STATEMENT
of the
The Forum on Privacy and Security in Healthcare
to the
National Committee on Vital and Health Statistics

Presented by:
Lisa Gallagher
Member of the Board and
Senior Director, Exodus Security Services

Regarding:
Early Implementation of the HIPAA Administrative Simplification standards
And specifically,
Industry Solutions: Leveraging Available Technologies, Standards, and Expertise

Good Morning. My name is Lisa Gallagher. I am a Senior Director in the Security Practice at Exodus Communications. I am here representing the Forum on Privacy & Security in Healthcare. We appreciate your invitation for a representative of the Forum to address your committee regarding industry solutions for implementation of Administrative Simplification.

It is a pleasure to be here in the company of these other panelists whose experience and specific knowledge shall certainly bring illumination to issues surrounding healthcare security and privacy.

State of the Industry

Why is healthcare not just another major application of information technology concepts*?* After all, other huge organizations, even whole industries, have successfully standardized security requirements over very large integrated information systems.

Healthcare is a unique environment with a variety of types of data, hierarchical requirements, a diverse set of stakeholders with unique needs, and a culture that prizes individualism. Implementation could not and did not wait for a system of standards to be produced by under-resourced standards development organizations. Within this hugely complex environment, the development and implementation of standards has lagged far behind the actual implementation of systems.

The issues were under-appreciated for years because healthcare was generally delivered at the community level – whatever the size of the community - and, until recently, there was not a compelling argument for healthcare information systems that extended beyond the community. Organization's resources were limited and the communications infrastructure would not support simple, cost-effective movement of large

amounts of data. Thus, system developers were comfortable, or rather not-too-uncomfortable, with non-standard approaches, local structures, local systems, even local languages and homegrown ideas of what their security processes should be.

In response to this situation, literally hundreds of developers sprung up to provide their customers with custom computer systems. Each medical specialty within a medical center might expect individual interfaces, languages, and even have distinct usage of common words. It is not uncommon for a single medical organization to have a variety of clinical and administrative systems that might run on the same network, but are not able to exchange data. Standards development activities just couldn't keep up with the profusion of development activities and the rapidly changing environment.

What has changed to prompt the need for information technology standards?

In the last several years, the organizational structure of healthcare changed drastically – new, larger organizations formed and old boundaries disappeared. For example, in New York City Mt. Sinai Hospital merged with NYU. These are two large organizations with radically different security architectures, now trying to have similar, coherent policies, along with a single mechanism to enforce or change the policies.

The current situation is difficult enough considering the issues surrounding healthcare technology and medical vocabulary, but almost insurmountable in the areas of privacy and confidentiality, where individual circumstances mold people's beliefs and even their specific idea of meaning of their words. Patients, security experts, and privacy advocates have all expressed concerns about the implications of the electronic exchange of patient health data. The passage of the HIPAA regulation and the upcoming proposed rules will go a long way to defining the needed goals and requirements, but there are still gaps in the definitions and level of understanding that we all need to have.

These gaps are caused by the lack of an industry-accepted vocabulary for requirements expression and a lack of industry-wide acceptance of values. The difficulty of finding explicit vocabulary to express our security and privacy requirements and the enormous variety of information environments has left security professionals with a daunting task. They must buy equipment, integrate systems, and implement secure environments without a clear statement of what goals need to be achieved.

What are the compliance issues? Currently, many healthcare providers are considering the implications of implementing architecture, policy, and procedure changes in order to establish compliance with the HIPAA security requirements. Chief among those concerns is how to establish and maintain such compliance in a manner meaningful to their patients, business partners, and the public.

There are too many interdependent factors for the goal of compliance to be achieved by any one segment of the community in isolation. Stakeholders need a compliance mechanism that can satisfy all of their different but related requirements:

- Policy makers must have a way to state their security needs and concerns in a way that can be clearly understood and implemented.
- Product vendors and system integrators need guidance to help them translate policy into compliant technology, as well as a way to demonstrate that they have done so.
- Those responsible for evaluating products and systems to confirm compliance need standards against which to evaluate, as well as mechanisms for doing so.

What is the Forum?

The Forum on Privacy & Security in Healthcare was created to address compliance issues in the healthcare industry by providing a venue and a mechanism for the exchange of ideas, technology, and expertise. The Forum is working on developing compliance blueprints for developers, healthcare organizations, and the accrediting organizations. The Forum is currently involved in the development of standardized "security profiles" to specify and measure the security aspects of IT products and systems.

The Forum's mission is to:

- encourage the healthcare industry to develop more efficient methods of providing a secure environment for their commerce,
- promote the use of the Common Criteria (ISO 15408) to aid in regulatory compliance,
- educate the industry about the worth of these standardized technology blueprints, and
- catalyze the industry.

To accomplish these ends, an active Forum has been created with a wide base of membership that will continue to provide structure for the many efforts to develop and articulate healthcare policy. The Forum actively seeks involvement and commitment from providers, academia, industry, and Government.

Vendors, hospitals, clinics accrediting organizations are now struggling to develop strategies to implement policies pertaining to security and to develop methods to assure compliance with security policies. The Forum participants believe that it is crucial that healthcare find coherent, efficient ways to express security requirements. It is equally important to measure the compliance of hardware and software applications to stated security requirements and policies. Healthcare organizations must have confidence that the security features of IT products and systems they build, buy, or use are implemented correctly and completely and that they behave as required.

What is the Common Criteria?

One way to establish such confidence is use of the Common Criteria (CC) for IT Security Evaluation (ISO 15048). The CC is the new, internationally recognized standard for specifying and evaluating the security features of computer products and systems. This standard facilitates a common, organized way to clearly and unambiguously articulate users' security needs as well as vendors' security solutions for addressing the stipulated security dilemma.

For the healthcare community, the CC can:

- provide a means to translate security policy into functional security specifications for products and systems and to select the desired level of assurance (defined as confidence in the correct operation of a product);
- allow prospective consumers or developers to create standardized sets of security requirements that meet their needs in the form of "protection profiles", that can then guide vendors and integrators in their efforts to produce compliant products and systems; and
- provide an evaluation method, supported by the availability of commercial evaluation laboratories, that offers a consistent, independent, cost-effective way to help confirm compliance.

Common-Criteria-based specifications can be written to reflect all security aspects mandated by policies, regulations and law. They also articulate the desired level of assurance in correct and complete security that is to be demonstrated by implementations claiming compliance to the specifications.

These kinds of specifications facilitate use of associated, standard evaluation methods (in this case, the Common Evaluation Methodology (CEM)), by independent, commercial security testing and evaluation laboratories that have been accredited by the Government. Such labs evaluate products and establish confidence that products are compliant with security specifications, policies, regulations and laws. Government validation of laboratory IT security evaluations allow healthcare professionals to confidently, reliably and consistently compare the security features of evaluated healthcare IT products and systems.

The Forum activity is based on the use of the Common Criteria and the creation of standardized security protection profiles. These criteria can be also used to specify and measure the level of confidence (or assurance) that security implementations function as claimed. These criteria thus help measure IT equipment compliance claims with community-recognized security policies and requirements.

The Forum is promoting community-wide use of the Common Criteria concepts. The Forum is working to have the Common Criteria technology and methodology recognized by accrediting

organizations, insurers and others as providing valid evidence, assurance, and due-diligence that security-enhanced IT products provide solutions compliant with stipulated requirements, policies, regulations and laws.

Who is Exodus Communications?

Exodus is the leading provider of Internet Data Center services to the increasing number of companies whose Internet sites are integral to their business operations. Along with Internet server hosting, Exodus also offers professional consulting services, to include security engineering consulting services. Recently, Exodus has seen a surge in the number of clients seeking initial HIPAA compliance planning and security evaluation services.

Exodus Security Services, part of Exodus Communications, joined the Forum last year because after participating in a research contract with National Institutes of Standards and Technology's (NIST) National Information Assurance Partnership (NIAP), to determine whether CC concepts were leveragable for use in addressing the healthcare security requirements compliance issue. This research convinced us that the CC approach is viable and worth investigating further. Our participation in the Forum thus far has centered on briefing, discussing, and educating the healthcare community's Forum participants about the usefulness of the CC technology. Our own work with helping healthcare providers using this approach is well underway.

Where are we now?

Currently, the healthcare industry is so huge and so fragmented, that individual providers have difficulty seeing the benefits of implementing the HIPAA requirements, or the benefits of helping anyone else implement the requirements. And, even when they are preparing to take action, the path to compliance, certification and due diligence is unclear, at best.

Industry providers of security services are currently attempting to bring to bear their expertise and technologies to help the healthcare industry prepare to establish and maintain compliance. Organizations such as the Forum can be conduits for such collaboration, which is a primary reason for the participation of Exodus Security Services. Our desire is to provide our services in the context of a well-established process for guiding healthcare providers towards full and ongoing compliance.

The Forum has advocated the use of the CC as one approach to the specification, evaluation, and certification of healthcare solutions. This approach benefits not only healthcare providers and the public, but also product and system vendors, because it provides a means to clearly articulate the security requirements and standards that apply to healthcare systems and products, and provides an objective method for assessing how well their products or systems comply with those requirements.

The Forum also believes that the entire healthcare community would benefit from standardized system evaluations and compliance certifications, perhaps from third party security evaluation facilities. This could enable healthcare IT purchasers to buy those products that have successfully achieved the security equivalent of a "Good Housekeeping Seal of Approval", and also allow those same organizations to pursue a recognized third party HIPAA compliance certification.

What role should the Federal Government play?

There is an incredibly complex set of issues, and there can be no simple set of solutions. There are, however, potentially enormous benefits if tangible solutions can be realized. All of the healthcare informatics industry and healthcare in general would benefit enormously from clear direction, and use of established processes and stable, complete standards.

The Federal Government, as both the largest potential beneficiary and the most influential single entity, can become the instigator and motivator for Government and industry partnerships to make progress. We would like to encourage the Government, in particular HHS, to proactively participate in efforts such as the Forum. In this way, the Government can serve as a facilitator, to encourage industry to move towards a commonly understood set of processes, and vet those organizations that have demonstrated the ability to do evaluations and certifications against the standards.

Conclusion

I, along with the Forum members, appreciate the opportunity to comment on work of industry to ensure that health care will be able to reap the benefits of information technology while preserving the confidentiality and data integrity that the American people expect. The Federal Government, just as it motivates and sponsors public health efforts, can help by active participation in Government/ industry partnerships to facilitate progress in this area.

Sig-

Lisa Gallagher
Exodus Communications, Inc.