Security Science International

HIPAA Simplification Presentation

by

John Butterworth, Ph.D.

What are the HIPAA Administrative Simplification Provisions?

Presentation Overview

1. **National standards** for electronic data transmission.
2. **Unique health identifiers** for providers, employers, plans, and individuals.
3. **Security standards** to protect electronically maintained health information.
4. **Privacy and confidentiality** provisions for individually identifiable health care data.

Fraud and Abuse Spotlight.

In the spotlight of fraud and abuse, are security and fraud issues lurking in the shadows of HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is changing the way healthcare is: **insured, documented, compensated, communicated, and policed.** Signed into law by President Clinton, **HIPAA is intended to curtail healthcare fraud and abuse**, enforce standards for health information, guarantee the security and privacy of health information, and assure health insurance portability for employed persons. Until recently, the spotlight has been on HIPAA's fraud and abuse of even greater consequence. The impact on information standards will be evolutionary in nature, codifying de-facto standards already in place. The portability provisions of the act focus on health plan eligibility rules; they are narrow in scope and will have little impact on health information technology.

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as the Kennedy/Kassebaum Act.
- Primary purpose was to improve health insurance accessibility for people changing employers or leaving the workforce.
- HIPAA also included "Administrative Simplification" provisions to encourage and protect the electronic transmission of health-related data.

What are the Administrative Simplification Provisions Objectives?

1. Reduce fraud and abuse
2. Protect patient rights, including the privacy of patient health data
3. Improve quality of care through access to consistent clinical data
4. Improve efficiency of national health system
5. Improve information available for decision-making
6. Establish security standards for Internet-based technology
7. Reduce administrative overhead costs

Fraud and Abuse

HIPPA's fraud and abuse provisions are based upon the False Claims Act, which it materially extends. Passed during the civil war, The False Claims Act was intended to protect the union army from fraudulent suppliers who sold faulty war material to the government. In support of the False Claims Act, Abraham Lincoln wrote: "*Worse than traitors in arms are the men who pretend loyalty to the flag, feast and fatten on the misfortunes of the nation while patriotic blood is crimsoning the plains of the south and their countrymen are moldering in the dust".*

HIPAA significantly expands the False Claims Act. It broadens the act's reach to healthcare claims, and lowers the bar for the definition of fraud itself. Webster defines fraud as the *intentional perversion of truth in order to induce another to part with something of value.*

HIPAA removes the concept of *intentional* from civil fraud, preserving it only for criminal acts. Under HIPAA, to be guilty of fraud you need only to have engaged in a pattern or practice of presenting claims that you knew or should have known will lead to greater payments than appropriate. This is an extremely broad

Fines and Monetary Penalties

HIPAA increased fines and monetary penalties to triple the overcharged amount plus up to $10,000 per violation. It increased the percent of the award that could be paid to whistle blowers, it returned the fines collected back into the Fraud and Abuse Control program which funds the investigations, and it created the Medicare Integrity Program, which contracts out the investigative work to the private sector.

Equally important, HIPAA set up a funding mechanism, increasing the amount available for fraud and abuse investigations every year through 2003. Funding will exceed $2.5 billion over the next 5 years. As a result, fraud and abuse activities are flourishing, 4000 civil fraud cases were filed in 1997, compared to 2,500 in 1996, and the OIG workforce will flow from 960 healthcare auditors in 1996 to 1,920 by 2002.

Overpayments estimated at $23.2 billion in 1996 dropped to $20.3 billion in 1997, and in February, HCFA's Office of the Chief Actuary reported the first ever drop in the DRG case-mix index with associated savings of $200 million. The office credited the fraud and abuse program for the improvement.

Summary and Conclusion

Has the act been successful?

One would think the act has been successful, judging from the savings and recoveries. The department of justice reported $1.2 billion in civil settlements and judgments in 1997 from its activities in healthcare fraud alone. The OIG declared savings of $11.6 billion in fiscal 1998 compared with $7.6 billion the previous year, and claims to recover at least $11 for every $1 spent on its fraud and abuse programs.

Is the Government pleased with these successes?

Is the government pleased with these successes? Not Congress, not the OIG and not the GAO. The OIG reported that in fiscal 1997 Medicare paid out over $1.6 billion in improper physician claims alone, compared with $900 million in improper claims the year before.

The Inspector General, in a January memo to HCFA, chided it for not doing more, and recommended HCFA "perform routine monitoring and analysis of hospital billing data and clinical data to proactively identify aberrant patterns of upcoding".

The GAO, in its report to congress the same month, noted that HCFA's deployment of the legal tools and financial resources provided by HIPAA to crack down on Medicare fraud "has lagged." And the Sparrow report, an Independent study commissioned by the DOJ and issued in February states that although "unprecedented attention to the issue of healthcare fraud produced many apparent successes nonetheless, little progress—in terms of practical improvements—seems to result." Congress has joined suit. Senators Susan M. Collins (R-Maine) and Dick Durbin (D-III) plan to introduce additional Medicare fraud legislation.

Why was legislation needed?

Technological advancements have resulted in substantial and increasing electronic transmission of health data, including:

- Rapid growth of health care Internet and intranet applications to transmit and share patient information, such as diagnoses, radiological images, lab tests, and prescriptions
- Advancements in the computerization of patient medical records.
- Increasing use of electronic prior authorizations for provider services, as well as claims submission and payments.
- Use of e-mail as a communication tool between caregivers and their patients.

Why was legislation needed? (continued)

- Lack of standardization for the collection, storage, and transmission of health data increased administrative costs AND decreased utility of data
- Increase health care costs demands for uniform health care data to evaluate alternative coverage and treatment approaches

Who must comply with HIPAA?

1. Health care providers or any other person or organization that furnishes, bills, or paid for health care in its normal course of business

2. Health plans that provide or pay the cost of medical care, including Medicare and Medicaid

3. Health care clearinghouse that process data elements or transactions

Provision 1: National Standards

Electronic Data Interchange standards have been adopted for:

- Health claims/encounter information
- Enrollment/dis-enrollment in a health plan
- Health care payment and remittance advise
- Health plan premium payments
- Health claim status
- Referral certification and authorization
- Coordination of benefits

Standards for claims attachments and first report of injury are required but have not yet been adopted.

Overview

Provision 1: National Standards
Electronic Data Interchange (continued)

- American National Standards Institute (ANSI) ASC X12N standards have been adopted for most transactions.

- For retail pharmacy, the National Council of Prescription Drug Programs (NCPDP) Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 both set the standards.

Provision 1: National Standards

Code Sets

Specific code sets have been adopted:

- ICD-9-CM, Volumes 1&2
- ICD-9-CM, Volume 3
- Combination of HCPCS and CPT-4
- HCPCS (other substances, equipment, supplies, other items)
- National Drug Codes
- CDT-2 (dental services)

NOTE: All local codes will be eliminated.

Security Program

The security standards require a two-phased program: risk ssessment and program management. During risk assessment, the organization assesses the potential risks and vulnerabilities of individually identifiable health information. Program management is an ongoing process in which security measures are: developed, implemented, maintained and documented.

Kept current Categories of Security Requirements and Implementation Features:

- Administrative procedures
- Physical Safeguards
- Technical Security Services
- To guard against unauthorized access to data that is transmitted over a communications network
- Technical security mechanisms
- To Guard Data integrity, confidentiality and availability

Security

The proposed information security rules specific 61 specific conditions that must be met, 6 or 7 additional conditions if a network is present. The proposed rules divide these conditions into requirements and implementation features, and further group them into 2 groups and 4 categories. The categories are obscure and overlapping at best, and some of the conditions appear redundant. HCFA acknowledges this implicitly by requiring only that the conditions be fulfilled categories can be ignored.

For a small medical office the requirements appear overwhelming. The notice of Proposed Rule making (NPRM) addresses this question specifically in a section explaining how a one to four physician office might implement the security requirements. HCFA suggests evaluation and certification by a consultant or the practice management system vendor during assessment and policy procedure development. Even the small office will need personnel security policies, assigned security responsibility, compliant hardware, software with internal audit trail capability, and physical plant changes such as locked rooms and closets to secure equipment. Employees must be trained and oriented to information security, chain of trust agreements with claims processors must be written, and each of these measures must be documented, maintained, and kept current.

Security Standards

Security standards for all patient-specific information that is or has been electronically stored and /or transmitted can be grouped into four categories:

1. **Administrative procedure safeguards**- comprehensive security policies and procedures.

2. **Physical Safeguards**- data integrity, backup, access Workstation location and security training.

3. **Technical security mechanisms** – security measures to guard against unauthorized access to data.

4. **Technical security services** – measures to protect patient information and control individual access to such information

HIPAA's Information Security Provisions

1. A written security plan with policies and procedures
2. A formal assessment of risks and data vulnerability
3. Certification of the security plan after implementation

Physical plant changes in accordance with security requirements:

- Evaluation of backup media, workstations in relation to public access, facility management processes.
- Hardware requirements including data storage, backup and disposal; user authentication (if hardware supported)
- Software capabilities including awareness training, education, termination procedures. HCFA acknowledges that small providers may need guidance regarding the content of documents required by this rule, which it expects to be developed by industry associations and vendors. Consultants and healthcare vendors are working on programs and products to support provider needs created as a result of these rules.

Security Standards (continued)

The standards establish a minimum threshold for:

- Compliance in each of four categories.
- The security standards do not specify particular
- Technology requirements – each organization MUST assess its own "risk" and develop security measures accordingly.
- Organizations MUST certify their security programs (either through a "self certification" or by private accreditation entity or vendor)
- The certification process has not yet been specifically defined.

What do they mean for providers?

- Procedures and systems MUST be updated to ensure that health Care data is protected.
- Written security policies and procedures must be created and/or
- Reviewed to ensure compliance.
- Employees MUST receive training on those polices
- Access to data MUST be controlled through appropriate mechanisms (e.g. passwords, automatic tracking of data, Full audit trail)
- Security procedures/ system MUST be certified to meet minimum Standards.

Consent/Authorization Provisions

- Individually identifiable health information may not be used or disclosed unless authorized by the patient or is specifically permitted under HIPAA
- Patient consent is required for the use or disclosure of information for three purposes: treatment, payment, and other health care operations
- The privacy rule refers to both patient consent and authorization.

In general, patient consent relates to information used for treatment-related purposes (such as employers, underwriters, or researchers).

Other Key Provisions

- Use of health information for non-treatment purposes must be limited to the "minimum necessary."
- A written agreement must be in place that provides for appropriate safeguarding of health information with all "business associates."
- This standard does not apply when information is being shared for treatment purposes.
- Development of policies and procedures: Each entity must designate a privacy officer, develop privacy policies and procedures, and provide staff training to ensure that health information is protected.

Patients' Rights Provisions

- Covered entities must provide a "notice of privacy practice" to each patient describing his/her rights regarding protected health information.

- Patients have the right to inspect and receive a copy of their medical records and to request amendments to their records. Though providers have the right to deny inclusion of an amendment, the patient has the right to file a Statement of Disagreement, which becomes part of the record. The provider can file a rebuttal to the Statement, should she so choose.

- Patients also have the right to receive an accounting of disclosure of information that go beyond those provided in the rule, but providers are not required to comply with those requests.

What do they mean for providers?

Consent is required for disclosure of identifiable information for treatment, payment, or health care operations (for example:

- Quality assessment and improvement activities, physician qualifications and competence evaluations, medical reviews, and audits).
- Health care providers may refuse treatment if they do not receive an individual's consent.
- Consent is not required for sharing a patient's medical records with another physician when referring the patient to that physician or when billing a patient referred for a specialty consultation.

What do they mean for providers?

Privacy regulations will require authorization for disclosure of identifiable information in all cases when used for ancillary purposes such as:

- Research, such as clinical or market
- Employers or employer groups
- Pre-enrollment underwriting

Authorizations must be written specific terms and must identify:

- The information to be discloses
- Persons authorized to make the disclosure
- Persons authorized to receive the information
- “Expiration date” of authorization

What do they mean for providers?

- If an individual refuses to give authorization, providers generally still must provide treatment.

- "National priority" activities are exempt from obtaining either consents or authorizations from individual patients. These include, public health emergencies, law enforcement, and judicial and administrative proceedings.

Next Steps: Security Standards

- **Gap Analysis.** Compare current security program to the HIPAA standard to identify gaps and develop action plans.

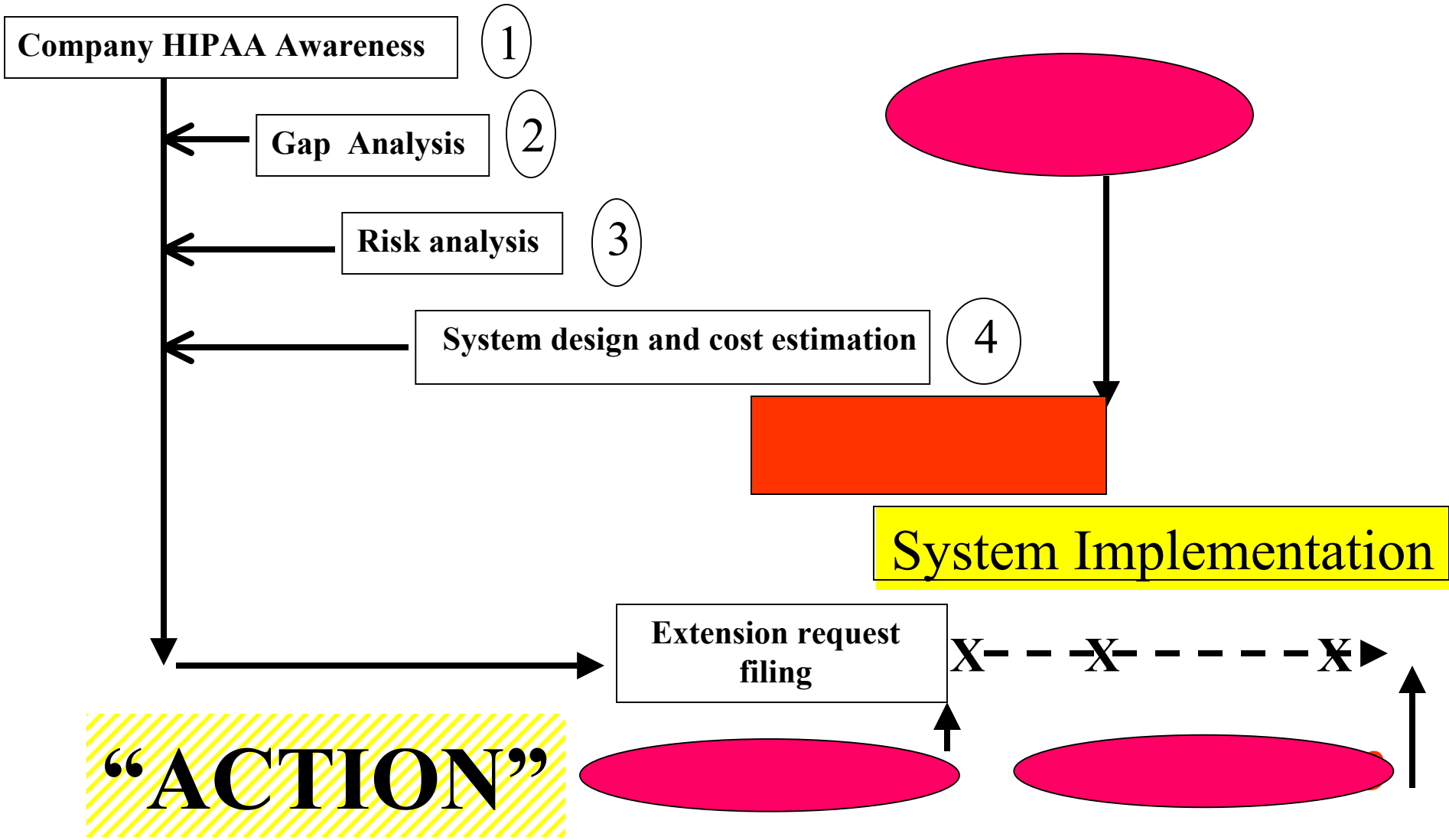
- **Risk Analysis.** Identify the likelihood and impact of adverse actions as inappropriate disclosure, corruption, or loss of patient information.

- Based on the gap analysis and risk analysis, determine what additional security measures are appropriate and develop a plan for implementation.

- Proposed standards require a “risk assessment,” which includes a cost/benefit analysis of security measures.

Summary and Conclusion

The HIPAA of 1996 is having a profound impact on fraud and abuse detection and prevention, electronic communication standards, and health information security. Moving forward into the new millennium, we can expect expansion of its scope to electronic medical records standards and acceleration of its ongoing programs.


Company HIPAA Awareness
1
Gap Analysis
2
Risk analysis
3
System design and cost estimation
4
System Implementation
Extension request filing
X
X
X
"ACTION"