.

Develop Plans Determine the detailed steps to achieve compliance and the timetable for each step. Implement the changes.

Get Certified Use an independent outside service or internal audit.

Keep Up Maintain compliance by establishing regular reviews, performing internal audits, and developing procedures for implementing updates and educating and notifying staff.

NOW IS THE TIME TO START!

Nick Mallouf, CPA, CISA, is president of MRC Insurance Consulting Group, Inc., providing compliance and consulting services to insurers, regulators, attorneys, and banks-in-insurance. www.mallouf.com

BOXED PIECE #1

DATA TRANSACTION AND CODING STANDARDS— ISSUED AUGUST 2000

Identifier standards:

- Employers
- Health Plans
- Providers
- Individuals

Consolidated Code Sets:

- Diagnoses
- Drugs
- Procedures

Privacy:

- Setting company policies/standards
- Identifying responsible persons
- Implementing procedures to prevent unauthorized sharing of PHI

Security:

See Privacy, but relates to confidentiality, integrity, and availability of PHI that is stored, processed, and transmitted electronically.

BOXED PIECE #2:

THREE KEY QUESTIONS FOR INSURERS:

1. “Covered Entity” Y/N? Generally, covered entities are health plans, healthcare clearinghouses, and healthcare providers that maintain and/or transmit health information electronically. Most insurers obtain PHI on the coverage application.
2. What is the definition of “PHI”?
3. “Business Partner” Y/N? Generally, these are third parties sharing PHI for business purposes and include lawyers, accountants, auditors and consultants; TPAs, accrediting organizations, healthcare clearinghouses, data processing firms, and billing firms.

BOXED PIECE #3:

To ensure compliance, HIPAA calls for the Secretary of Health and Human Services to conduct periodic reviews of covered entities. If determined to be non-compliant with issues unable to be resolved informally, written findings are forthcoming and could result in civil or criminal penalties.

Civil Penalties
\$100 per violation
\$25,000 per year

Criminal Penalties
General Rule: \$50,000 fine and/or one year imprisonment
False Pretenses: \$100,000 fine and/or five years imprisonment
Bad Intent: \$250,000 fine and/or 10 years imprisonment

BOXED PIECE #4:

PRIVACY STANDARDS INCLUDE:

Permitted Uses and Disclosures of PHI
Required Disclosures
Authorization Required
Authorization Form
Authorization Not Required
Minimum Necessary Rule
Contracts with Business Partners
Notice to Individuals of Information Practices
Access of Individuals to PHI

Restriction of Uses and Disclosures
Accounting for Uses and Disclosures
Amendment and Correction by Individuals
Designation of Privacy Official
Training
Safeguards
Complaints
Sanctions
Documentation of Policies and Procedures

BOXED PIECE #5:

SECURITY STANDARDS INCLUDE:

Administrative Procedures:
Certification
Partner Agreements
Contingency Plans
Information access control
Internal Audits
Security management processes
Training

Technical Security Mechanisms:
Prevention of Unauthorized Access via Networks

Physical Safeguards:
Assignment of security responsibility
Media controls
Physical Access Controls
Workstation Use and Security Guidelines
Security Awareness Training

Technical Security Services:
Access Controls
Audit Controls
Authorization Controls
Data Authentication