



*New Mexico
Coalition for Healthcare Information Leadership Initiatives **

**New Mexico HIPAA Conference, October 22 & 23, 2001
Session Results**

**Session Name: Privacy and Security: Communication and Training for HIPAA
Privacy and Security – Policy and training resources
Session Number: 125**

TOPIC	DISCUSSION	ACTION
1. Welcome	Jim Paulsel, Moderator for Session 125, welcomed the group and requested each attendee complete an evaluation form following the session. Jim then introduced Art Leyland, Senior Manager, Healthcare and Government Services Division, CGI, Inc.	
2. Overview	<p>Art advised he would keep his remarks focused on providers and noted he understood the diversity of the healthcare industry in New Mexico, having worked in the State in the past.</p> <p>He asked the question if the time was right for HIPAA, then answered in the affirmative. Hopefully, work on transactions and codes sets is largely underway. He noted Privacy rule clarifications were recently received from Health and Human Services and are fairly set in stone. He feels the work today will pay off in the end. Art also noted the final rule for Security is unlikely to change much.</p> <p>Art advised compliance with HIPAA Security and Privacy regulations prior to the effective date can be a valuable marketing tool for each organization.</p> <p>He plans to provide an overview for policies, training, cautions and resources for policy and training courses/materials.</p>	
3. Privacy Policies and Materials	<p>Art discussed with the group the need to be concerned with Business Associate contracting and monitoring, consents, notices and authorizations, patient access and amendment rights to medical records, disclosing all you can disclose under the minimum necessary rule and tracking of disclosures.</p> <p>The minimum necessary rule does not apply to treatment, but does apply when protected information is reported outside the organization. He cautioned the group to be very careful with this data. In addition, he recommended the organization keep very specific records of who requested and received the information. He highly recommended a strong tracking mechanism for the data.</p> <p>Art suggested developing strong Business Associate contract language, a Privacy Officer job description and forms, such as notices, consents and authorizations that protect the organization. He noted the Privacy Officer does not have to be a full time position, but one per organization should be named.</p>	
4. Security Policies	Art recommended security measures be implemented for each organization by producing overall written security policies, a	

	<p>disaster recovery and business continuity policy, automatic logoffs, passwords, audit trails on access to protected information, computer room security and Internet encryption and authentication.</p> <p>He reported, if possible, it would be a good idea to track when protected information is viewed, as well as transmitted. Tracking records must be maintained for 6 years.</p>	
5. Privacy & Security Training	<p>The entire workforce must be trained on Privacy and Security polices and procedures. CGI also recommends a cultural change in helping employees understand the importance of complying with HIPAA regulations and the extensive fines that could occur if the organization is out of compliance. Art feels compliance irregularities will be found with the people, not the equipment. He estimates 70% to 80% of the cost of HIPAA Privacy and Security compliance will lie with achieving cultural change.</p> <p>It is important to understand people's concerns about cultural change and address these issues through policies and procedures. Some concerns may include:</p> <ul style="list-style-type: none"> -what is the change? -what does it mean to the employee? -what is the process for compliance? -why is the change important? -how can a violation occur in an employee's area? -how can violations occur in other parts of the organization? 	
6. Preemption	<p>Art cautioned the group that HIPAA regulations can be preempted by State statutes, particularly Privacy, and possibly Security. State laws not preempted include those:</p> <ul style="list-style-type: none"> -determined to be exceptions by the Secretary of Health and Human Services, -allowing or prohibiting disclosures to parents or guardians of minors, -regulating controlling substances, -covering reporting of disease, injury, child abuse, birth and death, conducting public health activities, or requiring health plans to report or allow access to information for auditing purposes or for licensure or certification of individuals or facilities. 	
7. Cautions	<p>He cautioned the group to not believe everything you read or hear, because it is still early on in the process and a lot of misinformation is floating around. Federal clarifications have been helpful and he expects more to emerge.</p> <p>He added do not blindly accept model forms or policies, even from reputable sources, because some consents and authorizations do not meet the requirements. He recommended an in-house legal review.</p> <p>Art recommended do not misunderstand Privacy and Security training requirements. They relate to the overall regulations, not necessarily the details and apply to the employee, volunteer and trainee workforce.</p>	

	<p>The Security Rule is not yet final, but Art advised not to wait for the final ruling to begin work. Since Security and Privacy are very closely linked, it is likely there will be little change to the preliminary Security Rule and much of the language will overlap.</p> <p>Since most organizations already have Security and Privacy forms, and policies and procedures already in place, they should not assume they are starting from scratch. The key is to perform a gap analysis.</p>	
8. Resources	<p>Art referred the group to three kinds of resources for information:</p> <ol style="list-style-type: none"> 1. Conferences 2. Consultants 3. Websites <p>He then pointed the group to various websites and conferences currently available. He noted local websites would be a good reference for preemption information.</p> <p>Art recommended the group become active in the NM CHILI organization where HIPAA information is shared. He pointed the group to the Privacy/Legal Workgroup, which is working on a model Consent Form and Privacy Notice, currently under legal review before posting on the Website. He also noted this group is developing a Business Associate Agreement, working on clarification for the minimum necessary provisions as they apply to health plan requests, and developing a gap analysis tool. In addition, other workgroups through NM CHILI include a Preemption Analysis Workgroup, Awareness, Education and Training Workgroup, a Security Workgroup.</p> <p>Art then pointed to various websites and discussed their mission and focus. He tipped the audience off to the Google search engine and using links through websites as much as possible.</p>	
9. Summary	<p>Art summarized the session with the following points:</p> <ul style="list-style-type: none"> -resources are slowly becoming available. -websites are the best resource right now. -local resources can be most helpful. -don't forget the need for cultural change. -review everything you get. -you still have work to do. 	
10. Questions and Answers	<p>Q – What are the training requirements and are they for all employees? A – The overview of the HIPAA is required for all, but tailor the training to each area. A painter does not need as much training as a nurse in the emergency room.</p> <p>Q – What level of detail is required in the Notice of Privacy? A – Anyone who has direct contact. In general, train on the basics of why and when.</p> <p>Q – Monitoring too? A – Make some attempt to monitor Business Associates with protected health information. Take action if you become aware a</p>	

Business Associate is in violation of the regulation.

Q – What about breach of contract?

A –The Plan or Provider will be held liable, not the Business Associate. However, a breach of contract between the Plan/Provider and the Business Associate means the Plan/Provider could sue the Business Associate to the extent outlined in the Business Associate agreement.

Q – Who are Business Associates?

A – Organizations that you potentially provide protected information, including but not limited to an outside firm, organization or individual. The Plan/Provider must enter into a legal agreement with each of these entities.

Q – Is there a Chain of Trust agreement required between the State and a Hospital? For example, the Child Welfare Division requests specific hospital records.

A – State law preempts Federal law in this case and no agreement is needed.

Q – Are Business Associate agreements costly to the business?

A – Yes. It is expected the Business Associates agreement will pass on their costs to the Plan/Provider through the cost of their services.

Q – How are college or nursing students categorized for training?

A – They are considered the organization's trainees and have to be trained on HIPAA basics.

Q – How are call groups affected?

A – Create a consent form that outlines the arrangement and get all to sign so information can be exchanged.

Q – How does an organization create audit trails and user response time? What is the disk space requirements? Please discuss resources from their technical aspects.

A – This is not Art's area of expertise and recommended they seek out another source of information.

Q – What tips can be offered to distinguish between Privacy and Security?

A – Both groups meet together. Chain of Trust agreements apply to Security, but Business Associate agreements are discussed in Privacy. Some issues considered separate but collaborative.

Q – What if public agencies wish to jointly combine medical records, e.g. family planning?

A – Art recommends writing a very specific consent form.

Q – Where does Need to Know fit in?

A – The minimum necessary rule does not apply to treatment, but some allowances are made for affiliated entities. Chain hospitals

don't have to get multiple consents. Another example may be a radiology group who provides indirect treatment. A patient will sign a consent when admitted to the hospital that covers the radiology treatment and the hospital at the same time.

Q –How far does tracking have to go outside the organization?

A – HIPAA covers all protected health information no matter what form it comes in, i.e. verbal, written, electronic. This information must be protected and has a wide scope.

Q – What is the enforcement date of the Business Associates Agreement?

A – April, 2003.

Q – What consents are required to comply with law enforcement requests for information?

A – Preferably, when an individual presents for treatment, a separate consent/authorization form is signed or verbal authorization is given. There are circumstances where the Individual is incapacitated. There is a lengthy list of permissible information that can be provided to law enforcement. Art is not sure if immunizations are included.