Report on the Impacts of the HIPAA Final Privacy Rule on Hospitals

Prepared for the American Hospital Association by

March 2001

Table of Contents

Key Findings 3
Background 3
Summary Findings 4
Approach 6
Overview of Case Studies 6
Appendix A: Typical Hospital Approach for Complying with Minimum Necessary Requirements 9
Appendix B: Case Studies 13
Appendix C: Cost Projection Model from *FCG December Privacy Study* 25

Key Findings

Despite recent changes from an earlier proposed version, the final privacy rule under HIPAA (the Health Insurance Portability and Accountability Act of 1996) still represents a significant burden on hospitals.

- The response of hospital organizations surveyed ranged from *no net change* to only a *minor decrease* in their projected expenditures for complying with the new requirements.
- Many organizations surveyed are planning to undertake nearly *all* of the same comprehensive steps to comply that they were considering under the requirements of the proposed privacy rule. In many cases, their approach and therefore their cost projection is not expected to change based on the exclusion of disclosures for treatment purposes from the minimum necessary requirements.
- Given healthcare organizations' heightened awareness of patient privacy issues, the associated public relations risks and the criminal and civil liabilities levied for a breach of patient privacy under HIPAA, some organizations are still taking a cautionary and defensive approach to compliance.

Background

In December 2000, First Consulting Group (FCG) produced a report for the American Hospital Association (AHA) that projected the cost impacts on hospitals of three components of the proposed privacy rule set forth under HIPAA. Under this rule, the Department of Health and Human Services (HHS) did not estimate the impacts for these three components – components that AHA believed represented a significant burden for hospitals. These three components were:

- Minimum necessary standard
- Business partner contracting
- Lack of state law preemption

In its earlier study (henceforth referred to as the "FCG December Privacy Study"), FCG reported that the potential cost to hospitals of these three key provisions could range from $4 billion to $22.5 billion depending on the approach that organizations take to comply and the complexity of their information systems. Specifically, costs were estimated to be as low as $4 billion over five years if hospitals generally comply by modifying current information systems and as high as $22.5 billion if hospitals must invest in new information systems.

Figure 1: Projected Cost Impacts on Hospitals of the Proposed HIPAA Privacy Components

	HIPAA Privacy Component Studied			
	Minimum Necessary Use	Business Associate Contracting	State Law Preemption	Total Cost
Projected Cost Impacts of Proposed Rule*	$1.3 – $19.8 Billion	$2.4 Billion	$351 Million	$4.0 – $22.5 Billion

*Source: FCG HIPAA Privacy Study, December 2000

In late December 2000, HHS issued a final rule for HIPAA privacy standards. The key changes to the components for which FCG previously estimated costs included the following:

- The *minimum necessary* requirement was relaxed for disclosures of protected health information related to treatment, allowing healthcare organizations the latitude to determine for themselves how this information is externally disclosed and shared to treat patients. Uses and all other disclosures of protected health information must still meet this requirement.

- *Business partners* are now termed *business associates,* and the requirement for covered entities to closely monitor their compliance was dropped. Patients are no longer considered third-party beneficiaries to contracts between covered entities and their business associates.

No change was made to the *preemption of state laws*; as such, the final rule lets stand those laws that are deemed more protective of personal health information and in conflict with the HIPAA privacy rule.

In addition, other key changes were made to the privacy rule that may noticeably impact the compliance effort for healthcare organizations:

- *Notice of Privacy Practices:* Notice of an organization's practices related to the routine use and disclosure of patient identifiable information must be documented and made available to all new patients and others who request it. While the final privacy regulation included significant additions to the content that this notice must contain, it does not include a model format for such a notice.

- *Patient Consent:* The final rule added a requirement that provider organizations obtain patients' consent prior to the use and disclosure of their protected health information for treatment, payment, and healthcare operations. In doing so, it places an additional burden on covered entities to create an appropriate consent document, develop and implement the corresponding processes across their organizations, and explain these processes to their patients.

In this current report, FCG seeks to revisit cost projections previously put forth in the FCG December Privacy Study in light of the release of the final rule. This report also describes, through case study profiles, the impacts that this rule will have on institutions that represent a cross section of all hospitals.

Summary Findings

In its review of the impacts of the final HIPAA privacy rule on the hospital industry, FCG discovered the following:

- Based on recent changes to the rule, cost projections for the three HIPAA privacy components previously studied may represent *no net change* across all hospitals from the costs projected in the FCG December Privacy Study.

Figure 2: Changes to the Projected Cost Impacts Based on Final HIPAA Privacy Rule

	HIPAA Privacy Component Studied			
	Minimum Necessary Use	Business Associate Contracting	State Law Preemption	Total Cost
Projected Cost Impact of Proposed Rule*	$1.3 – $19.8 Billion	$2.4 Billion	$351 Million	$4.0 – $22.5 Billion
Anticipated Changes Under Final Rule	From *no change* to *a slight decrease*	*Slight decrease*	*No change*	*Overall slight decrease*

**Source: FCG HIPAA Privacy Study, December 2000*

- Because of the public relations risks and the criminal and civil liabilities associated with a breach of patient privacy under HIPAA, several organizations studied did *not* foresee a major decrease in their projected expenditures to comply with the new privacy requirements. These organizations were actually planning to undertake many of the same comprehensive steps to comply that they were considering under the requirements of the proposed privacy rule.

- The criteria that seem to best predict the cost impact of HIPAA privacy on hospital organizations include:
    - Size of the organization (number of hospitals and nature of hospital network),
    - Number and complexity of information systems, and
    - Compliance approach.

  This last criterion varied across the organizations studied and is based largely on the organization's risk tolerance and the leadership responsible for the HIPAA compliance effort. For example, those organizations where the HIPAA effort is led by the Compliance Officer or by Risk Management seem to adopt a more comprehensive and, therefore, more costly approach to compliance. Those organizations where HIPAA compliance is led by the Chief Information Officer seem to be adopting a less comprehensive and, therefore, less costly approach.

The projected impacts of specific components of the final privacy rule varied:

- While the final rule now excludes the application of minimum necessary requirements to treatment related disclosures of patient health information, several organizations interviewed still anticipate employing a resource-intensive process for determining access to this patient information, for developing the associated practices for its use and for monitoring those uses after the fact. Organizations felt that they will need to carefully review *all* of their current uses of patient identifiable health information in order to distinguish between treatment, payment, and healthcare operations uses and to set forth appropriate policies and procedures for each category.
    - In some instances, a case-by-case review of the uses and disclosures will still be required. They anticipate that outside third parties such as health plans and other payers will request more information than is deemed necessary and than will be initially disclosed by their organization. This will likely require legal counsel support, follow-up discussions to clarify the purpose of the request, and re-requests for information.

- Some organizations interviewed actually estimated a slight *increase* in the effort required to train their employees on patient privacy and confidentiality under the minimum necessary requirements given that they will all have to understand and discern the differences between treatment, payment, and healthcare operations uses and disclosures.

- Under the final rule, hospital organizations are no longer required to monitor the use and disclosure activities of their business associates, making compliance less burdensome. This monitoring component represented from 37-89% of the annual operating costs projected in the FCG December Privacy Study for complying with the proposed business associate requirements. Several organizations, however, still expected to have to review *all* business agreements across the organization – with legal counsel support – in order to make an effective determination of applicability under HIPAA privacy rules. Several also expected to work closely with and train their business associates themselves in interpreting and executing the minimum necessary requirements since any inappropriate handling of patient identifiable health information would reflect badly on the organization itself.

- Since the final rule posed no changes to the preemption of state laws, there are not expected to be any changes in the earlier cost projections for this component.

Approach

In order to quickly and effectively determine the operational impacts on hospitals of the changes reflected in the final privacy rule, FCG undertook the following steps:

- FCG prepared a brief outline of the expected implications of the final rule and its impact on hospitals.

- One-to-two hour telephone interviews were conducted with six hospital organization participants from the earlier FCG December Privacy Study.

- Participants were asked to review the previously projected cost estimates, to project the cost impact changes they anticipated for their organization based on the final rule, and to provide examples of the approaches their organization would likely take to comply.

- FCG compiled information from these interviews, looking for areas where quantifiable adjustments were needed in the overall cost projections as well as for specific examples that would help describe the expected burden on individual organizations.

Overview of Case Studies

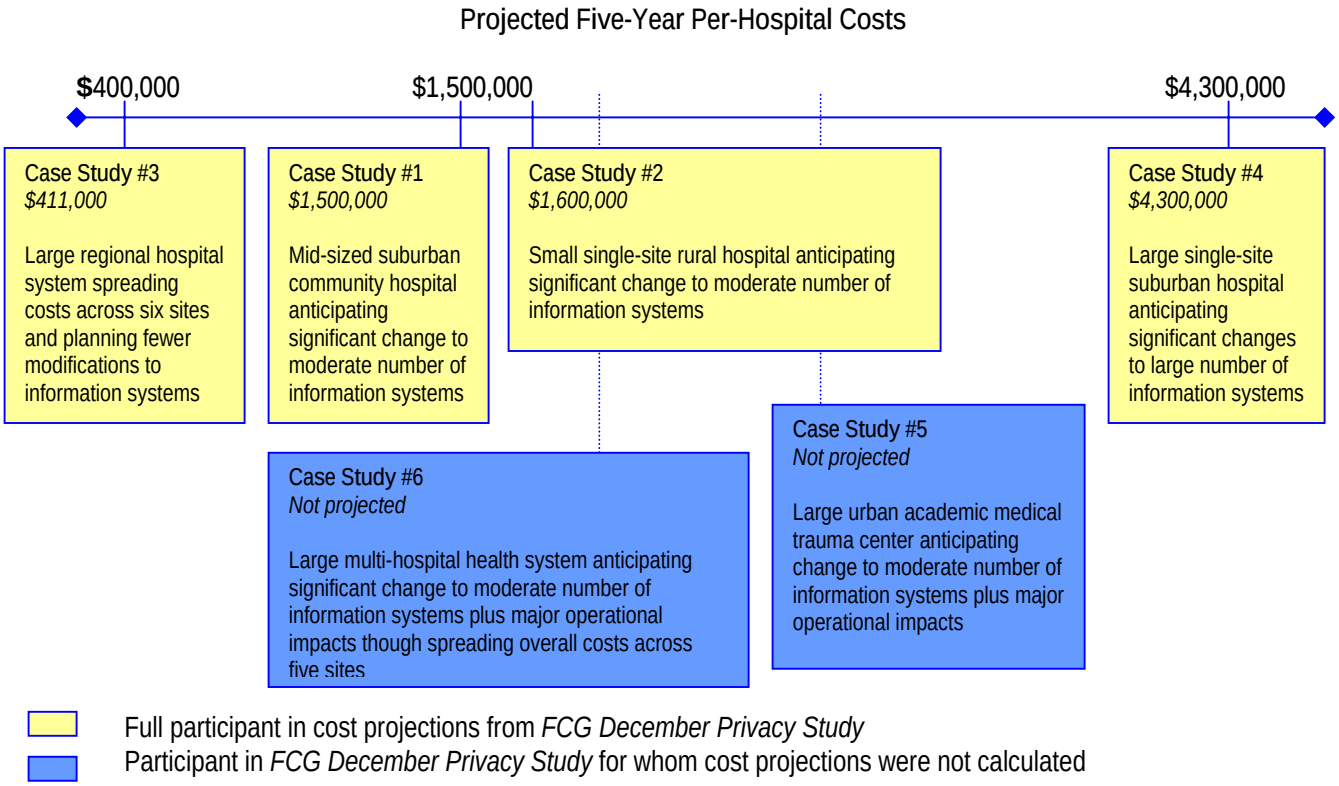
As in the FCG December Privacy Study, hospitals of diverse profiles were included in this report. Participants included both organizations for whom detailed cost projections were previously calculated as well as several other organizations who had participated in impact discussions in the FCG December Privacy Study but for whom no specific cost projections were calculated.

The cost impacts on the organizations profiled seemed to vary according to:

- Size of organization (number of hospitals and nature of hospital network),
- Number and complexity of information technology systems, and
- Compliance approach.

Given that the organizations' ranges of response to the HIPAA privacy requirements varied, their projected compliance costs varied as well.

Figure 3: Profile of Hospital Organizations Contributing to the Cost Impact Analysis



Appendices

Appendix A: Typical Hospital Approach for Complying with Minimum Necessary Requirements

In the *FCG December Privacy Study*, FCG outlined the steps that a hospital would have to take in order to meet the requirements for minimum necessary. These steps were based on those expected for a typical hospital, though the individual approach and interpretation varied for each hospital interviewed.

Under the earlier proposed rule, hospitals would have had to make reasonable efforts not to use or disclose more patient information than is necessary to accomplish an intended purpose. The proposed rule would have specifically required that:

- Hospital staff review, forward, or print out only those fields and records relevant to their need for information;
- The organization review each request on its own merits to determine appropriate use and disclosure;
- Information systems be configured to allow selective access to different portions of a patient's record;
- The organization document policies and procedures for determining such minimum use; and
- The organization maintains a process to periodically review routine uses and disclosures.

Typical Approach

In order to meet these requirements for minimum necessary, organizations would:

1) *Convene a steering committee to determine the overall organizational approach for use and disclosure of patient information.*

2) *Designate a person or team to conduct a comprehensive audit of all existing sources of patient specific information and the systems used to store and maintain such data.* This audit would involve uncovering and investigating each of the specific uses and disclosures of patient information for all of the following categories of staff:

   - Physicians (including radiologists and laboratory pathologists)
   - Nurses, physicians assistants, nutritionists, physical and occupational therapists, social workers, case managers
   - Laboratory technicians, diagnostic imaging technicians, other medical technologists
   - Unit coordinators, ward clerks, nurses aides, receptionists
   - Emergency room and telephone triage staff
   - Medical records staff: file clerks, coders, transcriptionists
   - Billing and collections staff
   - Compliance and risk management staff
   - Legal counsel
   - Clergy
   - Accreditation, licensing and inspection staff
   - Physician credentialing and peer review staff

- Quality assurance staff
- Utilization review and management staff
- Financial services staff
- Research investigators and analysts
- Information services staff
- Contractors, consultants and vendor staff

This investigation would seek to review all:

- Access and viewing of patient information;
- Printing of patient records and reports;
- Computerized queries, compilation and downloading of patient information to other sources (such as PC databases);
- Release of patient information to outside parties; and
- Manipulation of patient files by information services staff.

3) *Meet with leaders of key user departments to explain the organization's approach and confirm the specific access requirements for each department.* This discussion would seek to challenge some departments to reduce or eliminate their need for accessing some categories of patient information. It would also uncover new challenges inherent in managing and limiting access to patient information.

4) *Configure, upgrade or replace the information systems used to store patient identifiable information and manage the access to those data.* Hospital organizations typically maintain distinct information systems that support patient care and store patient identifiable information in the following areas:

- Hospital-wide Clinical
- Dental
- Operating Room
- Emergency Department
- Call Center/Nurse Triage
- Laboratory
- Radiology/Imaging
- Pharmacy/Medication Management
- Cardiology
- Transcription
- Patient Registration/Admitting
- Patient Scheduling
- Patient Billing
- Utilization Management/Review
- Case Management
- Tumor Registry
- Research

These systems perform a number of complex clinical, administrative and business tasks and store, display, transmit and print varying degrees of patient identifiable information to accomplish these tasks.

Hospitals would first make attempts to configure those systems so that the organization's intended access permissions and restrictions could be adequately carried out. Attempts would be made, for example, to restrict the access by non-clinical staff to portions of the system containing patient identifiable clinical information. If, based on the system's capabilities, the required or desired access restrictions were not possible, the organization would be required to make programming changes to the application itself so that it could carry out the desired restrictions. In many cases, the system design is such that many clients cannot make changes to the application themselves but instead must rely on the vendor to do so. In some cases, the vendor will make changes (at a cost) to suit the organization's individual needs; in other cases, the vendor may seek to gain input from other clients before installing changes to an application intended to affect all of those clients. In either case, these client-driven software changes and application upgrades cost the hospital client the resources in testing and installing the more advanced capabilities required to meet their needs.

5) *Train staff in appropriate uses and disclosures of patient information.* While most organizations already have a staff-training program in place, organizations would still need to either develop or revise its content to cover patient privacy and the use and disclosure of patient information. Additional training time would also be required for all staff across the organization. Medical records staff – as the principal keepers of the patient record – would require still more additional training in order to effectively understand and manage the disclosures of patient information outside the organization.

6) *Employ after-the-fact audit mechanisms (including audit trails) to monitor compliance with the minimum necessary requirement.* Organizations would develop an approach for auditing accesses to patient information and then devote a portion of a staff position to carry out that approach throughout the year. This staff resource might principally focus, for example, on accesses and disclosures by certain administrative staff, or on accesses to certain patients' records deemed more visible or sensitive in nature.

Changes in Final Rule

Although the final rule reduced some of the burdens under the minimum necessary component, hospitals will still be required to undertake reasonable efforts:

- Not to use *internally* more information than is necessary for treatment purposes; and
- Not to use or disclose *internally and externally* more information than is necessary for payment and other healthcare operations.

For disclosures that occur on a routine basis (such as for insurance payment, transfer of patient care or subpoenas), a covered entity is required to have policies and procedures in place governing such exchanges but does not have to make case-by-case determinations. Providers must also have a process for reviewing non-routine requests on a case-by-case basis to ensure that only the minimum necessary information is disclosed.

The rule also now applies to *all* paper-based information – not just that which was in electronic form at some point.

Typical Approach – Final Rule

Under the final rule, all of the above steps will still be required with a few resulting changes:

1) All paper-based information would be covered, expanding the scope of the investigation and controls necessary to satisfy the minimum necessary requirement.

2) Although the disclosure of patient information to external entities for treatment purposes is no longer subject to the minimum necessary requirements, the organization must still investigate and limit all uses and disclosures internally and externally for payment and healthcare operations, and all internal uses for treatment purposes. In addition, organizations must now clearly delineate the difference between uses and disclosures of patient information for treatment purposes.

Appendix B: Case Studies

Case Study Number 1
Single-Site Suburban Community Hospital

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
1	167	900

Highlights of Approach to Achieve Compliance

The HIPAA compliance effort at this organization is being lead by the Chief Information Officer. At the center of their challenge in complying with the minimum necessary requirements lies their core hospital information system, a clinical and financial application developed in the 1970's for hospital organizations seeking to minimize the onsite technical support that other information systems can require. This "off-the-shelf" application lacks the capability, however, for hospital clients to make their own major changes to fit local needs. In order to meet the expected requirements for minimum necessary – as well as any other HIPAA requirements that require technological support – this organization must rely on this information system vendor to produce and distribute an updated version of its software that is capable of handling the intricate data management functions that the new rule requires. While the cost that their vendor will charge them for this update is not yet known, the organization will incur staff and other technical costs for preparing, testing and installing that software and for re-training staff in its use.

In addition to this core application, this organization maintains dozens of other information systems – each of which handles patient identifiable information and each of which will need to be upgraded at an additional cost to the organization.

In order to meet the full requirements of the privacy rule – particularly as they now apply to paper-based information as well – this organization plans to install chart-tracking software in order to manage and monitor the flow of this information throughout the hospital organization.

This hospital also plans to hold several executive-level committee meetings in order to determine their overall approach for addressing minimum necessary requirements across the organization. The subsequent effort to investigate the current uses and disclosures of patient identifiable information will involve the time and commitment of managers from fifty departments plus an analyst to coordinate the effort. Once these uses and disclosures are understood and classified, associated policies and procedures will be developed and implemented and an additional thirty minutes of training will occur for each of its 900 employees.

Initial Cost Projection

	Implementation	Annual Operating	Total Five-Year Costs
Minimum Necessary	$796,370	$ 9,939	$836,126
Business Associates	$261,204	$97,395	$650,784
State Law Preemption	$14,718	$ 7,408	$ 44,350
Total Cost	$1,072,292	$114,742	$1,531,260

Changes Based on Final Rule

Minimum Necessary	• Overall, there were no significant cost changes associated with implementing the new minimum necessary requirements. • This organization does anticipate increased costs to support clinical research projects and clinical drug trials for: 1) Developing policies and procedures and reviewing requests for minimum necessary use and disclosure of patient identifiable information, and 2) Maintaining a list of the actual uses and disclosures of patient identifiable information under those projects. • This organization expects that there may be a slight decrease in costs associated with implementation of new or upgraded systems due to the reduced burden of tracking clinical access to treatment-related information.
Business Associates	This organization estimates that although there may be a slight decrease in implementing the new business associate requirements because the need to closely monitor business associates has been eliminated, the organization is still creating a process that captures and tracks the history of disclosures of patient identifiable information to all business associates.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Case Study Number 2
Small Rural Single-Site Hospital

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
1	52	320

Highlights of Approach to Achieve Compliance

The HIPAA compliance effort at this small rural single hospital is currently being lead by its CEO. Though the number of information systems that will likely be impacted by HIPAA is smaller than that for its larger hospital colleagues, their resources are also much thinner, creating in comparison a larger burden on the hospital's operating budget. This organization is budgeting a relatively huge capital expenditure (nearly $750,000) for the purchase of a new core hospital system specifically to meet the anticipated compliance requirements of HIPAA that it currently cannot handle. This organization is also planning to install software to track paper records throughout the organization given the final privacy rule's expansion to cover paper-based information.

One of the key areas of HIPAA impact and focus for this organization – particularly under the minimum necessary requirements – involves staff training and education related to patient privacy and the use of information. Both the initial training development and its execution are expected to consume a large quantity of staff resources in the first year of implementation.

Initial Cost Projection

	Implementation	Annual Operating	Total Five-Year Cost
Minimum Necessary	$891,935	$ 58,246	$1,124,919
Business Associates	$132,379	$ 71,221	$ 417,263
State Law Preemption	$ 9,705	$ 1,550	$ 15,905
Total Cost	$1,034,019	$131,017	$1,558,087

Changes Based on Final Rule

Minimum Necessary	• This organization estimates a potential increase in the annual operating costs for staff training on patient confidentiality issues and discerning between treatment, payment and healthcare operations uses and disclosures of patient identifiable information. This organization expects that each member of the workforce will need to go through annual retraining in order to fully understand the requirements. • This organization also estimates increased costs to establish a process for reviewing research requests under the minimum necessary standard as well as documenting disclosures of patient identifiable information related to research so that an accurate accounting of disclosures can be provided to the patient.

Case Study Number 2 – *continued*

Business Associates	In reviewing its previous cost projections, this organization estimates a potential *increase* in the expected business associate costs based on the new definition of business associate in the final rule. • They now plan to review *all* business contracts to determine HIPAA applicability rather than allow department heads to determine whether the uses of information under that relationship are governed by the new HIPAA privacy rule. This could add to the projected implementation costs under the business associate component. • In addition, they now anticipate developing contracts, policies and procedures to cover the processing with state agencies of patient identifiable information previously thought to be de-identified but now covered.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Case Study Number 3
Large Multi-State Multi-Hospital System

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
6	1,099	7,960

Highlights of Approach to Achieve Compliance

The HIPAA effort at this large multi-state, multi-hospital system is being lead by a special HIPAA coordinator responsible for compliance across the organization's three-state region. Because of its size and geographic spread, there is a much larger coordination effort required. Uncovering and understanding all of the current uses and disclosures of patient identifiable information becomes difficult and tedious in such a large and dispersed organization. Their biggest area of risk and concern involves the thousands of patient-related reports generated monthly across the organization – each of which needs to be reviewed and potentially reconfigured to meet the minimum necessary requirements. These reports currently contain various levels of patient-specific clinical information and are used for a variety of purposes both internally and externally.

Making and implementing system-wide decisions regarding access to patient information can be difficult and bureaucratic at such a large multi-state organization. Their ten-member Steering Committee meets for two hours every two weeks to make policy-level decisions about who should be able to access which pieces of patient information, then their eight-member manager team meets four hours per month to review and implement the resulting recommendations. At the most granular level, an analyst must then meet with each department manager across the organization regarding all of the affected reports in order to understand the purpose of each, and then make appropriate recommendations and adjustments. As a result, the time and resources required to understand and implement the minimum necessary standard are larger for this organization than most others interviewed.

While some of the system requirements to support the minimum necessary standard will need to be programmed by this organization's own internal information systems staff, some of the changes are likely to require the support of the organization's core systems vendor. Internally, many hundreds of hours are expected to be required *for each computer application* to be reprogrammed to support the organization's revised access requirements. But for those instances where the expertise of a systems vendor is required, the cost and resource burdens on the organization for these changes are not fully known. As a result, this organization has earmarked a half million dollars (included below) in a contingency fund for this as-yet-unknown computer system expense.

Initial Cost Projection

	Implementation	Annual Operating	Total Five Year Cost
Minimum Necessary	$1,011,618	$ 68,567	$1,285,886
Business Associates	$ 415,546	$128,411	$ 929,190
State Law Preemption	$ 53,023	$ 48,797	$ 248,211
Total Cost	$1,480,187	$245,775	$2,463,287
Total Cost Per Hospital	$ 246,697	$ 40,963	$ 410,548

Changes Based on Final Rule

Minimum Necessary	This organization's biggest concern with respect to minimum necessary use and disclosure involves internal and external reports. • They currently produce between 1000 and 2000 reports per month for financial and clinical purposes and will have to determine what information is required for each purpose, who will have access to these reports under the new requirements, and with whom this information can be shared. • Ad hoc requests for patient identifiable information are also problematic. For example, requests by physicians for profile reports on their patient panels must be reviewed to determine whether minimum necessary restrictions will apply based on the purpose and intent of the request.
Business Associates	This organization does not expect any significant changes to their projected costs for addressing the new business associate requirements. They currently have a centralized process to identify, review, develop and revise business associate contracts – an effort which they will continue under the new rule. This ongoing effort utilizes Microsoft Access to track *all* business associate contracts.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Case Study Number 4
Large Single-Site Suburban Hospital

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
1	491	3,400

Highlights of Approach to Achieve Compliance

The HIPAA effort at this large single-hospital organization is being lead by a specially designated HIPAA project manager who reports to the Chief Information Officer. As a result of its focus on information technology, this organization expects a huge burden in its HIPAA compliance efforts to upgrade or replace many of its dozens of clinically focused systems. This organization estimates that its few core systems supporting the hospital could each require over 1,000 hours of staff time to assess current system capabilities, reprogram or receive from its vendors upgraded software, test these upgraded systems, install them and train appropriate staff. In addition, dozens of other smaller clinical applications may require a similar effort (though of smaller proportions) to achieve compliant capabilities. The majority of these multi-million dollar changes are required to support restricted access and tracking requirements related to the minimum necessary standard.

As a result of the new applicability to paper-based information, this organization also anticipates the need for software to track the distribution of and access to medical record charts. Early estimates of the capital costs associated with this installation are $100,000.

Initial Cost Projection

	Implementation	Annual Operating	Total Five Year Cost
Minimum Necessary	$3,230,580	$ 21,443	$3,316,352
Business Associates	$ 169,237	$ 175,062	$ 869,585
State Law Preemption	$ 52,642	$ 21,831	$ 138,966
Total Cost	$3,452,459	$ 218,336	4,325,803

Changes Based on Final Rule

Minimum Necessary	This organization estimates a 5-10% decrease in overall costs related to the minimum necessary provision as a result of the revised final rule. • With the inclusion of paper-based information in the final rule, the organization believes that developing policies and procedures will be less burdensome since the organization no longer must distinguish between electronic and certain forms of paper information. • This organization does anticipate an increase in the projected training costs to cover annual employee retraining on patient privacy policies and procedures that it now feels will be necessary to effectively convey the differential requirements for the use and disclosure of patient information.

Case Study Number 4 – *continued*

Business Associates	Because this organization believes that their earlier cost projection with regards to the business associate requirement was low (indeed it was low compared to their colleagues), they now believe that their initial cost estimate *stands* and that it now more appropriately reflects the level of effort expected under the final rule.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Case Study Number 5
Large Single-Site Urban Hospital

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
1	547	4,600

Highlights of Approach to Achieve Compliance

The HIPAA compliance effort at this large urban trauma and teaching hospital organization is lead by a director under the Chief Information Officer. While their ability to invest in major changes to their information systems will likely be limited for budgetary reasons, the culture and size of this community based organization will make the operational implementation of HIPAA all the more challenging – particularly under the minimum necessary standard. Dozens of specialty treatment units and clinic based programs in both the inpatient and ambulatory settings across the city each maintain its own clinical requirements and relationships for treating patients and handling the associated clinical information. Community-based social programs and numerous state agencies are all involved in the treatment of this hospital's patients. The effort required to uncover and investigate all of the uses and disclosures of patient identifiable information and implement the necessary restrictions while still effectively supporting the organization's current functions, therefore, is expected to be more like that of a multi-hospital system.

The ongoing effort to comply with minimum necessary requirements at this organization is also expected to be greater than that typically required for similar organizations of its size. Because of its decentralized structure and leadership, increased measures for restricting and monitoring access to patient information are anticipated. Again, given the community-based nature of its clinical programs and the multiple outside agencies supporting patient care, ongoing use and disclosure of patient information could be difficult to manage and monitor.

Initial Cost Projection

No cost projection is available. This organization participated in the earlier *FCG December Privacy Study* but did not project detailed costs. The comments below reflect projected changes to the core financial projection model costs based on the adjustments that this organization would *likely* have to make to comply with the new requirements.

Changes Based on Final Rule

Minimum Necessary	This organization estimates a slight increase in the projected costs for implementing the minimum necessary requirements • They believe that it will take them more time to: 1) determine which hospital activities are considered treatment and 2) to document the routine uses and disclosures under these circumstances. • They anticipate training specific staff and providing access to triage mechanisms for determining how to categorize different types of requests for patient identifiable information. One example they cited involves requests for lab results by physicians unknown to the organization. While it might be assumed that the request is for treatment purposes, the organization will need to review *all* cases such as this to determine the purpose of the request and whether minimum necessary rules would apply. Another example involves physicians requesting patient profile information regarding pap smear findings and treatment. The organization feels that it will need to determine whether such a request meets the guidelines for treatment; if it does not then minimum necessary restrictions would apply. (If the request is in support of clinical research or patient marketing, for example, then more stringent use and disclosure restrictions would apply.) • They are also not confident that their training and triage approach alone would be effective given the potential for inappropriate information to still be released in a decentralized organization. As a result, they anticipate developing auditing mechanisms to ensure that the right patient information is disclosed to the right requestors under the right circumstances. • This organization also anticipates an increased burden in handling re-requests for information when less patient information is provided than originally requested. • Since clinical research occurs in a decentralized manner throughout the organization (and because it makes up such a large component of what this organization supports), control and tracking of access to this subset of patient information will be a challenge. They expect to review all requests for patient identifiable information related to clinical research and to document all disclosures of this information. • Finally, this organization anticipates extensive training to educate business associates in interpreting and administering the minimum necessary requirements.
Business Associates	While this organization estimates a slight *decrease* in the projected costs for becoming compliant under the new business associate requirements, they: • Anticipate that an audit process will be put in place to track the history of disclosures of patient identifiable information to business associates that are not conducting payment, treatment or healthcare operations on behalf of the organization. • Plan to review *all* business contracts to determine HIPAA applicability rather than allow department heads to determine whether the uses of information under that relationship is governed by the new HIPAA privacy rule. This could add to the projected implementation costs under the business associate component. • Will likely employ Microsoft Access to track business associate contracts.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Case Study Number 6
Large Single-State Multi-Site Hospital System

Organizational Profile

Number of Hospitals	Number of Beds	Number of Employees
5	1500	25,000

Highlights of Approach to Achieve Compliance

The Vice President for Compliance and Risk Management is overseeing this organization's HIPAA effort. They are already well along in their work to achieve compliance and their approach is relatively comprehensive and detailed as compared to their colleague organizations. While their efforts have not yet been focused on information systems, they do anticipate significant costs in that regard and have requested capital reserves be set aside to cover those expenses.

The majority of this organization's current efforts and projected costs involve the review of access to patient identifiable information and the development and implementation of policies and procedures to address those uses. While the organization maintains a well-functioning process to update policies and procedures, such an effort involves extensive centralized coordination and nearly all department managers across this large regional health system. Given their past experience and success with JCAHO accreditation, they anticipate that this effort could take up to two years to complete.

The organization is also investigating processes that will support efforts to locate and update all affected business associate contracts. This process is currently decentralized. The organization anticipates implementing more centralized review and control – including the involvement of external legal counsel for interpretation and support.

Initial Cost Projection

No cost projection is available. This organization participated in the earlier *FCG December Privacy Study* but did not project detailed costs. The comments below reflect projected changes to the core financial projection model costs based on the adjustments that this organization would *likely* have to make to comply with the new requirements. Overall, this organization anticipated no significant change in the cost projections for minimum necessary, state preemption and business associates.

Changes Based on Final Rule

Minimum Necessary	This organization estimates that costs could be as high as initially projected or slightly reduced depending on the approach that they use for establishing role based access. • Costs would be higher if upgrades are still required across all of their information systems in order to effectively implement the minimum necessary requirements. • This organization strongly believes that in the spirit of HIPAA privacy and to decrease its risk and exposure regarding patient privacy, it will still attempt to minimize the use of information for treatment. One example cited involved the use and disclosure of patient information to distinct radiology groups who read patient films. The organization plans to restrict access for each group to only their own patients' films. Similar situations exist in many of their contracted specialties. • This organization also anticipates that many outside third parties will request more information than is deemed necessary and than will be initially provided by the organization. This will likely require legal counsel, follow up discussions to clarify the purpose of the request, and re-requests for information. Examples are expected to include insurance plans, workers compensation and disability requests. • This organization anticipates a challenge in reviewing and categorizing uses and disclosures of patient information for pharmaceutical research given that some of these efforts potentially involve marketing uses.
Business Associates	No change is expected in the cost projections for business associate contracting.
State Law Preemption	No change is expected in the cost projections for state law preemption.

Appendix C: Cost Projection Model from *FCG December Privacy Study*

Sample of Cost Projection Model for Implementation of Minimum Necessary Requirements from the *FCG December Privacy Study*

Organizational Profile #1: Small standalone hospital									
Minimum Necessary Use - Key Action Steps	**Implementation Costs**								
	Hours	**FTE**	**Hr Rate or Salary**	**Volume or Frequency**	**Salary Cost**	**Benefits Percentage**	**Benefits Cost**	**Capital Costs**	**Total Cost**
Access Review									
Steering Committee meetings	4		$36	10	$1,427	30%	$428		$1,855
Departmental reviews	2		$27	50	$2,729	30%	$819		$3,548
Research & compilation	160		$23		$3,747	30%	$1,124		$4,871
Monitoring									
Develop approach and strategy	30		$36		$1,080	30%	$324		$1,404
Ongoing audit trail and review					$0		$0		$0
SUBTOTAL POLICY REVIEW/MONITORING									$11,678
IT Assessment	20		$21		$425	30%	$128		$553
IT Implementation									
Configure current systems	160		$21		$3,402	30%	$1,020		$4,422
Vendor Upgrades/Implementations									
IT Department staff	1,200		$21	12	$306,144	30%	$91,843		$397,987
Department staff	1,000		$27	12	$327,480	30%			$327,480
Application (user) training	2		$16	900	$29,574	30%	$8,872		$38,446
Paper Charts									
Select chart tracking software	40		$21		$850	30%	$255		$1,106
Install chart tracking software	40		$21		$850	30%	$255		$1,106
Train users on chart tracking software	2		$11	7	$154	30%	$46		$200
SUBTOTAL IT									$771,299
Policy Implementation									
Training development	160		$18		$2,909	30%	$873		$3,781
Policy and procedure training	0.50		$16	900	$7,394	30%	$2,218		$9,612
SUBTOTAL TRAINING									$13,393
			GRAND TOTALS		$688,165		$108,205	$0	$796,370

Explanation of Key Components and Compliance Steps:

Cost Component	Compliance Issues and Steps Involved
Access Reviews	Includes designating a *Steering Committee* to oversee the steps in tackling this requirement. Also includes overseeing the identification of all sources of patient specific data. This is accomplished by an analyst or other designated staff person conducting *departmental reviews* and identifying what patient information is being accessed and for what purpose. *Research and compilation* of these findings would help inform the steering committee of current practices and help determine the appropriate approach to take. Establishing categories of access to patient information then determines the access privileges granted or denied to staff.
Monitoring	Hospitals will have to determine an approach for monitoring access to patient information. After-the-fact monitoring is complicated, time consuming and resource intensive. Most hospital information systems do not provide complete or user-friendly audit reporting capabilities; many capture edits or changes to patient information but not accesses or views. Many do not provide a user-friendly, meaningful report format. Many organizations do not currently have sufficient resources to devote to widespread audit review of system accesses. More effective approaches involve random sampling or targeted monitoring of certain types of information access. Organizations that employ after the fact monitoring of patient record accesses estimate it would require up to a full time staff resource to accomplish this task effectively.
IT Implementation	Once determinations are made of the organization's access requirements, staff in Information Technology will need to modify current software applications to execute the desired configuration and controls.
Vendor Upgrades/ Implementation	In addition to configuring current information systems for minimum necessary requirements, hospitals will also need to implement additional system capabilities. The upgrade of information technology (IT) systems to meet the minimum necessary requirements comprises the greatest portion of the compliance burden. Of the five major hospital information systems currently in use, most cannot provide the components necessary to assist in meeting the current requirements for minimum necessary. These requirements include user access restrictions at the level of specific data fields and user-friendly reports that comprehensively track both changes to and views of patient data. Most organizations will need to install upgrade versions of software supplied by their vendors to provide the additional required capabilities; some will even have to replace applications that cannot and likely will not be able to provide the access and monitoring capability for compliance with minimum necessary requirements.
Paper Charts	Computer-based audit trails do not capture accesses of paper-based patient information. In order to effectively comply with minimum necessary requirements involving paper-based records, organizations will likely need to purchase and implement software that tracks the location of patient charts throughout the organization including who has requested and accessed each patient record. Hospitals will have to go through a process to select, install and train users on the selected chart tracking software.
Policy Implementation	After determining access requirements, hospital organizations will have to develop policies and procedure for implementing and complying with the minimum necessary requirement. Time will be spent developing policies and procedures as well as a training program that clearly explains the procedures. Staff would then be trained both initially and on an ongoing basis.