Gartner SYMPOSIUM/ITxpo 2000

insight for the connected world

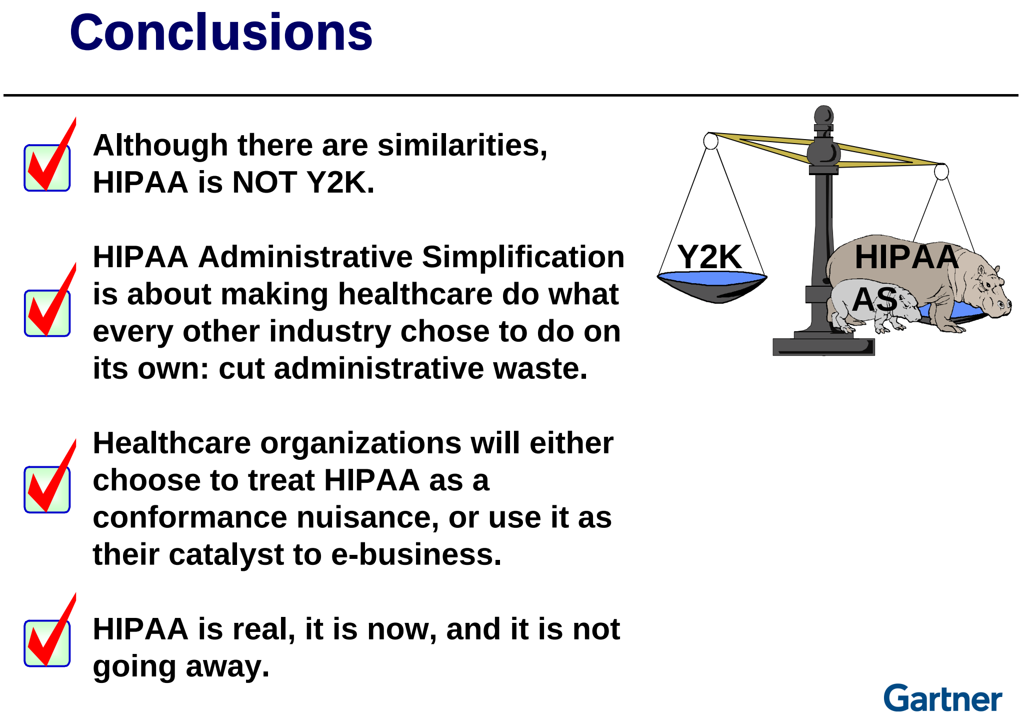
16—20 October 2000

Matt Duncan

Walt Disney World
Orlando, Florida USA

56 Top Gallant Road
P. O. Box 10212
Stamford, CT 06904-2212

Conclusions



Conclusions

- ☑ Although there are similarities, HIPAA is NOT Y2K.
- ☑ HIPAA Administrative Simplification is about making healthcare do what every other industry chose to do on its own: cut administrative waste.
- ☑ Healthcare organizations will either choose to treat HIPAA as a conformance nuisance, or use it as their catalyst to e-business.
- ☑ HIPAA is real, it is now, and it is not going away.

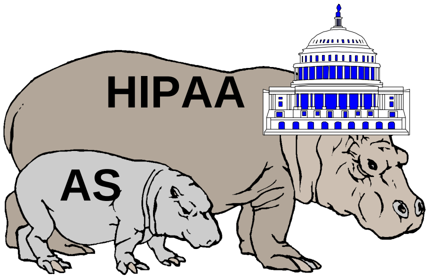
Gartner

After the immutable deadline for year 2000 passed, the healthcare industry turned its attention to the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification (AS) provisions. Attention has grown since the U.S. Department of Health and Human Services (DHHS) recently signed its first final rule — on electronic data interchange (EDI) transactions. Until recently, there was management disinterest in HIPAA based on the realities of the federal Balanced Budget Act and the general success in dealing with year 2000. Consultants, vendors and internal HIPAA coordinators have attempted to break through that resistance by listing the substantial civil and criminal penalties in various proposed rules, and worst-case interpretations of the regulations' impact on legacy systems.

This presentation will examine HIPAA AS and offer practical, common-sense advice for HCOs to approach HIPAA as efficiently and effectively as possible. First, we will define the major categories of AS regulations and explore their impact on business and IS departments. Then, we offer strategies for HCOs to "attack" the opportunities inherent in HIPAA, as well as reasons to act now vs. "hiding in the bell curve" of compliance. Finally, we will present options for external assistance on assessment projects and will begin to explore the expected costs and benefits of HIPAA AS for payers and providers.

Definition: Draft Administrative Simplification regulations were prepared in 1994 and added to numerous bills until the Kennedy-Kassenbaum bill finally passed and became law in 1996.

HIPAA Administrative Simplification



Electronic Transactions, Code Sets and Identifiers

Security and Electronic Signature Standards

Privacy

Source: Gartner Research

The HIPAA AS standards are generally grouped into three categories:

Electronic Transactions (EDI) and Code Sets (ANS X12N and NCPDP for Rx)

- PLUS National Identifiers (separate standards)
  - Employers, providers and health plans (individuals on hold pending privacy legislation)

Security and Electronic Signature

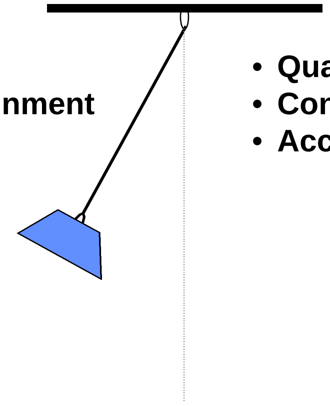
- Administrative
- Physical
- Information storage and access
- Information transmission
- Electronic signatures

Privacy of Individually Identifiable Health Information

- Release requires written patient authorization (uncoerced, revocable) except for:
  - Treatment, payment, healthcare operations and specific exceptions
- Accountable disclosure
- Compartmentalization and minimum necessary disclosure
- Patients have the right to examine and correct information about themselves
- Provides for release of “disidentified” data

Imperative: In 1994, the Workshop on Electronic Data Interchange (WEDI) forecast that e-transactions could save $73 billion year, or about one-third of all healthcare administrative costs.

HIPAA AS: The Reason



- Cost Containment

- Quality
- Convenience
- Access

- **Cost-driven initiative**
- **Good for healthcare, but strong medicine**

Gartner

Source: Gartner Research

HCOs should not be misled by the emphasis on security and privacy. HIPAA forces HCOs to do what other industries did on their own: reduce costs by replacing people, paper and postage with electronic communications. Healthcare costs have risen to 15 percent of the gross domestic product and represent a burden on U.S. enterprises selling goods abroad. In provider and payer enterprises together, three to four people handle the paper to administer a case for each person who is given hands-on care. Nonetheless, the industry has responded to cost reductions by squeezing clinicians rather than finding ways to streamline the paperwork.

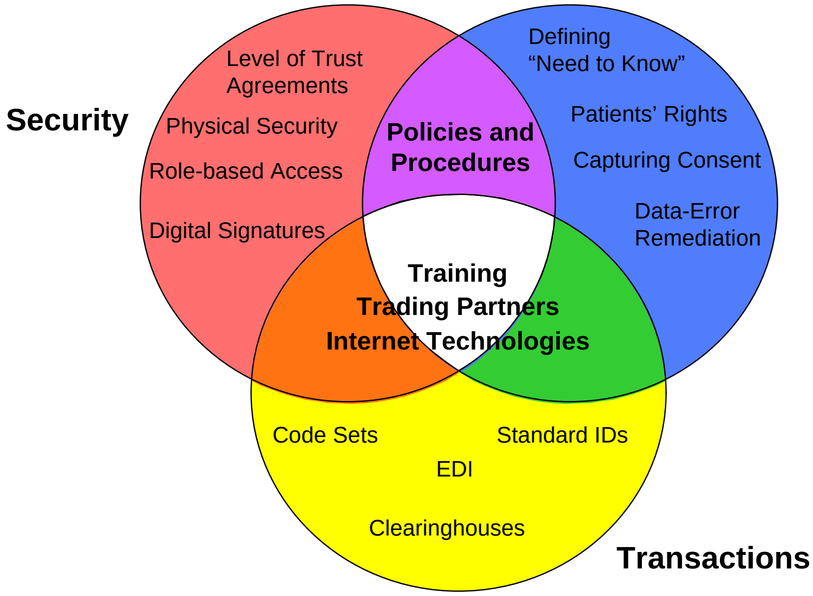
The government sees two opportunities to force the industry to pursue administrative savings through the HIPAA standards:

- Mandating standard e-transactions, codes and identifiers.
- Establishing standards that enable the use of the Internet instead of expensive, private networks.

Both political parties share the view that a substantial portion of these savings can be realized and will generate reductions in the federal budget and improvements in the competitiveness of U.S. enterprises. HIPAA AS is about saving money, and it will not go away.

Strategic Planning Assumption: After signing the EDI final rule in August 2000, the Department of Health and Human Services (DHHS) will publish the final rule on HIPAA security standards by 4Q00, resulting in a compliance date in 1Q03 (0.8 probability).

New Challenges, Many Overlapping



Security

Level of Trust Agreements

Physical Security

Role-based Access

Digital Signatures

Privacy

Defining "Need to Know"

Patients' Rights

Capturing Consent

Data-Error Remediation

Policies and Procedures

Training

Trading Partners

Internet Technologies

Transactions

Code Sets

Standard IDs

EDI

Clearinghouses

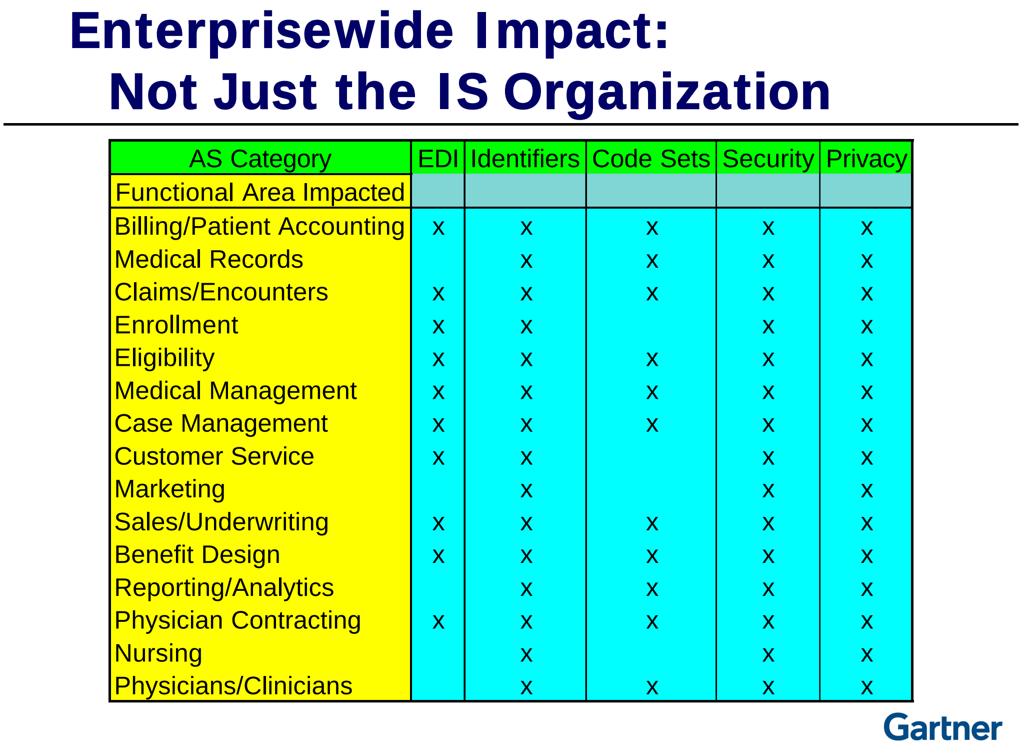
Gartner

Source: Gartner Research

The HIPAA AS EDI standards are based on ASC X12N. This standard is appropriate because all codes have been fully specified. Initial beneficiaries will be clearinghouses as HCOs scramble to meet deadlines. The larger impact will be to accelerate healthcare e-commerce. Proposed security standards require comprehensive, formal, written procedures for protecting all patient-identifiable information stored or transmitted by any electronic system. Privacy regulations cover patient-identifiable health information ("healthinfo") in any form that is or has been in electronic form. Healthinfo may be used for treatment, payment, healthcare operations and explicitly covered exceptions (public health, oversight, law enforcement) without the authorization of the patient. Patients must give their written, uncoerced and revocable permission for any other use. Compartmentalization of access is required, and only the minimum information necessary may be released. Records of disclosures must be kept, and patients have the right to challenge and correct their own information. "Disidentified" data may be released without the patients' permission.

Action Item: HCOs at this point should have at least conducted formal education and awareness programs. That effort should lead to a formulation of organizational consensus on the impact of HIPAA AS; an HCO (led by its compliance committee) must establish a working interpretation of the rules, with the understanding that these interpretations will evolve over time.

Tactical Guideline: Considering the implications of HIPAA AS throughout almost every functional area of an HCO, early education of management and clinicians is essential, and training of all employees must be included in action plans for operationalizing HIPAA.



Enterprisewide Impact: Not Just the IS Organization

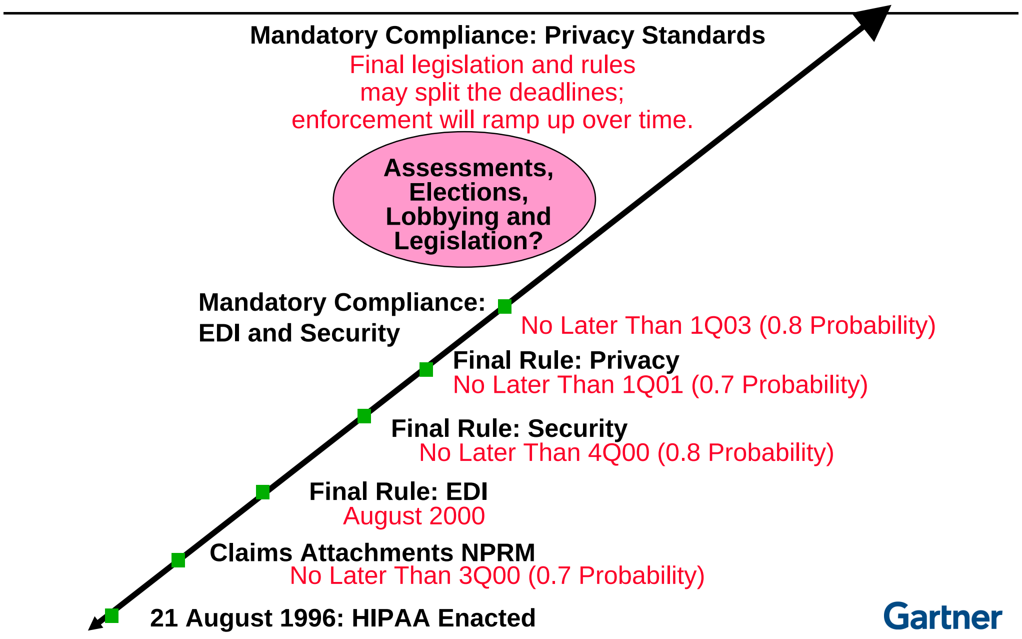
AS Category	EDI	Identifiers	Code Sets	Security	Privacy
Functional Area Impacted					
Billing/Patient Accounting	x	x	x	x	x
Medical Records		x	x	x	x
Claims/Encounters	x	x	x	x	x
Enrollment	x	x		x	x
Eligibility	x	x	x	x	x
Medical Management	x	x	x	x	x
Case Management	x	x	x	x	x
Customer Service	x	x		x	x
Marketing		x		x	x
Sales/Underwriting	x	x	x	x	x
Benefit Design	x	x	x	x	x
Reporting/Analytics		x	x	x	x
Physician Contracting	x	x	x	x	x
Nursing		x		x	x
Physicians/Clinicians		x	x	x	x

Source: Gartner Research

Despite an early misconception shared by many HCOs that HIPAA is just another challenge facing IS departments, the AS mandates will have a profound impact on almost every functional business unit throughout payer and provider organizations. This will be represented by the modifications needed to core transaction processing and ancillary departmental software applications. Even where vendors assume most responsibility for implementing those changes, users will still face training and testing on modifications. The e-transaction, identifier and code-set standards will require a careful inspection of every application that transmits financial, administrative or clinical data to other HCO departments and to outside enterprises. In many cases, HCOs will find applications — usually departmental — that are no longer supported by vendors, and will either be forced to investigate modifying source code in escrow (internally or using third parties) or to select replacement solutions. These same applications must also be studied to ensure that they have appropriate security precautions built in, such as audit trail capabilities. Most significantly, almost every employee in every department must undergo education on new policies and procedures for handling patient-identifiable information to protect both the patients and the HCOs.

Strategic Planning Assumption: By year-end 2003, all HCOs will have substantially changed their systems, processes and organizations to meet all the principles set forth in the HIPAA mandates, although implementation details and deadlines will vary (0.8 probability).

Administrative Simplification Timeline



Mandatory Compliance: Privacy Standards
Final legislation and rules
may split the deadlines;
enforcement will ramp up over time.

Assessments, Elections, Lobbying and Legislation?

Mandatory Compliance: EDI and Security
No Later Than 1Q03 (0.8 Probability)

Final Rule: Privacy
No Later Than 1Q01 (0.7 Probability)

Final Rule: Security
No Later Than 4Q00 (0.8 Probability)

Final Rule: EDI
August 2000

Claims Attachments NPRM
No Later Than 3Q00 (0.7 Probability)

21 August 1996: HIPAA Enacted

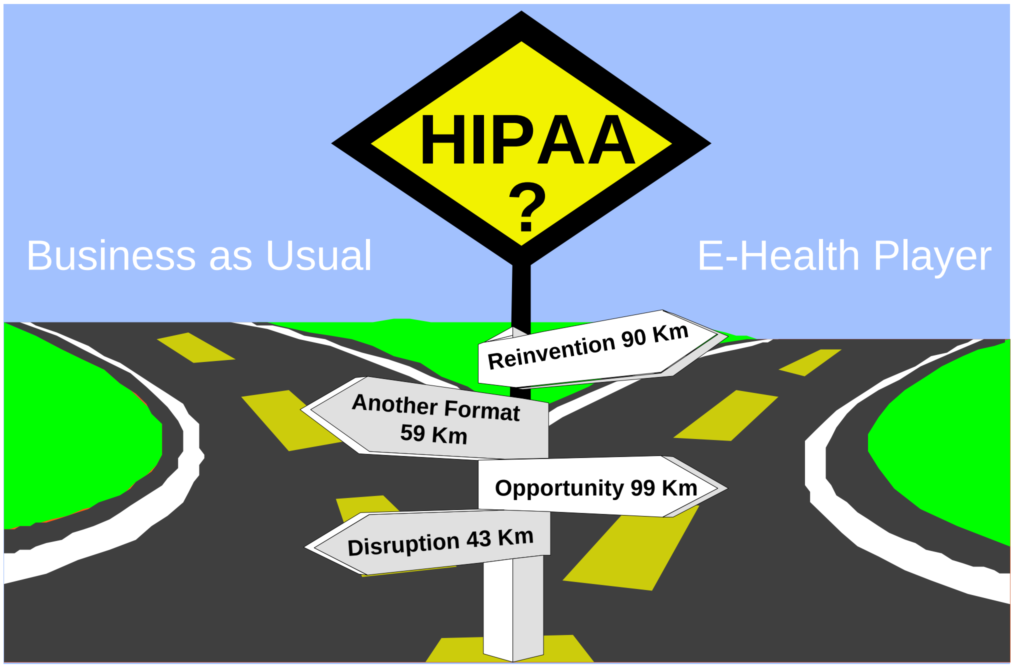
Source: Gartner Research

While DHHS has postponed each self-imposed deadline for finalizing requirements to accommodate public comments and resolve issues, it appears that most regulations — with the possible exception of privacy — will soon be enacted. Compliance enforcement will build gradually. As the government and the industry build experience during the ramp-up period, enforcement priority decisions must be based, in part, on a comparison of the HCO being examined with the industry as a whole. If the HCO has not wantonly ignored a standard for its commercial gain, if it has addressed the most critical issues necessary to comply with a standard and if its compliance paces that of the majority of its peers, it is unlikely to face the dire penalties that the acts describe. In other words, an HCO will be "graded on the curve" in the security and privacy standards, at least for several years.

Action Item: When resources are tight and priority decisions must be made, the best amount to invest in security and privacy is just enough to immediately meet the most pressing needs, and to accompany this with a budget for improving practices over time as industry compliance improves.

New Rules/New Realities: HIPAA will be the catalyst that enables a reinvention of healthcare processes around e-business for those healthcare organizations that choose to embrace the opportunity.

A Nuisance or an Opportunity?

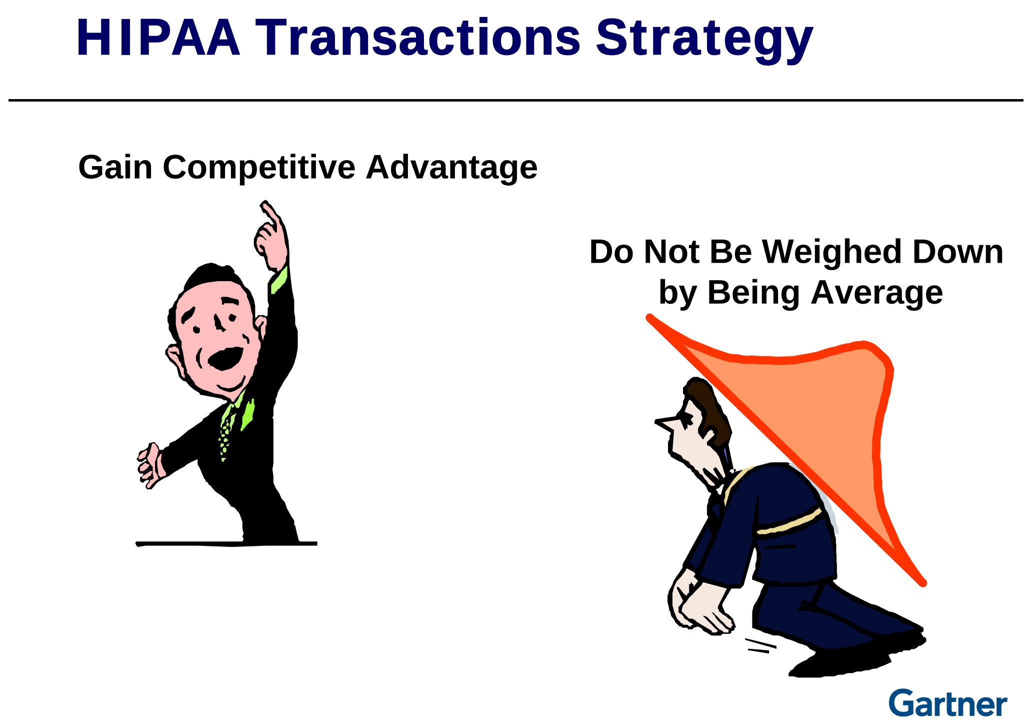


Source: Gartner Research

It is important to assess an HCO against all the HIPAA requirements because the different standards impact many of the same systems. But it is not critical to address all requirements strictly on the deadlines that might be projected from the rules. An HCO can save one-time costs by gauging its response to security and privacy standards to do as well as the industry in general, but it gains no benefit by spending more to excel. Instead, it should direct funds toward meeting the standards necessary for electronic transactions to bring the cost advantage to the HCO. Staying ahead of its competitors on this front will allow it to survive, perhaps even thrive, as the government drives down average healthcare payments in an attempt to recover the benefits of HIPAA.

However, it takes money to make money or, for that matter, to save money. The investment to comply with HIPAA has a front-loaded component that must be made before the savings are realized. Fully realizing the savings will require considerably more investment than that required for simple compliance.

Strategic Planning Assumptions: By year-end 2003, 50 percent of HCOs will conduct at least 40 percent of administrative and financial healthcare transactions and customer service queries using Internet-based technologies (0.7 probability). These HCOs will be the competitive leaders in their markets. Through 2003, most HCOs will react to the costs of HIPAA compliance by seeking clearinghouse alternatives or clinging to manual, paper-based transactions. Healthcare costs will continue to escalate, resulting in further government intervention (0.3 probability).



HIPAA Transactions Strategy

Gain Competitive Advantage

Do Not Be Weighed Down by Being Average

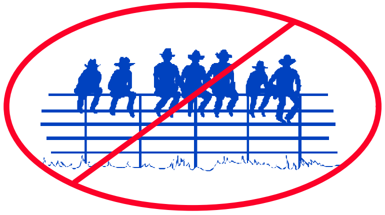
Source: Gartner Research

It is important to regard HIPAA as an opportunity, at least with regard to the transaction standards. A sure path to loss of competitive standing is to find the least-cost methods of compliance with the opportunistic HIPAA requirements without finding a way to capture the cost savings. *Opportunistic requirements* are those that provide a return on investment (e.g., cost savings). These include the standards that require or enable e-commerce, such as the transaction, code and national identifier standards.

Action Item: Management should put its most creative and aggressive efforts into the opportunistic AS requirements. HCOs should not simply strive to meet these requirements, but should do so in a way that actually captures the cost savings by restructuring in-house processes to take advantage of EDI and standardization. These efforts include streamlining and automating eligibility and referral checking, providing better customer relationship management through online interfaces, and automating some collection steps.

Tactical Guideline: From 2001 to 2003, clearinghouses will be major beneficiaries of the HIPAA transaction and code-set standards as HCOs struggle to meet implementation deadlines.

Transaction Standards: What to Do Now



- Assess impact to implement the standard transactions (batch and real-time).
- Identify integration broker requirements, if any, and begin the selection process.
- Begin coordination with your vendors, clearinghouses and trading partners.
- Develop transaction implementation plans from IS and business perspectives.
- Develop testing criteria, including testing with trading partners.
- Draft “Chain of Trust” language.
- Use commercially available or independently developed tools to test compliance with implementation guide.

Whatever strategy you adopt, the clock is ticking! Gartner

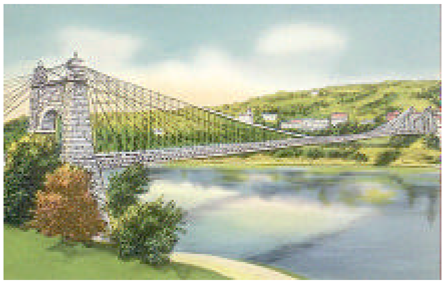
Source: Gartner Research

The transaction standards final rule was postponed often over the past few years, in order to ensure that synchronization of definitions between rules were reconciled to assure consistency across them. However, the implementation guides for these standards have not significantly changed over the past year, allowing early movers to advance toward competitive advantages. Gartner has been advising HCO clients since 1999 to take the following actions (from the WEDI Bulletin, with additions): 1) Commence an assessment of the gaps and impacts to implement the transactions. 2) Identify any translator requirements, if appropriate, and commence the selection process. 3) Involve vendors, clearinghouses and other entities to determine their plans and any assistance that may be available. 4) Determine specific plans for implementation of the transactions from both an IS and business perspective. 5) Determine testing criteria and identify trading partners. 6) Develop “chain of trust” language to provide to vendors and others, as appropriate. 7) Use any third-party testing tools to determine HIPAA compliance with the Implementation Guides.

Action Item: HCOs should make all efforts to accommodate their core applications’ ability to handle standard transaction and code sets — especially with high-volume systems — rather than automatically seeking out clearinghouse options. Use of clearinghouses will eliminate many, if not most, of the financial and intangible benefits intended by HIPAA AS for provider organizations.

Strategic Planning Assumptions: For the first year of enforcement for each HIPAA rule, the government will be tentative and will focus on the most egregious and deliberate violators, rather than on detailed, across-the-board compliance (0.8 probability). The new political administration and Congress will consider HIPAA a top priority, allocate nearly $1 billion for Department of Justice and other agency enforcement activities, and launch aggressive policing of all regulations by 2003 (0.2 probability).

"Good Enough" Security and Privacy



Generations of Civil Engineers

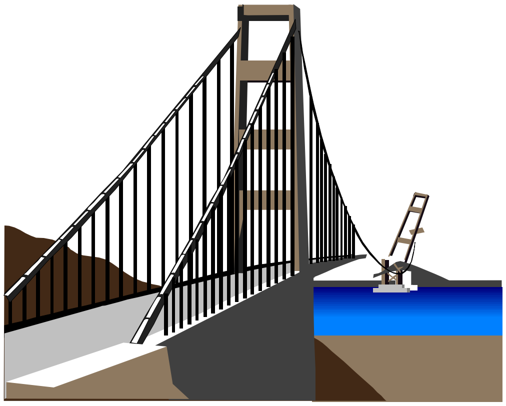
Have Learned That

"Good Enough Is Best."

However, They Have Also

Learned That It

Must Be Good Enough.

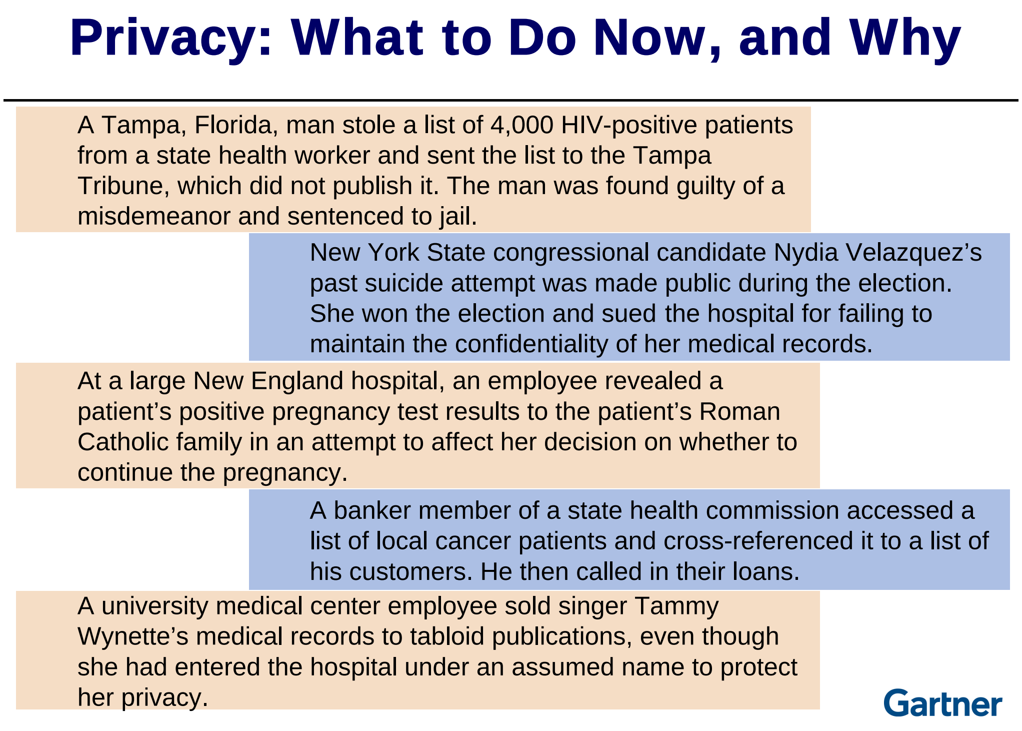


Source: Gartner Research

While it is not possible to delay compliance with the security and privacy standards, it is possible to avoid being frightened by worst-case analyses and committing funds to crash projects. Judicious application of the "80-20" rule can allow an HCO to address the most important concerns first and to get to the final details in the outlying years. The proposed rules have made it clear that DHHS intends to ramp up enforcement gradually: The rule on transactions says so explicitly. Complying with the proposed DHHS security standards will impose significant new costs on HCOs. One must be careful, however, to avoid hysterical and worst-case thinking. The standards generally prescribe common sense requirements for security precautions. They are also vague and usually offer several alternatives to meet each requirement. Security is a threshold requirement. There is little benefit to investing more than is required to meet the regulatory requirement. The old engineering adage applies here: "Good enough is best." The challenge lies in identifying what is good enough.

Action Item: The initial goal for HCOs should be to find the "just enough" level that meets the real needs and keeps the HCO on par with the industry, and then to continuously improve compliance over the years.

New Rules/New Realities: HCOs face fines of up to $250,000 and 10 years imprisonment for wrongfully disclosing patient information. In addition, the information security risks to healthcare providers include civil liability for not protecting patient information.



Privacy: What to Do Now, and Why

A Tampa, Florida, man stole a list of 4,000 HIV-positive patients from a state health worker and sent the list to the Tampa Tribune, which did not publish it. The man was found guilty of a misdemeanor and sentenced to jail.

New York State congressional candidate Nydia Velazquez's past suicide attempt was made public during the election. She won the election and sued the hospital for failing to maintain the confidentiality of her medical records.

At a large New England hospital, an employee revealed a patient's positive pregnancy test results to the patient's Roman Catholic family in an attempt to affect her decision on whether to continue the pregnancy.

A banker member of a state health commission accessed a list of local cancer patients and cross-referenced it to a list of his customers. He then called in their loans.

A university medical center employee sold singer Tammy Wynette's medical records to tabloid publications, even though she had entered the hospital under an assumed name to protect her privacy.

Gartner

Source: Gartner Research

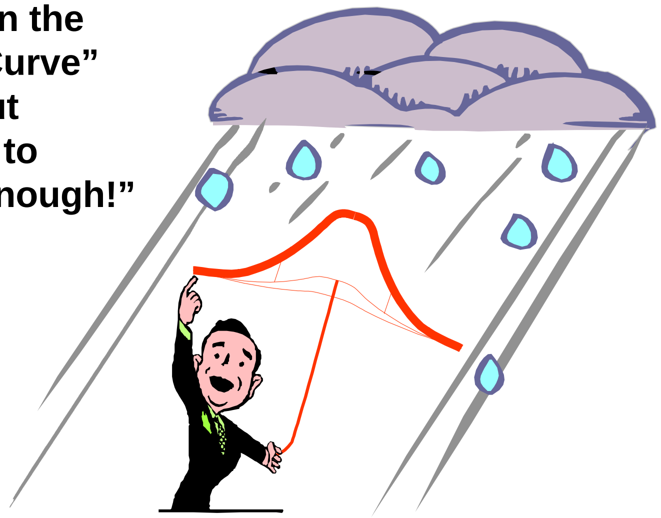
While we advocate a common sense approach to the privacy regulations (e.g., do not accept worst-case interpretations and thus attempt to do too much too soon), there *are* compelling reasons to address this area now. Most of these suggestions are procedural enhancements.

1) *Maintain warning banners* on systems telling employees of their responsibilities to protect patient privacy. 2) *Implement audit tracking* and communicate its existence to identify when medical information is accessed. Although nearly 70 percent of HCOs do not review such logs, their disclosure will inhibit casual browsing. 3) *Require all employees to sign confidentiality agreements annually*. 4) *Program workstations* to log off after inactivity. 5) *Establish policies* to withdraw access for terminated employees to patient information. A recent survey found that only half of HCOs deactivate ex-employee access within 24 hours of termination. 6) *Deliver staff training* on the legal and ethical requirements of patient data privacy. Groups such as the American Health Information Management Association and the American Medical Association should be viewed as partners in this process. 7) *Pilot small information protection projects* such as secure e-mail. 8) *Hire a chief security officer*. Information security officers can be promoted from the medical records, legal or data processing departments of the HCO. 9) *Focus management and board attention* on the problem by contracting an ethical hacker to access, with permission, the health-related information of a board member. Such guerrilla tactics, coupled with a presentation on HIPAA requirements, can be effective attention-getters.

Strategic Planning Assumption: In the second and third years after HIPAA compliance becomes mandatory for each rule, government enforcement — and scrutiny by accrediting agencies — will ramp up gradually, but HCOs that are diligently attempting to meet the standards and pacing the industry in general will not face severe sanctions (0.8 probability).

HIPAA Security and Privacy Strategy

Hide in the
"Bell Curve"
but
Get to
"Good Enough!"



Gartner

Source: Gartner Research

While AS transaction standards represent opportunistic requirements for HCOs, security and privacy mandates should be considered more as support requirements. These are necessary and require investment, but do not have the same potential for cost savings.

The HIPAA security and privacy standards do not directly contribute to the return on investment. They are included to assure the public that there will be no loss of confidentiality caused by using more EDI. It would have been ideal if compliance on these were delayed, so that the industry could begin to use the savings from electronic data exchange to fund compliance. However, that is not legally or politically possible.

The proposed Privacy Rule, which is the most challenging, has the weakest enforcement provisions. The secretary of DHHS will accept complaints through an as-yet-unbudgeted office and evaluate them for civil and criminal penalties after attempting to reconcile the parties.

Action Item: HCOs should build a culture that is fanatical about protecting patients' privacy, but should not go overboard with "crash" solutions: for example, building one HCO-wide database to manage all data for the sake of simplifying access rules and control is probably excessive and definitely expensive.

Market: At least 70 vendors and systems integrators claim to have formal HIPAA service offerings. Many are just entering the healthcare market, seeing HIPAA as a natural extension of their security/privacy experience with other industries.

Preliminary Shortlist for Assessment Help

IBM

KPMG

SAIC

First Consulting

Superior

E&Y (Cap Gemini)

Deloitte & Touche

CSC

Next Tier (could move rapidly):
AC, Arthur Andersen, CBSI, Data Dimensions, EDS, Phoenix, PWC, SMS

Gartner

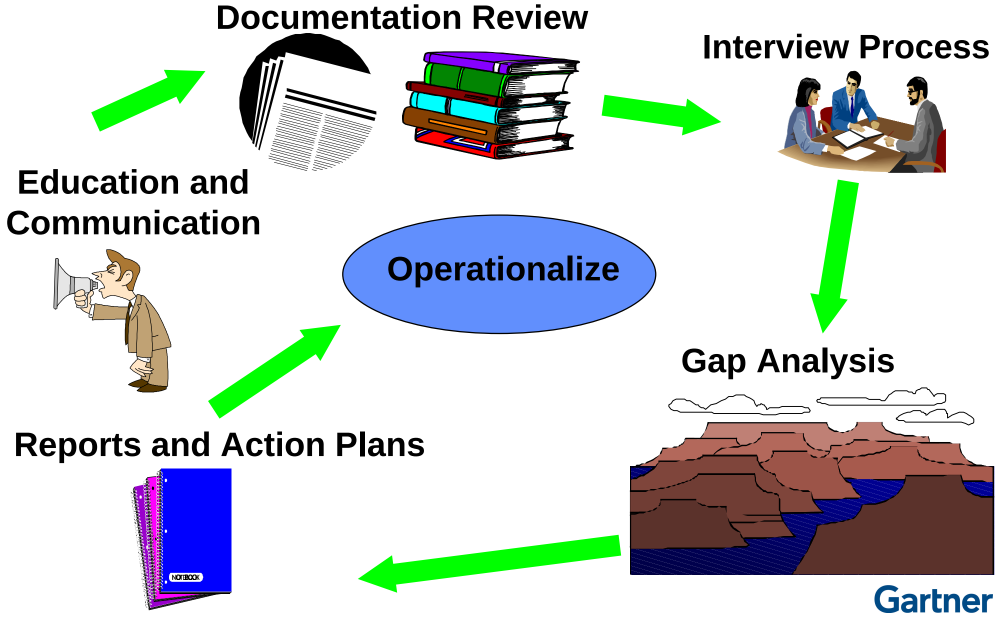
Source: Gartner Research

Although the HIPAA consulting market is too early in its life cycle to differentiate strengths and weaknesses of competitors and their offerings, each of the enterprises listed above has distinguished itself with these key characteristics:

- Strong healthcare-specific industry expertise
- Large parent organizations with extensive staff members and capital resources
- Specific experience and depth with security policy and technology consulting
- Proven capabilities in designing and implementing e-business solutions
- Demonstrated thought leadership in interpreting HIPAA's impact on HCOs via published articles, conference presentations, workshops and participation in summits and committees
- Formal methodologies for helping HCOs efficiently assess their HIPAA-related risks, vulnerabilities, opportunities and compliance costs
- Solution kits or educational tools for communicating HIPAA's impact throughout HCOs
- Commitment to their HIPAA practice through dedicated resources

Tactical Guideline: There are many options for third-party HIPAA assistance beyond the largest consulting enterprises. For a more comprehensive list of enterprises and their services, HCOs should see www.chim.org/Advocacy/mbrcapbl.html.

Assessment Approach: Simplified Version



Documentation Review

Interview Process

Gap Analysis

Reports and Action Plans

Education and Communication

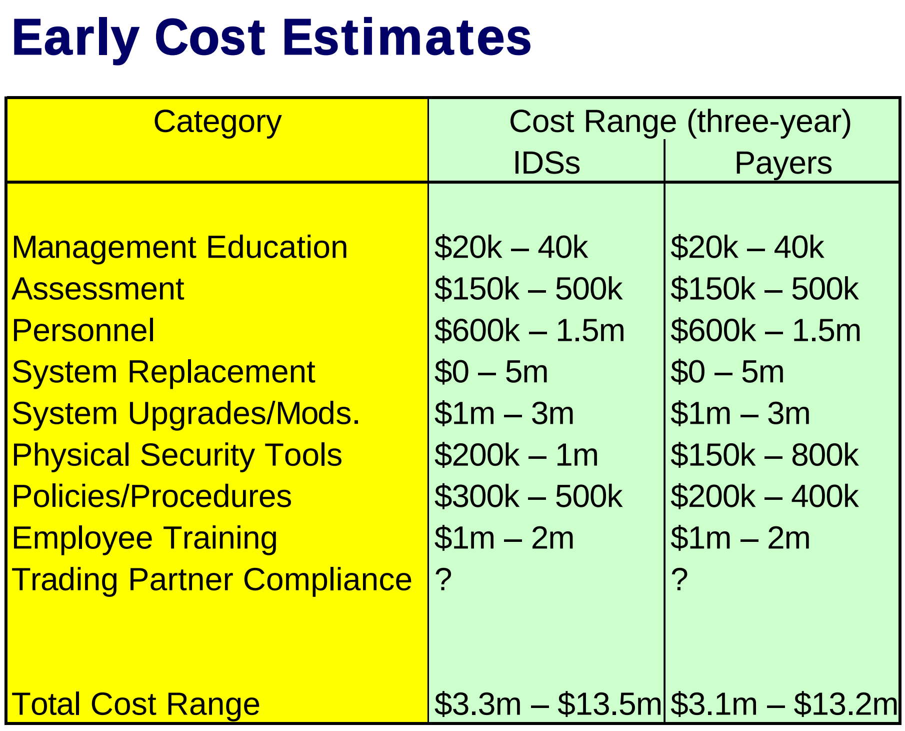
Operationalize

Source: Gartner Research

All of the major consulting enterprises with HIPAA practices have at least a few clients for whom they are conducting assessment projects. They mostly follow a two-tier approach to assessments, usually beginning with financial and administrative electronic transactions and code sets (often calling this service “e-business enablement”), and following with a security and privacy assessment. While the consultants offer formal methodologies and can draw upon specialized skills sets both internally and via partnerships (e.g., with attorneys), their assessment approaches all follow a fairly straightforward approach. However, since HIPAA’s impact affects almost every area of an HCO, this will be a resource-intensive effort. Depending on the HCO’s size, it can expect an initial assessment to take eight to 12 weeks using outside assistance, and 12 to 24 weeks if done internally.

The electronic newsletter HIPAAlert conducted a recent survey of a broad sample of HCOs. Perhaps the most significant finding of the survey is that two-thirds of provider organizations have not yet begun their HIPAA compliance assessments, and 20 percent of providers were waiting until at least August 2000 before beginning action plans. Despite delays in the publication of the final HIPAA privacy regulations, HCOs still face a two-year window for realizing compliance for the approved and nearly approved standards; however, those not yet conducting assessments will use much of those two years for planning.

Strategic Planning Assumption: For at least 50 percent of healthcare organizations, the time and money spent by 2003 on making their applications and processes HIPPA compliant will equal or exceed that spent on year 2000 compliance (0.7 probability).



Early Cost Estimates

Category	Cost Range (three-year)	
	IDSs	Payers
Management Education	$20k – 40k	$20k – 40k
Assessment	$150k – 500k	$150k – 500k
Personnel	$600k – 1.5m	$600k – 1.5m
System Replacement	$0 – 5m	$0 – 5m
System Upgrades/Mods.	$1m – 3m	$1m – 3m
Physical Security Tools	$200k – 1m	$150k – 800k
Policies/Procedures	$300k – 500k	$200k – 400k
Employee Training	$1m – 2m	$1m – 2m
Trading Partner Compliance	?	?
Total Cost Range	$3.3m – $13.5m	$3.1m – $13.2m

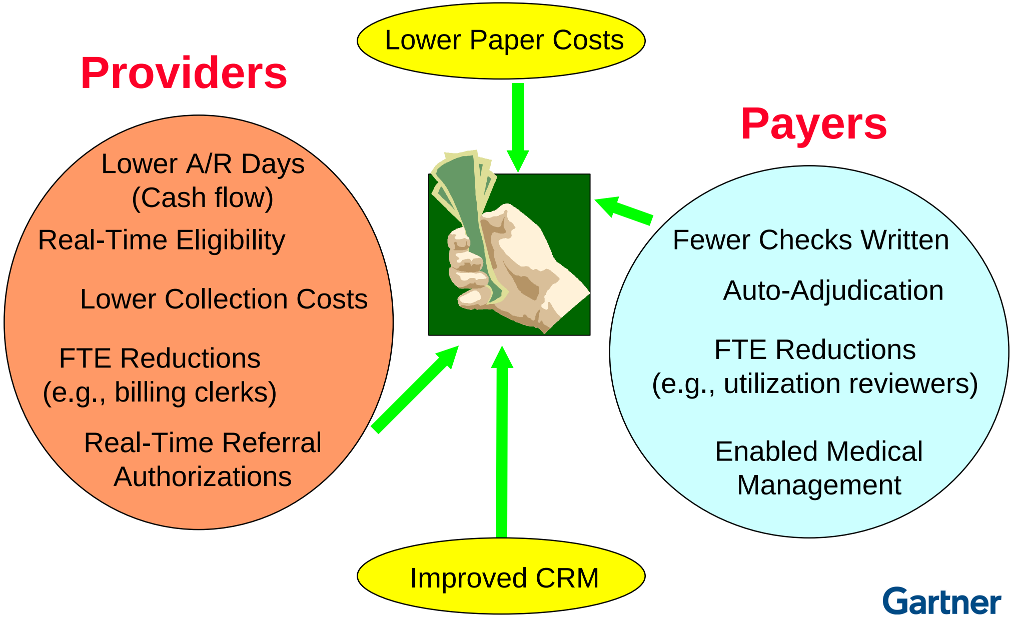
Source: Gartner Research

Many agencies, consultants, analysts, HCOs and reporters have tried to forecast the total spending required for the industry to realize compliance, but calculating realistic figures is not possible until regulations are published and assessments complete. Gartner will frequently survey the industry to provide comparative and summary spending estimates based on real data. In the meantime, we have polled those consulting enterprises that have already completed several assessments for providers and payers, and these figures represent average expected spending ranges for their clients. In specific categories: *Assessments* assume reliance on third-parties that typically charge between $50k and $150k per AS category, which may be higher for larger HCOs; the costs for *dedicated personnel* represent an expectation of three to six full-time staff members; *system replacements* refer to cases where core transaction processing or departmental applications cannot be modified; *system upgrades* include the costs of converting data to accommodate new transaction, identifier and code set standards; the relatively lower figures for payers on *physical security tools and policies and procedures* reflects the expectation that those organizations have slightly fewer points of vulnerability (i.e., fewer departments and applications); and *trading partner compliance* represents a potentially large mystery cost.

Action Item: HCOs should use preliminary cost estimates to set expectations only; comprehensive assessments must be completed to understand individual HCO's expected required spending, none of which have the same makeup or requirements.

Tactical Guideline: As an output of HIPAA assessment efforts, HCOs should focus on identifying and quantifying improvements for those processes offering the highest potential returns via automated transactions and standardization.

The HIPAA Payoff — Tangible ROI



Lower Paper Costs

Providers

Lower A/R Days (Cash flow)

Real-Time Eligibility

Lower Collection Costs

FTE Reductions (e.g., billing clerks)

Real-Time Referral Authorizations

Payers

Fewer Checks Written

Auto-Adjudication

FTE Reductions (e.g., utilization reviewers)

Enabled Medical Management

Improved CRM

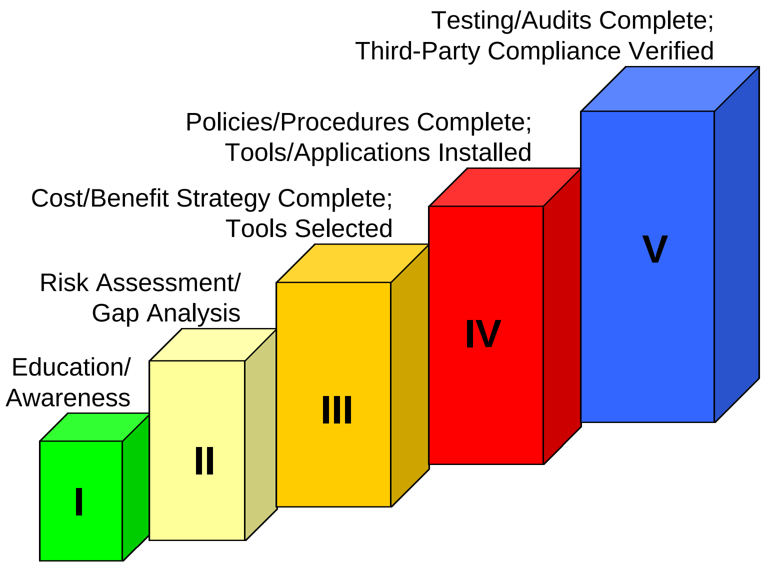
Source: Gartner Research

While WEDI has estimated that HIPAA transaction standards could save $73 billion per year for the U.S. healthcare industry, quantifying the tangible return on investment for individual HCOs is challenging. For example, how does one put a dollar figure on better customer service or improved medical management capabilities? Still, certain savings are inherent, including:

- By reducing its average accounts/receivable days by five, a typical integrated delivery system with $500 million in annual revenues could realize more than $500,000 in additional annual interest income on its receivables, if placed in asset accounts generating eight percent return.
- ADVANCE for Health Information Executives recently reported that the cost of manually processing a referral was close to $70 with the originating provider expending cost to close to $40 and health plans expending close to $10. The majority of these costs are labor costs. On average, physician office staff were spending close to 2.5 hours to complete all of the required processes. With automation, the cost of referrals is reduced to less than $1.50 for health plans and an estimated $5.50 for the originating physician’s office.
- An individual HCO should be able to assess its annual lost revenue from rejected claims, unauthorized referrals and failure to collect co-pays. Standardized and automated transactions will go a long way toward recapturing those revenue.

Decision Framework: Various surveys, coupled with Gartner research, indicate that fewer than 25 percent of HCOs have reached the second level of the HIPAA compliance scale as of August 2000.

HIPAA COMPARE Scale


Testing/Audits Complete;
Third-Party Compliance Verified
Policies/Procedures Complete;
Tools/Applications Installed
Cost/Benefit Strategy Complete;
Tools Selected
Risk Assessment/
Gap Analysis
Education/
Awareness
I
II
III
IV
V

Source: Gartner Research

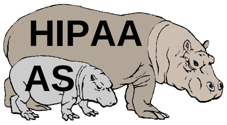
To rate the activity and readiness of HCOs, Gartner has developed the COMPARE (Compliance Progress and Readiness) scale for HIPAA Administrative Simplification:

Level One: At this stage, an HCO has completed its organization-wide general education and awareness program; all preliminary activities are complete. *Level Two:* An HCO has completed (either internally or with outside assistance) a formal assessment of its vulnerabilities and activities needed to achieve compliance with EDI, security and privacy requirements. *Level Three:* At this stage, an HCO has quantified tangible and intangible costs and benefits to realize compliance, and used that information to formulate a comprehensive compliance strategy. This strategy will address HIPAA as an enabler for achieving the HCO’s overall e-business strategy. *Level Four:* An HCO has completed and communicated policies and procedures for achieving compliance to all affected entities, departments and employees. Selection is complete for all physical tools needed for EDI and security compliance, including upgrade or replacement of applications when necessary; there is nothing left to plan or negotiate. *Level Five:* All tools and applications have been implemented and tested. For security and privacy, the HCO has benchmarked the industry and has implemented all measures believed necessary to adequately address requirements. A formal process is in place to address “evolving” requirements and pursue “absolute” compliance.

Recommendation: HCOs should treat HIPAA as a business opportunity, or they will lose competitive advantage.

Recommendations

- **Embrace HIPAA EDI and standardization mandates as the change agents to bring your organization (and its people) the skills it needs to support e-health.**
- **Create a culture of zealous privacy and implement the security to support it, but do not go overboard — address privacy and security regulations with an eye on the "80-20" rule.**
- **If you have not begun detailed assessment efforts, get help, and get busy.**



Source: Gartner Research

Although HIPAA in many ways is *not* like year 2000, it is not going to go away. Analysts have compared HIPAA to year 2000 as a gross measure of impact and a way to grab attention. It is important, however, not to blindly follow the metaphor. Unlike year 2000, the deadlines are not fixed and it is possible to make business decisions to delay or minimize conformance with some of the provisions in the early years. So, what should be the foundations of HCOs' HIPAA strategy?

Carrots (for transactions):

- competitive cost advantage from compliance opportunity to improve process
- straight-through processing and zero latency
- potential as e-health momentum builder

Sticks (for privacy and security):

- civil and criminal penalties
- loss of trust and damage to good name

Timing: uncertain and modestly flexible

Strategy for privacy and security:

- from engineering wisdom: "Good enough is best."
- from military boot camp: "Hide in the bell curve."