Patient Privacy: Securing Protected Health Information

By Kip Wolf

Doing business in, or serving businesses in, the health care industry now requires more accountability. Each entity must now prove that the protected health information that it gathers, transmits or maintains remains private and secure. Which is no small task in today's information age.

What the Rules Say

Modified in the August 2002 revisions to the final rule published in the Federal Register by the United States Department of Health & Human Services (HHS), the patient privacy amendments to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) define health information as "any information, whether oral or recorded in any form or medium that: [i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[1]

Privacy and security regulations for protected health information present an uncanny resemblance to the regulation of similarly protected data familiar to companies regulated by the Food and Drug Administration (FDA).

The FDA's regulations for electronic records and electronic signatures published in the Code of Federal Regulations, Title 21, Part 11 (21CFR Part11) sets forth the criteria under which "the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper"[2].

Understanding Both Improves Compliance

Compliance actions taken for Part 11 requirements are solutions for HIPAA information privacy and security compliance as well.

In fact, the verbiage in the HIPAA rule may just be more readable and readily understandable than its FDA counterpart, Part 11. Familiarity and a thorough consideration of both will provide an exceptional grasp of the common concept and intent of the two separate rules.

And for covered entities that are regulated by both HHS and the FDA, a centralized effort involving a single solution for compliance with both rules can produce more cost effective and efficient results.

Twin Regulations?

The parallels in the regulations are astounding. HIPAA regulated entities must "assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures"[3]. The rule goes on to detail specific measures necessary, while Part 11 simply requires that procedures and controls are in place "to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records"[4].

Even with their close parallels, and very different degrees of explanation, both rules

[1] 45CFR§160.103

[2] 21CFR§11.1(a)

[3] 45CFR§142.308

[4] 21CFR§11.10

absolutely require the independent verification and validation of the computer system for quality control and compliance.

What HIPAA calls *certification* and defines as "the technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements"[5], Part 11 calls *validation* of the computer system to "ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records"[6].

No matter what it's called, (certification or validation) it starts with an assessment and ends with a summary report which defines how the computer system meets all of the user and regulatory requirements. Continued maintenance by the computer system owner and periodic assessments (e.g. annually) of the compliance status by a third-party are absolutely valuable for compliance, and inspectors approve of such diligence. A lack of diligence has its consequences.

The Cost of Non-Compliance

In May 2002 Schering-Plough received a record fine of $500 million for non-compliance. Penalties for failure to comply with HIPAA and Part 11 can result in fines, interruption of business operations and even imprisonment.

Compliance is taken seriously by the regulatory agencies. The choices for action are simple for regulated entities: be proactive or reactive.

What to Do Next?

As audits have shown during the enforcement of the regulations, the agencies prefer impartial, third-party involvement in the validation process. Finding a qualified, experienced and effective firm to perform such efforts can be challenging. But a proactive investment can save a costly reactive penalty for non-compliance.

Start with an assessment of the current computer systems and a clear definition of your business practices. The rest is all downhill from there.

Mr. Wolf is president and Chief Executive Officer of Manheim, Pennsylvania-based GxP Data Services, LLC.

GxP Data Services is an established leader in providing exceptional regulatory compliance and computer validation contract services to companies in regulated industries. Our highly qualified professional staff is equally proficient in quality systems and information technology which makes us a premier provider of computer systems compliance services to incubator start-ups and established Fortune 500 companies alike.

[5] 45CFR§142.308(a)(1)
[6] 21CFR§11.10 (a)