Chapter 3
HIPAA Cost Considerations

Background

Actual costs for HIPAA compliance will vary among covered entities (CEs) because of various factors such as size, type of business, organizational culture, geographic locations, and number of business associates. In addition, costs will depend on how "compliant" that CE can be and the amount of risk it can feasibly accept. Obviously, costs will vary depending on whether the organization chooses to implement completely new systems and business processes, only the bare minimum requirements, or something in between. Unfortunately, there is no one good answer to how much HIPAA will cost. However, we believe it is safe to say that initial HIPAA compliance will most likely range from a few thousand dollars for small CEs to a few hundred thousand dollars or more for larger CEs.

Research firm Gartner Group has estimated that HIPAA is expected to cost the healthcare industry at least $3.8 billion between 2003 and 2008, and potentially even 10 times that. The American Hospital Association (AHA) reported* early in 2001 that doctors and healthcare providers are spending vast amounts of money and time to comply with state and federal privacy laws. According to AHA-funded research, hospitals nationwide are planning to spend as much as $22 billion during the first 5 years to comply with applicable HIPAA laws. For example, they project that implementing minimum necessary requirements will cost a minimum $1.3 billion over 5 years for hospitals and up to $19.8 billion if hospitals must invest in new or upgraded computer systems.

The AHA has compiled several other compelling statistics** with regard to estimated HIPAA Privacy Rule implementation costs. A sampling includes:

* Available at http://www.healthdatamanagement.com.
**Available at http://www.hospitalconnect.com.

- Baylor University Medical Center in Dallas has budgeted $7.5 million over 5 years to pay for implementation of HIPAA.
- Texas Health Resources trained 22,000 workers before the April 14, 2003 deadline, and it expects to spend more than $10 million to comply with the law.

The Department of Health and Human Services (HHS), on the other hand, estimated that implementation of the Privacy Rule will cost CEs $17.6 billion over the first 10 years. At the same time, HHS performed a regulatory impact analysis on the Administrative Simplification standards and expects them to save the industry $29.9 billion over 10 years. These estimates were made prior to the Privacy Rule NPRM changes that were released in August 2002, which, with eased requirements, will likely lower the cost estimates and possibly even raise the savings estimates.

In December 2000, Clinton administration officials did some number crunching to determine what costs may be involved. Peter Swire, the Chief Privacy Counsel for the administration at that time, projected the Privacy Rule cost would equate to $6.25 per year for every insured American. According to the administration numbers, the electronic transactions and code sets requirements will save the industry $29.9 billion over 10 years, leaving a net savings of $12.3 billion after paying for privacy implementation costs. These numbers do not incorporate the Security Rule implementation costs.

Studies are showing that HIPAA compliance will cost as much or more than Y2K preparations did for CEs. The positive side of this is that HIPAA costs can be spread out over a longer period of time, perhaps making them a little easier to deal with. Regardless of who turns out to be closest in their estimates of savings or costs related to implementing the HIPAA requirements, the fact remains that CEs will need to spend at least a fair amount of money up front to implement the requirements. Time, probably over a decade or so, will tell if and when the savings occur for HIPAA implementation activities.

Privacy Implementation Costs

Exhibit 1 contains the Privacy Rule implementation activities that will likely involve costs. Use this table to estimate and keep track of your organization's Privacy Rule implementation costs. The estimated costs will vary greatly among organizations, depending on the type of CE, the size, the amount of computer systems used, the number of business associates involved, and other aspects unique to each organization. There may be no cost involved with some of these activities if your organization already has the personnel or resources indicated.

Exhibit 1. Estimated Privacy Rule Implementation Costs

Privacy Rule Implementation Activity	Estimated Cost
Performing a privacy gap analysis to establish your baseline compliance state	
Performing a privacy risk assessment to identify risks to PHI	
Creating and distributing a notice of privacy practices	
Creating required policies	
Creating required supporting procedures	
Assigning personnel to be responsible for privacy	
Assigning personnel to be the point of contact for individuals with questions about their privacy rights, and to report complaints	
Providing initial personnel privacy training	
Implementing electronic technologies to provide safeguards	
Printing, paper, and other notice- and procedures-related costs	
Updating the provider facility directory	
Establishing PHI disclosure accounting mechanisms	
Establishing resources to archive and maintain necessary documentation for at least 6 years per document	
Establishing business continuity plans, including backup and recovery facilities and resources	
Establishing sanctions and the related resources	
Implementing physical safeguards where necessary	
Reviewing and updating marketing and fundraising plans	
Reviewing and updating research procedures and associated forms and documents	
Establishing identity verification mechanisms and practices	
Establishing mitigation mechanisms and practices	
Creating alternative communications methods to give individuals copies of their PHI	
Establishing mechanisms to update and correct PHI in response to individual requests	
Establishing mechanisms to review authorizations and ensure their currency	
Establishing mechanisms to obtain and document acknowledgment of receipt of notices	
Reviewing and updating business associate agreements as necessary	
Establishing mechanisms to de-identify PHI	
Other Expenses	
Total Estimated Costs	

Privacy Ongoing Maintenance Costs

Once you have implemented the Privacy Rule requirements, you will not be finished with your compliance obligations. There are ongoing responsibilities that are necessary to maintain compliance. Exhibit 2 below will help you estimate these costs.

Costs Related to Providing Access to PHI

One of the most hotly debated cost recoup issues is whether or not the Privacy Rule allows CEs to charge individuals who request copies of their records. The rule is pretty clear about this. CEs are permitted to charge a cost that is based on the actual expenses involved with sending the copy of PHI to the requester. These costs include, but are not necessarily limited to, the following:

- Copy supplies (paper, toner cartridges, etc.)
- Postage
- Labor involved with the actual copying

If the individual wants a summary or explanation of PHI, the CE may also charge a fee for the actual clerical preparation of this summary or explanation. The CE must communicate this to the individual and get agreement for the cost before preparing this summary or explanation. This cost may not include the costs related to searching for and retrieving the information, however. Some states have established a cap on the fees that can be charged for the clerical time used. For example, California has set a limit of $6 per hour for the clerical charges incurred in the course of copying and providing access to the PHI. HIPAA does not allow a CE to charge for the time someone supervises an individual within facilities while the individual reviews the PHI. Even though some state laws may allow for such a charge, HIPAA preempts this allowance.

Privacy Officer Costs

A requirement of HIPAA is to appoint a person or position the responsibility of ensuring compliance with the Privacy Rule. A Medical Records Briefing (MRB) survey* reveals that most hospitals are not spending money to create new positions to meet this requirement, but rather the responsibility is being assigned to existing health information management (HIM) directors or someone else within the information technology department. The 329 MRB survey respondents indicate 64 percent of hospitals have appointed a privacy official to address HIPAA requirements, but in only 5.5 percent of these situations acting as the privacy officer is the person's only job. It is likely that smaller organizations will need to assign the privacy responsibilities to existing staff because of their limited budgets.

*Available at http://www.hin.com.

Exhibit 2. Estimated Ongoing HIPAA Privacy Costs

Privacy Rule Maintenance Activity	Estimated Cost
Doing regularly scheduled follow-up privacy gap analysis (recommend every 1 to 2 years) to see where you may now be out of compliance	
Doing follow-up privacy risk assessments to identify new risks and ensure previous risks have not reoccurred	
Creating and distributing a notice of privacy practices	
Personnel to be responsible for privacy	
Personnel answering individuals' questions about their privacy rights, and to report complaints	
Providing ongoing personnel privacy training	
Maintenance of technologies to provide safeguards	
Printing, paper, and other notice-related costs	
Health plans establishing mechanisms to distribute notices on an ongoing basis (at least every 3 years and when significant changes occur within the notice)	
Performing PHI disclosure accounting activities	
Archiving and maintaining necessary documentation for at least 6 years	
Maintaining, testing, and updating business continuity plans, including backup and recovery facilities and resources	
Applying sanctions	
Maintaining and upgrading physical safeguards where necessary	
Maintaining identity verification mechanisms and practices	
Performing mitigation activities	
Utilizing alternative communications methods to give individuals copies of their PHI	
Updating and correcting PHI in response to individual requests	
Reviewing authorizations to ensure their currency	
Obtaining and documenting acknowledgment of receipt of notices	
Reviewing and updating business associate agreements	
Maintaining mechanisms to de-identify PHI	
Other Expenses	
Total Estimated Costs	

However, in larger organizations it will probably be necessary to assign a person to dedicate his entire time to addressing the privacy requirements. AHIMA indicates* the salary range for a privacy officer will be in the $80,000 to $140,000 range.

Use Exhibit 2 to help you plan for and estimate all the various costs related to ongoing Privacy Rule compliance.

Security Implementation Costs

If you do not have thousands of dollars to completely harden your information systems, fear not. There are plenty of things you can do to secure your PHI that will not break the bank or your budget. Remember, there is no such thing as 100-percent information security and there will always be residual risks. You can, however, implement certain measures to reduce your exposure. The risks identified during your security risk analysis combined with security measures that are already in place will help you determine how much money will be spent on Security Rule compliance. Sure, HIPAA is a set of laws that must be adhered to, but the costs associated with protecting information (i.e., time, effort, and money) cannot exceed the value of the information or the consequences if the information is compromised. Your goal should be to align what is needed to reasonably protect PHI with your overall business objectives.

Do not worry about return on investment (ROI) on technology infrastructure and security spending. You have got to spend money on HIPAA compliance anyway, right? True; just make sure you are spending it wisely. Besides, it is difficult changing the lens through which executives see IT and security investments. They need to see money spent on information security as a business expense or investment — not just another IT expenditure. Why? Because it is a business expense — it is the cost of federal compliance, the cost of reasonably protecting confidential health information, the cost of demonstrating due diligence, and the cost of embracing IT to streamline operations and provider higher-quality healthcare.

As discussed in the final Security Rule, HHS utilized Gartner Group to study the impact changes in the healthcare industry might have on the expected impact of the final Security Rule. Gartner estimated that the cost of implementing the Security Rule standards in 2002 is less than 10 percent higher than it would have been in 1998. They go on to say that the preparation for the Security Rule that many CEs have begun offsets this cost difference, making it essentially the same now as it was in 1998. Gartner also determined that compliance with the Privacy Rule may even slightly reduce the overall cost impact of the Security Rule.

*Available at http://www.healthcare-informatics.com.

A really positive aspect of the Security Rule is its flexibility regarding costs. There are many security standards that are "addressable," meaning that CEs have some flexibility, depending on their specific situation. In addition, there are several information security best practices that can be put in place with relatively little or no cost at all, such as:

- Sending out periodic security reminders
- Applying critical patches
- Using stronger passwords
- Turning on logging functions that are built into existing applications and operating systems

There is specific verbiage in the final Security Rule backing HHS' stance on the flexibility of this final rule:

> *While cost is one factor a covered identity may consider in determining whether to implement a particular implementation specification, there is nonetheless a clear requirement that adequate security measures be implemented…*
>
> *Our decision to classify many implementation specifications as addressable, rather than mandatory, provides even more flexibility to covered entities to develop cost effective solutions.*
>
> *…the implementation of these security requirements will reduce the potential overall cost of risk to a greater extent than additional security controls will increase costs.*
>
> *With respect to security, covered entities will be able to blend security processes now in place with new processes. This should significantly reduce compliance costs.*

You should keep these things in mind when the time comes to budget for and spend money on Security Rule compliance.

If you end up outsourcing some HIPAA initiatives to consultants, systems integrators, or large accounting firms, you can expect to be presented with a wide range of hourly rates. The following estimates will vary, depending on your location and the current state of the economy, but should give you a good idea of what some of the going rates are:

- $50 to $100 per hour for basic computer and network work
- $150 to $225 per hour for highly skilled information security experts
- $275 to $350+ per hour for larger accounting/consulting firms that can provide brand recognition

Exhibit 3 contains the Security Rule implementation activities that will likely involve costs. Use this table to estimate and keep track of your organization's Security Rule implementation costs. Like the privacy costs outlined previously, these estimated costs will vary greatly or in some cases not even apply, depending on your needs.

Exhibit 3. Estimated Security Rule Implementation Costs

Security Rule Implementation Activity	Estimated Cost
Administrative Security Costs	
Performing a security gap analysis to establish your baseline state of Security Rule compliance	
Performing a security risk assessment to identify risks to PHI — this may include hiring outside experts to help with penetration testing and vulnerability assessments	
Hiring internal information security experts to build up your compliance team	
Establishing security incident plans, including specific technologies and external resources/expertise to assist in these efforts	
Establishing contingency plans, including backup and recovery systems and facilities and resources such as Uninterruptible Power Supplies (UPS), generators, failover sites, backup devices, and backup media storage and retrieval services	
Implementing security awareness reminders such as screen savers, posters, and mouse pads, along with the necessary training programs and materials	
Establishing employee sanctions along with the associated HR and legal resources	
Reviewing and updating current business associate agreements as necessary	
Creating required security policies and their supporting procedures	
Establishing resources to archive and maintain necessary documentation relating to Security Rule implementation for at least 6 years	
Physical Security Costs	
Implementing physical safeguards where necessary, including facility access controls such as card readers, biometrics, cameras, and alarm systems	
Implementing shredders or other physical media destruction mechanisms	
Technical Security Costs	
Implementing network infrastructure technologies to facilitate confidential data transmission such as VPNs, firewalls, secure e-mail servers, and intrusion-detection systems	
Implementing computer and network strong authentication mechanisms, including tokens and biometrics	

Exhibit 3. Estimated Security Rule Implementation Costs (Continued)

Implementing encryption systems to ensure confidential data transmission	
Implementing secure fax servers and fax machines	
Establishing computer and network access control mechanisms such as new operating system upgrades, policy servers, and possibly even routers and firewalls	
Establishing computer and network auditing mechanisms, including log monitoring and analysis software	
Other Expenses	
Total Estimated Costs	

Security Ongoing Maintenance Costs

Once you have implemented the Security Rule requirements, you will also have ongoing maintenance costs to consider. These ongoing costs of delivering secure information services that adhere to the Security Rule and meet your customers' needs must be low enough so that it is not cost-prohibitive to continue with them. Rather than using theoretical models of total cost of ownership (TCO) and ROI that do not always apply in the real world, look at the overall value that these security investments are bringing to your organization. Look at how it not only enables you to be compliant but also makes your business better by enabling newer technologies that can streamline operations and ultimately lower your overall IT costs.

Security Officer Costs

As with the mandated Privacy Officer position, HIPAA mandates that an individual be assigned as your HIPAA Security Officer for ensuring compliance with the Security Rule. Salaries for this position will vary greatly, depending on the size of the CE and specific needs. Most of the smaller CEs cannot afford to hire a dedicated Security Officer. These CEs will most likely make an existing position, typically the Office Manager, responsible for both privacy and security compliance. This is reasonable in a small environment, especially if most information security services are outsourced. Medium-sized CEs of 50 employees or more might consider hiring a dedicated HIPAA Officer that is responsible for both privacy and security and possibly other areas of IT or operations. Large CEs such as hospitals and health plans will most likely want to have a dedicated Security Officer that focuses solely on security compliance efforts.

Based on various general surveys and job postings, the annual salary ranges for a Security Officer position could vary widely — anywhere from

$30,000 to $300,000 and up. This position is new to a lot of healthcare organizations so there are no specific criteria to determine exactly how much the Security Officer should make. As the healthcare industry sees just how important this position is, more-specific salaries and job descriptions will evolve. For comparative purposes, according to study done by Giga Information Group, Security Officers in the financial services industry can expect to make between $125,000 and $400,000 plus bonuses, depending on who they report to within the organization. This will very likely be lower for the healthcare industry, but shows you how important the position is within larger organizations.

Exhibit 4 lists potential activities that will cost money for ongoing maintenance of your Security Rule compliance.

Moving ahead, you should always assess information security purchases in terms of what is the best fit for your organization — you might not be able to afford the best or need the solution with all the whistles and bells. The "best" for others might be the worst for your particular situation. So do not always assume that the highest priced, or even highest rated, security products or services are the best ones for you. Shop around, try stuff out, and always make sure there is some sort of contingency in case the product or service ends up being a bad match. By all means never, ever, make security purchasing decisions based on price alone.

Chapter 3: Practical Checklist

- Decide how to staff your Privacy Officer and privacy contact responsibilities.
- Decide how to staff your Security Officer responsibilities.
- Do not position technology expenses required by HIPAA as IT expenses but rather as business expenses.
- Budget for your Privacy Rule implementation activities.
- Budget for your Security Rule implementation activities.
- Budget for your Privacy Rule ongoing and maintenance activities.
- Budget for your Security Rule ongoing and maintenance activities.
- Obtain budget approval.
- Keep track of your Privacy Security Rule related spending.

Exhibit 4. Estimated Ongoing HIPAA Security Costs

Security Rule Maintenance Activity	Estimated Cost
Administrative Security Costs	
Performing ongoing security gap analyses (recommended every 1 to 2 years) to ensure ongoing compliance with HIPAA	
Performing follow-up security risk assessments (recommended at least every year) to identify new risks and ensure previous risks have not reoccurred	
Performing risk mitigation activities	
Testing and maintaining your security incident plans to ensure they are still viable for new information systems and business changes	
Testing and maintaining your contingency plans to ensure they are still viable for new information systems and business changes	
Ongoing training costs for personnel, including class and conference registrations, publication subscriptions, and association dues	
Reviewing and updating business associate agreements as necessary	
Maintaining security policies and their supporting procedures	
Establishing resources to archive and maintain necessary documentation relating to Security Rule implementation for at least 6 years	
Applying sanctions	
Ongoing maintenance of the risk management function	
Physical Security Costs	
Ongoing maintenance of physical safeguards and systems	
Management of facility maintenance records	
Technical Security Costs	
Administering and maintaining network infrastructure technologies	
Administering and maintaining computer and network authentication mechanisms	
Administering and maintaining encryption systems	
Administering and maintaining secure fax servers and fax machines	
Administering and maintaining computer and network access control mechanisms	
Administering and maintaining computer and network auditing mechanisms	
Other Expenses	
Total Estimated Costs	