"Security for healthcare will need to be a continual activity, not just virus detection and not just a firewall. It's a complete formula between processes, people, and your network."

Just as successful healthcare entities need to have clear policies for governing their financial resources and their patients care, your organization also needs clearly defined policies for managing your network infrastructure and traffic. Your policy needs to deliver the scalability, ease of use, manageability, security, and control that you need to help maintain network efficiency, reliability, and performance in addition to meeting all HIPAA requirements.

"Determining your organization's HIPAA readiness and determining appropriate security measures to implement will be based upon your organization's current policy and procedures."

Your network security requirements should embrace both the computer systems used to maintain secure electronic medical records and the administration of those systems.

Your organization might seek to protect personal patient information, but without an effective policy for security and privacy, procedures, services and mechanisms, you cannot guarantee confidentiality and the right cost control apparatus.

Define

Your approach to HIPAA security compliance should follow a "life-cycle" approach. A Gap Analysis should be prepared to determine where your organization needs changes to become compliant. Be realistic and brutally factual with this phase; have it checked and re-checked. A factual Gap Analysis will not only give you accuracy on your current HIPAA readiness status, it will also save you time, resources, litigations and unnecessary financial burden.

Risk Analysis follows Gap Analysis. No matter how well your system is designed, there will be vulnerabilities. The main goal of this phase for your organization is to select cost-effective safeguards. You should calculate the risks against assigned monetary values and identify the threats and the likelihood of each threat. This is vital to a sound and practical security policy for your organization.

Design

"People make security." To achieve a sound and effective cost control initiative for your HIPAA security which includes: Administrative Procedures, Physical Safeguards, Technical Security Services, and Technical Security Mechanisms, a policy should be built and established on your business processes and internal focus on access controls and audit trails.

Your policy should be using technology to support your business posture, not personnel supporting your technology. This policy is a set

of laws, rules, and day-to-day practices that regulate how your organization will manage and protect PHI. This is also to be incorporated with a sanctions policy to enforce any breach of your security or policy. The policy should be clear, concise and without any ambiguous statements.

Deploy

Regardless of the size or practice the following are considerations during the deployment phase:

1. Integrate. Don't replace.
2. Comply with all regulatory and accreditation standards.
3. Contain costs.
4. Consider scalability.
5. Be consistent with your organizational business posture.
6. Best-of-Breed usage.
7. Encourage social engineering.

Inside the issues of HIPAA, there will be ways to budget for the investment into your HIPAA security implementation resolutions. Investments into HIPAA security implementations must be measured alongside fiscal responsibility of other important but unrelated strategic initiatives. The "best" HIPAA deployment will depend on how well your entity can parallel HIPAA requirements with other business objectives including your e-Health and Commerce.

COMMON$_d$ Expert Services will guide and support your entity to accomplish a successful HIPPA security process in addition to insure your alignment of HIPAA initiatives with your core strategic business values to help control costs.

Manage

With HIPAA, a covered entity must maintain information. Any method of communication, access point, or audit trail in reference to HIPAA and PHI must be maintained and modified in a prompt manner. The covered entities must retain any required documentation and transactions for at least 6 years. You must have a proactive and constant monitoring method for managing this process. Planning is essential to the management of your network and HIPAA compliancy. This will reduce and control costs, improve efficiency, and protect the privacy of patients. The industry estimates that full implementation and compliancy can save up to $9 billion per year from overhead without reducing the amount or quality of healthcare services.