FOCUS: HIPAA

HIPAA Readiness Collaborative in Hawaii

ABSTRACT

The vision of Hawaii’s HIPAA Readiness Collaborative (HRC) effort is to realize the positive potential of HIPAA through a collaborative process that engages the entire healthcare delivery system. Goals include reducing the cost of healthcare through streamlining, reducing the cost of HIPAA implementation for HRC participants, and improving the interoperability between facilities through use of standard technologies.

Marva Chun, Susan Forbes, DrPH, Steven Gose, Brenda Kumabe, Jeffrey Loo, Lorraine Nichols, Luis Rosa, Laura Sherrill, and Jim Turner

The Hawaii healthcare marketplace, like all else in this most remote land mass in the world, is relatively small, with 25 acute care hospitals, 45 long-term care facilities, 3,000 physicians, and two major private sector health plans. People rarely travel to the mainland for healthcare. What competition exists occurs with recognition that cooperation is necessary for success in this unique environment.

Hawaii is also famous for its “aloha spirit,” the hallmarks of which are collaboration and sharing. In that spirit, Hawaii’s hospitals, working with the Healthcare Association of Hawaii, Hawaii Medical Association, Hawaii Permanente Medical Group, and Hawaii Medical Service Association (Hawaii’s Blue Cross/Blue Shield program), formed the Hawaii Health Information Corporation (HHIC) in 1994. The mission of this not-for-profit organization is to collect, analyze, and disseminate statewide health information to support efforts to improve the quality and cost efficiency of the healthcare provided to the people of Hawaii. Collaboration has been a central theme of HHIC’s work in such endeavors as data standardization, selecting a severity adjustment tool, standardizing the approach and selecting a vendor for measurement of “patient satisfaction,” and implementing HIPAA. HHIC is the neutral, fair broker of information and, in HIPAA parlance, a business associate of hospitals and other covered entities that submit individually identifiable health information needed to address individual business needs and to further HHIC’s mission.

KEYWORDS

HIPAA  Compliance strategies  EDI  Security policies
Privacy policies  Awareness training  Technical security
Background and Vision

In early 2000, hospital CIOs approached HHIC to initiate a collaborative approach to HIPAA implementation. Myriad reasons supported this approach:

- Hospitals had (and still have) limited resources to devote to HIPAA.
- Following Y2K implementation efforts, garnering the financial and human resource support needed for HIPAA implementation would be difficult.
- All covered entities needed to address the same issues, suggesting a standardized approach.

The vision of the HIPAA Readiness Collaborative (HRC) is to realize the positive potential of HIPAA, including improving the flow of patient information to enhance patient care, and reducing administrative overhead. More immediate objectives relate to reducing HIPAA implementation costs by standardizing approaches, pooling resources, and, potentially, sharing consultant expenses. Specific objectives are cited in the body of this article.

Currently, 51 member organizations have directed 105 individuals/employees to participate in HRC activities. This membership includes nearly all hospitals, health plans, long-term care facilities, home care agencies, practice management companies, and laboratories, as well as the state departments of Health and Social Services (Medicaid agency).

Benefits of participation in HRC include embracing the entire healthcare community, establishing relationships and building expertise to overcome our geographic isolation, building an infrastructure for work that must be performed, reducing risk of noncompliance, and positioning Hawaii as a progressive healthcare marketplace. By embracing the entire healthcare community, Hawaii’s covered entities, and related business associates, increase the chance of successfully achieving the “goodness” of HIPAA. Working together, we can make our work scalable and “bootstrap” the smaller providers and agencies.

First Steps

Early in the process, HRC worked as a committee of the whole, with about 15 regular participants. We identified the “low hanging fruit” of HIPAA — those activities all covered entities needed to address and for which work could begin before final rules were in place — and our structure evolved.

HRC’s first step was to sponsor HIPAA education sessions for CEOs, physicians, and other hospital and health plan staff. In 2000, three such sessions were held, reaching nearly 500 people:

- SAIC’s (Science Applications International Corp.) half-day conference in February 2000 served as a “HIPAA 101” to raise awareness of the upcoming challenges.
- Comdisco HIPAA two-day summit for Hawaii healthcare community was held in March 2000 to provide overarching security and EDI education to stage quick-start of community HIPAA implementation components and scope of work.
- Hawaii ITEC two-day conference was held in December 2000 and offered a Healthcare Track that included a session to rollout the subcommittee’s HIPAA pilot policies to the healthcare community.

Additionally, HRC sent a request for proposal to key HIPAA consultants to address our initial priorities. After reviewing the proposals and meeting with the consultants, we determined that everybody, consultants included, was learning about HIPAA in real time and that our group’s knowledge base was both deep and broad. We decided to address initial priorities ourselves, and call in consultants later for more complex work.

To develop policies and training materials and to address EDI (electronic data interchange), HRC needed to move beyond the committee of the whole, and it needed financial resources. The structure that evolved is shown in figure 1.
FOCUS: HIPAA

Financing/Structure
Membership fees provide financing for the Collaborative. HRC has two membership categories: Charter Members (hospitals) and Affiliate Members. Charter Members contributed most of the budget between July 2000 and December 2001.

A representative of each Charter Member participates on the Steering Committee, along with the chair of each subcommittee. The Steering Committee establishes priorities and identifies and resolves overlapping or conflicting issues, creates new subcommittees as needed, and provides final review and formal adoption before subcommittee deliverables are released to the Collaborative as a whole. The Steering Committee meets monthly and the full Collaborative meets quarterly.

Subcommittees develop their overall goals and objectives for ratification by the Steering Committee. They develop deliverables, with feedback from individual organizations included in their process. Compliance officers and corporate counsel often review the two policy committees’ work in progress. Subcommittee schedules vary, depending on the work to be done.

EDI Subcommittee

Goals and Objectives. HIPAA costs have been justified primarily through the savings attributed to the Administrative Simplification portion of the regulation. Unless payers and providers work together, potential savings could be lost and/or large costs could be incurred to prepare and implement HIPAA electronic data interchange (EDI). The EDI Subcommittee was therefore formed with the following objectives:

- Promote education and shared learning.
- Identify high-value HIPAA EDI transactions/data elements.
- Minimize costs associated with HIPAA implementation.

Structure. The subcommittee consists of appropriate payer and provider representatives of HMSA (the Hawaii Blue Cross/Blue Shield program), Medicaid, three other smaller payers, all major hospitals (15-plus), four major practice management vendors, two clinical laboratories, and Tripler Army Medical Center. (Fortunately, Hawaii has a relatively small number of provider and payer organizations, and they have a good track record for collaboration. HMSA has a large market share and an 80 percent EDI penetration using a proprietary EDI format. The other large payer is the Medicare Part B intermediary, which has 70-80 percent of claims submitted electronically using the NSF format.)

Accomplishments.

Education. The Washington Publishing Company was engaged to present a two-day education session on ANSI X12, which was attended by about 30 people from seven organizations. Representatives from the Utah Health Information Network (UHIN) and Claredi were also invited to speak at ITEC 2000. Creation of a Hawaii version of the UHIN community-based clearinghouse was considered but rejected because of the ease of connecting the relatively few providers and payers in Hawaii and the high degree of electronic claims submission already using existing “free” infrastructure without clearinghouse fees.

HIPAA business benefit. We developed a priority ranking for the business opportunity offered by each transaction, as follows:

- Claims (837I/837P) — Create the opportunity for 100 percent electronic claim submittal (excluding claims with attachments) because smaller health plans in Hawaii would be required to offer claims EDI.
- Remittance (835) — Same as above.
- Eligibility (270/271) — Providers prefer a real-time eligibility transaction, but most payers do not consider real-time eligibility to be a HIPAA requirement and feel they have inadequate time to develop such a transaction given the October 16, 2002, deadline. Batch eligibility does have value if responses are returned before the next clinic day.
- Claim Status (276/277) — Most providers prefer a batch implementation of the transaction to check on outstanding claims.
- Authorization (278) — Hawaii does not have a high degree of managed care penetration, and requests for medical attachments cannot be supported by the transaction.
- Enrollment, Premium Payment — Excluded from scope.

For each transaction, we identified the high-value data elements beyond the minimum HIPAA requirements necessary to actually bring business value. For example, the minimum eligibility response (271) is a simple Yes or No. This transaction must include eligibility dates, plan codes, and PCP information to have business value to providers. We are working with local payers and vendors to incorporate this minimal level of information into their HIPAA transactions.

Local codes. HMSA and Hawaii Medicaid use approximately 2,500 local codes, all of which must be converted to national codes by October 2002; other local payers frequently use these same local codes for their contracts and billing procedures. We are working with all payers to convert to national codes in a consistent, measured manner by June 2002.

Communication. We asked the Technical Subcommittee to develop approaches for both batch and real-time EDI that would comply with HIPAA Security and Privacy regulations. Over time, it became apparent that payers were not committed to developing real-time eligibility using the HIPAA transactions, so the real-time communication was dropped as a requirement. It also became apparent that dial-up modems were being interpreted as secure communications. We are still investigating developing a private, secure communications hub for secure e-mail and to connect Hawaii payers and providers.

Testing/certification. The WEDI/SNIP White Papers on testing and certification have been important sources of information for this subcommittee. Based on the White
Papers and discussions with Clareti, we decided to recommend claims and remittance certification testing for the full six levels. The many payers and providers in Hawaii that do not develop their own software will make this testing recommendation to their software vendors. We expect to achieve more thorough and consistent testing by using a certification company and to reduce the amount of testing done between payer and provider.

We have tracked the EDI strategies and readiness dates for each provider and payer in the HRC and for their clearinghouse partners. It now appears that most payers/vendors will be ready for internal testing in March or April 2002 and external testing in June 2002. Testing will be coordinated through the Collaborative.

Trading partner agreements. The final product is a framework for a common trading partner agreement, to contain legal trading partner language, communication standards/protocols, and payer implementation guides for each transaction where HIPAA allows flexibility. The framework will provide a starting point for each vendor and will promote the HIPAA values of standardization and administrative simplification.

Technical Security Subcommittee Goals and Objectives. The Technical Security Subcommittee’s goals and objectives are to:

• Evaluate technical security options and reach consensus on Hawaii’s preferred approaches.
• Explore standard technology options for achieving interoperability and streamlining the delivery of healthcare.
• Achieve consensus on the best approach for Hawaii to achieve interoperability.

The subcommittee has committed to deliver a secure network connectivity solution that can support the transmission of HIPAA-compliant transaction data by April 2002.

Structure. The subcommittee includes 12 senior network and security administration analysts from Hawaii’s major hospitals and health plans. Participants bring extensive experience and knowledge from government, financial services, and healthcare information security. Experts in other areas, such as EDI and security policies, meet with the committee as needed. This subcommittee has been meeting weekly for seven months.

Accomplishments. The subcommittee began with a preliminary review of draft HIPAA technical security provisions to assess the scope of compliance requirements and identify areas that may dictate significant or unexpected compliance efforts on the part of HRC participants. Based on our findings, the subcommittee initiated activities to identify areas where collaborative technical solutions or community standards could be beneficial to HRC participants. Attention was focused on prospective technical solutions that support information communications between covered entities and that require consensus technical standards to facilitate deployment among the many HRC participants, and on assessing technical solutions that would be difficult for single institutions to deploy and that would be prohibitively expensive for any but the largest organizations.

To date, we have identified several areas where HRC participants have an interest in offering solutions to address HIPAA requirements in critical clinical and administrative process areas. Among these are solutions offering secure network connectivity options for electronic information transfers between covered entities, and secure e-mail for transmission of messages containing protected health information between providers, payers, and the public. We are currently refining design concepts and qualifying implementation strategies for deploying recommended technical solutions in these areas.

The subcommittee has experienced a high level of ongoing support from HRC participants. Besides committing many of their most talented technical resources to participate in subcommittee work, HRC participants have been most willing to share their technical expertise and information regarding their internal systems and requirements. Reflecting the perceived value of this community effort, many HRC participants have also committed to adoption of HRC-recommended solutions and have prioritized their internal HIPAA-related project development activities accordingly.

Barriers. Several issues have challenged our efforts to deliver timely and responsive solution sets. Among these are the current draft status of the HIPAA technical security provisions, the broad span of technical solution sets required to support the compliance needs of small to large covered entities, and the anticipated costs of deploying prospective technical solutions.

While we have made significant progress in qualifying prospective technical alternatives, final selection of a preferred solution has been hampered by uncertainty regarding specific technical features required for HIPAA compliance. Without approved HIPAA technical security regulations, the subcommittee must choose between recommending an interim solution that may require revision when final HIPAA technical security regulations are adopted, or incorporating conservative and potentially costly technical features that will ensure HIPAA compliance.

Identifying solution sets that address HIPAA requirements and also account for the diverse installed systems and technical capacities of both large and small covered entities has also been a challenge. The result has been the need to define multiple-solution and system feature sets that recognize the diversity of needs and capabilities that exists among HRC participants and provides options best fitting individual institution circumstances.

Finally, there have been considerable challenges in developing technical solutions that are both HIPAA compliant and cost-effective for both large and small covered entities. In performing our assessments and design work, we confronted considerable difficulty in defining technical solutions responsive to HIPAA requirements and cost justifiable with respect to upfront development and ongoing operational costs.
Security Policies Subcommittee

**Goals and Objectives.** HRC chartered the subcommittee to meet four primary objectives:

- Develop a policy baseline deliverable that satisfies HIPAA Security NPRM (notice of proposed rulemaking) requirements and can be easily customized/updated by HRC member organizations
- Promote community-wide collaboration to minimize the overhead costs associated with policy development and implementation
- Agree on community HIPAA security guidelines to streamline Hawaii healthcare business processes and relationships.
- Propose Hawaii community guidance in implementing HIPAA security policies and community-defined minimum best practices to support relevant Hawaii 21st century healthcare business models.

**Structure.** Our aim was to include representatives of payers, hospitals, physicians, and all other healthcare services, such as laboratories, rehabilitation programs, and long-term care facilities, on the subcommittee. The initial 10-member group included representatives from HMSA, five major acute care hospital systems, a major laboratory, and a major health information service company; while not fully representative, subcommittee members represented a significant portion of the Hawaii healthcare marketplace. This working together of competitors in the community to share practices and operating expectations/issues was a first.

Standing subcommittee meetings of one and one-half to two hours were held weekly over a six-month period. Whenever possible, documents were prepared and reviewed prior to meetings, so meeting goals were to obtain clarification, present and walk through deliverables, approve HRC Steering Committee policy submittals, and receive/provide HIPAA development and/or resource updates.

A protected web site on the HHIC/HRC URL was established to provide members with common access to inventory deliverables, work-in-progress policies, resource material, meeting notes, schedules, agendas, etc. In addition, the committee used e-mail for quick communication.

After approval of the Steering Committee, subcommittee policy drafts were released to other HRC subcommittees for comment, and were then released for broad Collaborative comment after incorporating primarily the feedback of the Technical Security and Privacy Policies subcommittees.

**Accomplishments.** The subcommittee reviewed HIPAA Security NPRM policy requirements to determine how HRC members could implement them consistently and cost-effectively. Quoted estimates averaged $150,000 to $200,000 for developing HIPAA security policies for the Collaborative or an individual organization. In addition, average organizational development and implementation timeframes spanned a year or more, with an average of half a man-year of relatively expensive mid-to-senior management resources.

The subcommittee prioritized the pilot set of policies for the collaborative proof-of-concept, primarily referencing the Security NPRM Implementation Guide and Comdisco’s HIPAA Implementation Guide to evaluate alternative policy set deliverables. The Chain of Trust and Nondisclosure/Confidentiality agreements and Systems Access, Data Stewardship, Data Classification, and Electronic Mail (e-mail) policies were selected as the proof-of-concept policy set. The selection strategy was to deliver those policies we believed would best support the upcoming HIPAA EDI implementation and address common community security issues. To equip committee members to consistently format draft policies and support the policy content with standard practices and laws, we researched policy development references and community policy formats and drafted a standard policy template/outline for adoption by HRC to promote policies consistent in look, feel, and content. The references included CPRI Toolkit, Baseline Software, MIS, Hawaii healthcare organizations’ policy formats, other states’ HIPAA collaborative policies, and recommended best practices.

Policy content was researched initially via the Security NPRM Implementation Guide list of references. The British Standard 7799, For the Record, HCFA Internet Security Policy, NIST Common Criteria for Information Security Evaluation, NIST Internet Security Policy, WEDI/SNIP White Papers, and the Security NPRM were important sources of information. Nine additional references were added for the post-pilot policy set deliverables, and other sources of information are still being added to the committee reference library. In all, 30 references were provided to individual committee members and their organizations’ reference library and for use in customizing HRC’s policies drafts (see figure 2).

The HRC Steering Committee directed the Security Policies Subcommittee to be inclusive rather than selective in policy content regarding best or required standards/practices. To best serve the diverse HRC membership, policy completeness in addressing the HIPAA Security NPRM was considered to be higher priority than having the Committee judgmentally scale down the policies for reasonableness; customizing efforts were deemed more appropriately undertaken by each member organization.

The committee also developed a policy-mapping matrix as a working tool, based on the Security NPRM Implementation Guide, to facilitate committee identification of NPRM requirement coverage, policy overlaps/cross referencing, consistency checks, and potential operational issues associated with the policies.

The 20 policy/agreement deliverables are available for HRC member use; however the entire set will be revised after the Security final rule is released and after HRC legal counsel makes its review. Annual policy reviews have been scheduled to keep the deliverables relevant.

Specific accomplishments to date include:

- Eighteen HIPAA baseline policies and two confidentiality agreements were published within six months of subcommittee inception. Each member contributed an

2. Department of Health & Human Services Administrative Simplification, Subscription to HIPAA-REGS Listserv, hotlinks to NPM, final rulings, FAQs, Tentative Schedule for Publication of HIPAA Administrative Simplification Regulations, http://aspe.hhs.gov/adsmsnp


docs

6. Health Care Financing Administration (HCFA), Balanced Budget Act (BBA) of 1997 (Public Law 105-33) was signed into law by President Clinton in August 1997. This legislation enacts the most significant changes to the Medicare and Medicaid Programs since their inception 30 years ago. Additionally, it expands the services provided by HCFA through the new Child Health Insurance Program (Title XXI), http://www.hcfa.gov regs/bbapdfat.htm

7. Medicare Modernization Act of 2000. This legislation contains reform elements of the detailed specifications released by the Administration last June. The proposal is the centerpiece of the Administration’s efforts to modernize and strengthen the Medicare and Medicaid Programs since their inception 30 years ago. Additionally, it expands the services provided by HCFA through the new Child Health Insurance Program (Title XXI), http://www.hcfa.gov/regs/bbapdfat.htm


9. National Committee on Vital and Health Statistics (NCVHS), In adopting standards, the law requires the Secretary to rely upon the recommendations of NCVHS, HHS’s policy advisory committee in health data, standards, privacy and health information policy, http://www.ncvhs.hhs.gov/


12. Office for Civil Rights - Final Privacy Regulation and Related Information, • Rule in PDF Format: Zipped (2.6MB), in or 8 parts: Part 1 Part 2 Part 3 Part 4 Part 5 Part 6 Part 7 Part 8, • Rule in Text Format: Zipped (725KB), in or 8 parts: Part 1 Part 2 Part 3 Part 4 Part 5 Part 6 Part 7 Part 8, • Rule in HTML Format: Preamble Part 1 Part 2 Part 3 Part 4 Part 5 Part 6 Part 7 Part 8, • Technical Corrections to the Rule, published in the Federal Register on 12/29/00 (Text | PDF), • Summary of Regulation/HHIS Fact Sheet, 12/20/00 (HTML|Microsoft Word), • Press Release, 12/20/00 (HTML|Microsoft Word), • White House Statement on Health Information Privacy, 12/20/00 (HTML|Microsoft Word), • Remarks by the President on Medical Privacy, 12/20/00, • Press Briefing on new Privacy Rule, 12/20/00, • Other Fact Sheets (coming soon), • Answers to Frequently Asked Questions (FAQs) (coming soon), http://www.hhs.gov/ocr/hipaa/

Security, Privacy, & Policies


2. CPIR Tool Kit, The CPIR Toolkit outlines general principles and provides best practice and examples of how health care providers should manage the security of their paper and electronic records. Sections of the CPIR Toolkit identify key activities to integrate into the process of managing information security, http://www.cpi.org/security/cprr/index.html

3. Hawaii Health Information Corporation (HHIC), Hawaii HIPAA Readiness Collaborative policies and hot links to other references and sites, http://www.hhic.org


5. HCFA Internet Security Policy formalizes the policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information, http://www.hcfa.gov/security/secipolicy.htm

6. Healthkey is a multi-state, Robert Wood Johnson Foundation funded project to create a replicable model for Public Key Infrastructure (PKI) for the health care industry. It is being executed by the following five organizations: Massachusetts Health Data Consortium (MHDC), Minnesota Health Data Institute (MHDI), Foundation for Health Care Quality (FHQC), Washington), North Carolina Healthcare Information and Communications Alliance (NCHCA), Utah Health Information Network (UHIN), http://www.healthkey.org/

7. HIPAA alert, HIPAAUDIO features expert commentary, case studies, Q&A, compliance tips, links to original, full-text documents and helpful HIPAA resources, HIPAA Primers, http://www.hipaaalert.com/

8. Kapiolani Health Information Security Policies

9. Massachusetts Health Data Consortium (MHDC), Our members are the most prominent health care organizations in the region. The Consortium collects data, publishes comparative reports, promotes electronic standards, educates through information exchange events and research, http://www.mhshealthdata.org/


12. NIST Information Technology Security: An Introduction to Results-Based Learning, This bulletin introduces some of the principles for the training of staff members according to their roles within their organizations and for measuring the results of the training. The material in this bulletin was excerpted from NIST Special Publication 800-10, Information Technology Security Training Requirements. A Role- and Performance-Based Model, http://csrc.nist.gov/publications/nistbd/1498 -04.txt


14. Queens Medical Center Information Security and Confidentiality Policies


16. WEDI Strategic National Implementation Process (SNIP), The WEDI HIPAA SNIP Task Group has been established to meet the immediate need to assess the industry-wide HIPAA Administrative Simplification implementation readiness and to bring about the national coordination necessary for successful compliance, http://www.wedi.org/hips Snip/hipaa SNIP

17. Tripler Army Medical Center Policies, Information Systems Security Program, Automated Information System Incident Detection, Handling, and Reporting Procedures

estimated 150 hours, or one-half man week per month over the six-month period.

- The first six proof-of-concept documents were delivered in two months, with each subcommittee member contributing approximately 45 hours.
- The pilot policies created have been referenced as usable templates by several groups and/or publications: Phoenix Health Systems HIPAA Policies audioconference, HCPro, WEDI SNIP, and the Gartner Group.

Privacy Policies Subcommittee

**Goals and Objectives.** The subcommittee’s goals are to:

- Develop a community understanding and interpretation of the privacy rule
- Create policies and procedures to meet the requirements of the rule

Based on many of the participants’ previous experience with the enactment of Hawaii’s health information privacy law, the group paid special attention to possible interpretations of the law and interpretative and operational issues.

**Structure.** Subcommittee members represent hospitals, laboratories, health plans, long-term care facilities, and private physician offices. Participants bring experience and knowledge from medical records, risk management, compliance, legal affairs, laboratories, practice management, long-term care, and independent physician practices. Experts in other areas, such as research or billing, meet with the committee as needed.

**Accomplishments.** Initial efforts focused on individual rights of access and amendment and the uses/disclosures of protected health information (PHI) that do not require consent, authorization, or agreement. This decision to focus in this manner was based on previous experience with implementation problems that occurred in the interface between providers as custodian of PHI and community uses and needs for that PHI. By addressing these uses and disclosures first, we hoped major implementation issues that affect our entire community would surface and be addressed, by legislative action if necessary, before the effective date of the privacy rule.

To date, policies, procedures, and implementation tools for individual rights to access and amend PHI and use/disclosure of PHI pursuant to judicial and administrative proceedings have been developed and distributed for comment to HRC.

The policy on access to PHI includes the individual’s right to access, specified reasons for denial, and a formal written denial/appeal process. Letter templates were created for the written responses required with the reviewable and unreviewable denials, as well as the appeal process.

Interpretive concerns include how each entity will define its designated record set, and state preemption concerns with denial of access (state and federal law differ in language on grounds of denial of access to the individual). Operational concerns include the difficulty of wording a denial letter in plain language that covers all the legal reasons an entity may deny access (such as CLIA); how to determine “reasonable” cost-based fees; developing a reasonable verification process for telephone requests for information on billing records; whether denial of telephone access to billing information must be in writing; and how to note and handle access to billing records for minors who have legally consented to their own care.

Amendments to PHI policy include the individual right to request amendment; specified reasons for denial; a formal written denial/appeal process; linking the amendment and/or request to the PHI; and informing others of accepted amendments. Templates were created for the amendment request and the variety of letters required by the rule. Interpretive concerns revolve around the issues of provider inability to determine the accuracy of the amendment, or original documentation if the document creator is unavailable. The proposed solution was to develop two categories of acceptance — verified and unverified — so future providers will have additional information about the accepted amendment before they make treatment decisions based on the information. Operational concerns include educating providers on the difference between verified and unverified amendments; the process of linking amendments to PHI; and how to apply the amendment policy to billing records (for example, whether a formal written process is necessary or reasonable when an individual calls about an error in name spelling or a wrong charge on the bill).

The Disclosures for Judicial and Administrative Proceedings policy outlines the requirements for obtaining specific statements and documentation prior to responding to a subpoena or discovery request. Templates were created for Affidavits of Appropriate Notice and Protective Court Order, as well as letters for use when necessary statements or documentation are missing. Interpretive concerns include exceptions to this process for health oversight, public health, and law enforcement; the entity’s obligation to determine if statements and documentation demonstrate compliance with the requirements; and ambiguity in state law regarding when the time for objection has elapsed.

Operational concerns include how to distinguish between the varying types of subpoenas and related requirements, and periods of objection.

The subcommittee’s next steps are to review comments on the above policies and continue to develop a community interpretation and identify and address compliance issues. Work has already begun on policies and procedures relating to business associates; law enforcement; abuse, neglect, and domestic violence organizations; organ donation; decedents; threats to health and safety; health oversight; and research. Once the exceptions portion of the law is addressed, the committee will focus on legal requirements related to the internal operations of the entity, such as responses, authorizations, notice, and minimum necessary.

**Barriers.** While subcommittee members have knowledge gained in the state’s process with Chapters 323C Hawaii Revised Statutes, the scope and challenges imposed by HIPAA privacy rule can be daunting.
Education and Training Subcommittee

**Goals and Objectives.** This subcommittee provided a mechanism for HRC members to develop and impart the tools, skills, and knowledge necessary to maintain and evolve an ongoing security and privacy awareness training program.

Our aim was to accomplish as much as possible through voluntary effort, with the objective being a comprehensive training methodology the members of the HRC could use and tailor to their own organizations’ needs.

**Structure.** The six-person core group meets every other Friday afternoon. The extended subcommittee membership included 20 individuals representing primarily hospitals, and also some health plans and payers. The core team coordinated most of the work and obtained input from the subcommittee in testing the waters prior to presenting final work to the HRC membership.

**Accomplishments.**
- Security awareness packet, including virus prevention and protection, workstation security (both desktop and laptop), computer security incident reporting, password management, Internet and e-mail usage, backup and recovery, social engineering, and information confidentiality, sanctions, and penalties.
- Privacy and security rule summary, seven topics in two sections derived from the Privacy and Security regulations. The first section covers topics all workers need to know; the second covers topics relevant to workers who need to use PHI to do their job.
- Lending library, including videos and CDs on protecting patient confidentiality. Ready-made presentations. Privacy and security awareness presentations created by committee members include PowerPoint slides and handouts for use by HRC members. Topics covered include security and awareness, pre- and post-test security awareness games, and a web-based training demo.
- Awareness handouts, including information on computer backups, insider threats, and training the trainer; a collection of HIPAA and security slogans; computer backups, insider threats, and training the trainer; a collection of HIPAA and security slogans; computer backups, insider threats, and training the trainer.
- Training infrastructure for HRC members, which vary greatly in size and type of organization, have very different training needs. Our deliverables are very much controlled by the willingness and ability to volunteer, and by the various employers' willingness to recognize the value we add, not only to our own organizations, but to the community as well. To find common ground as to what to develop to meet HIPAA requirements, we all agreed that what is listed in the regulations is the absolute minimum.

**Conclusions and Lessons Learned**

Because Hawaii’s location makes travel to mainland conferences costly, both in dollars and excess travel time, we have had to find alternate, cost-effective means to educate ourselves. HRC helps accomplish this by sponsoring member attendance at mainland HIPAA conferences, with attendees sharing information and materials with others. Also, through networking at WEDI/SNIP meetings and other conferences, we have developed relationships with experts, some of whom travel to Hawaii to conduct local conferences. As our expertise increases, consulting resources are used more judiciously. By building the infrastructure of knowledge, collaboration, and consensus on technical issues, we reduce individual organization overhead to develop and conduct training and develop and implement policies and technical security. Through HHIC’s website (www.hhic.org), members access a wide array of HIPAA resources and tools. Through the subcommittees, community standards are developed.

Challenges also arise from our diversity. Our intent to make our products scalable so a large hospital or health plan will use the same basic policies as a single physician office or a home care agency, is laudable, but making it happen is difficult. In practice, the needs of large organizations, primarily the hospitals, drive development. Once the basic policies, training, and infrastructure to meet the needs of these organizations are established, work begins to address scalability to physician offices and smaller organizations. Central to our ability to meet the needs of different sizes and types of organizations is the need to understand relative HIPAA risks.

Some organizations impacted by HIPAA have yet to be included in the Collaborative, such as social service agencies, which may have great HIPAA-related needs, but may have small-to-nonexistent support staffs to address them.

The final challenge to HRC is faced by healthcare organizations across the country. The implementation schedule is fragile, and the events of September 11, 2001, and its aftermath may compound this fragility. The challenge is to keep the momentum — to keep pushing to develop and implement the various policies, training, and infrastructure necessary to realize the “goodness” of HIPAA.

On a practical level, the lessons learned include:

“To keep pushing to develop and implement the various policies, training, and infrastructure necessary to realize the ‘goodness’ of HIPAA”
FOCUS: HIPAA

• Establish clear, definitive deliverables and target milestones. Keep accountability high, and keep committee meetings orderly and measurable for effectiveness. Keep striving for buy-in and ownership. Be sure work is equally shared and contributed.
• Start with a steering committee to develop clear objectives and deliverables. Once those are approved, the broader collaborative can seek volunteers. The ideal committee member should have a personal stake in the deliverables, want the experience, and view his/her efforts as giving back to the community.
• The committee chair sets the pace and the tone. Chairs must support members’ effectiveness with clear direction and the opportunity to be prepared, focus on building relationships, and keep communication high, for example with documented status reporting, meeting notes, e-mail, and conference calls.
• Be inclusive — everyone has an equal vote.
• Collaborative work/decisions cannot be all-encompassing for individual healthcare organizations. Each organization must assess its own business and patient care environment, benchmark itself against what others are doing and thinking, and then make implementation decisions specific to the organization they are entrusted to steward.
• There’s no “magic bullet.” Effective policy development is time consuming and requires research and knowledge of micro and macro business environments, including issues and culture. Remember that perfection is not always attainable.
• Hire legal counsel to represent your collaborative/organization’s interest in policy content review and litigation issues.
• Since HIPAA is about standards, it’s best not to stray too far from community standards. Strive for consensus and allow disagreements/issues to be aired in a productive manner.

About the Authors
Marva Chun is director of IT projects & planning at Kapiolani Health Hawaii, Honolulu.

Susan Forbes, DrPH, is president and CEO of Hawaii Health Information Corporation, Honolulu.

Steven Gose, CISSP, is information systems security officer at The Queen’s Medical Center, Honolulu.

Brenda Kumabe, CPA, is project manager at Kapiolani Health Hawaii, Honolulu.

Jeffrey Loo is a principal at J.W. Loo & Associates, Honolulu.

Lorraine Nichols is a coordinator in information services at The Queen’s Medical Center, Honolulu.

Luis Rosa is information security manager at Kapiolani Health Hawaii, Honolulu.

Laura Sherrill is manager of medical records & transcription at The Queen’s Medical Center, Honolulu.

Jim Turner is business relations coordinator for HIPAA at Hawaii Medical Service Association, Honolulu.