GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Matt Kramer
9/16/2003 4:25 PM
GIAC (GSEC) Practical Assignment
Version 1.4b Option 1

Practical Guide to the HIPAA Security Rule

Abstract
What is HIPAA? The Health Insurance Portability and Accountability Act (HIPAA) was introduced in1996 with specific rules regarding privacy of patient information, security of patient information, and standards for transaction and code sets. Through the Privacy Rule and the recently released Security Rule, Congress is giving the healthcare industry a mandate to implement standard best practices for securing critical healthcare information also known as protected health information. This paper focuses on the recently published final Security Rule. What is the Security Rule? What is required? What are some of the activities that enable organizational compliance, but in a cost-effective way? I intend to answer all these questions within this document.

The HIPAA rules apply to healthcare organizations known as “covered entities”. Covered entities are defined as any healthcare provider, healthcare clearinghouse, or health plan. The rules are specific to how covered entitles use “protected health information”. PHI, as referred to throughout this document, is defined in the Privacy Rule as “individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium”. [1] Although HIPAA, at a high level, covers PHI in all forms, the Security Rule applies to PHI only in electronic form. The most important thing to remember when reviewing the HIPAA Security Rule is that while the security rule is specific to practices concerning the security of electronic PHI, or e-PHI, this is NOT a technical project for the technology department. The HIPAA Security Rule addresses key administrative and clinical processes that need to be addressed through policies and procedures to provide for secure health information. Technology will assist in implementing the procedures defined by a covered entities’ HIPAA Security Plan. The goal of getting healthcare organizations to comply with these standards and something that healthcare organizations should see as a beaconing light is to have covered entities realize that they are not just trying to secure data or comply with a federal mandate, but they will be in essences improving their core business processes while adhering with improved levels of security. The standards laid out here are best practices regarding security and will help an organization mitigate and recover from any type of business security event.

1. HIPAA Privacy Rule and Its Impact on Research

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The HIPAA Security Rule can be easily broken down into 3 major sections; Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Each section describes both "Required" compliance standards and "Addressable" compliance standards. All covered entities must comply with the required standards at some level. They must, at a minimum, define, document and implement policies and procedures that attempt to comply with the required standards. In respect to the addressable standards, every covered entity must assess the standard to determine if it is reasonable and appropriate in its particular environment and then take one of two courses of actions. The covered entity may implement policies and procedures to comply with the standard if it is reasonable and appropriate or the covered entity may document why it would not be reasonable and appropriate to implement the standard and then implement an equivalent alternative measure reasonable and appropriate to that environment.

Administrative Safeguards

Section 164.308(A) describes the steps healthcare organizations can take administratively to comply with the HIPAA Security Rule. This section includes required standards for security management processes, managing information access, incident response, contingency planning, and evaluation. Also included in this section are addressable standards for employee management and promoting security awareness.

Security Management

The most important aspects to the security standards are an organization's security management processes. These processes will dictate how well your organization is prepared to comply with the standards and if done right will allow your organization to comply at a minimal cost.

First, to adequately secure you electronic patient information, it is essential that a complete risk analysis be done. A well thought out risk analysis will provide a good foundation on which to build the rest of your security plan. A clearly defined risk analysis will first identify the risks. This is usually done with the help of a business continuity matrix. In the healthcare environment there are 3 critical objectives:

- Patient access
- Quality of care outcome
- Reimbursement of services

A business continuity matrix is a list of the business processes that are required to support the 3 critical objectives above which will keep the business up and running in the event of a disaster or security event. Once the critical business processes are identified, risks can be associated with each process. For example, to allow patients to be seen, covered entity "A" developed an online patient scheduling application for patient self-service. A risk for this type of process would be it's online nature and accessibility to the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The next step in the risk analyses is to identify the risk factor. To do this you will need to identify the threats and vulnerabilities to the identified risks. Threats and vulnerabilities come in many forms such as technical, operational, social, and natural. Make sure you cover every form. The risk factor then, is a product of threat vs. vulnerability essentially meaning that "the level of risk in your organization increases with the level of threat and vulnerability"[2]. Going back to our example, we know the online application runs on IIS. Therefore, this risk would have a high threat level because of the prevalence of website hacking and a high vulnerability due to the nature IIS thus producing a high risk. This is demonstrated in the following diagram.

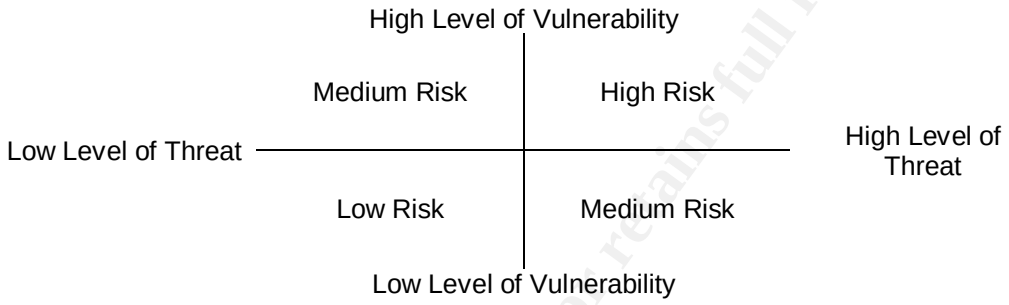

Figure 1. Threat vs. Vulnerability Chart [3]

After the risk analysis is done determine what will it take to reduce the risk factor of all medium to high risks to as close to zero as possible given budget requirements. This process is known as risk management. Managing your risk correctly is critical to cost effectively achieving the requirements of the HIPAA Security Rule. There are lots of ways to reduce risks. Some are more expensive than others. Highly expensive technical solutions are great to have and may succeed in mitigating the risks, but depending on your organization, they might be overkill. It boils down to knowing your organization. In our example, covered entity "A" is a small to medium size healthcare provider with a moderate patient base. An easy solution would be to remove and/or modify all the default settings of IIS and implement a high level of logging for auditing and alerting purposes because the low amount of traffic on the site will be easy to monitor. An organization can do this with a little research and the right tools, most of which come with IIS, and without spending a lot of money.

Other security management standards that are required to comply with the security rule are sanction policies, information system access review, contractual agreements, and documentation

2 - 3. Microsoft Security Operations Guide to Windows 2000 Server p.12-13

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sanction policies must define what actions will occur when an employee of the healthcare organization fails to comply with the policies and procedures defined by the organization. Effective policies are only those policies that get enforced regularly and are used to educate the workforce.

Information system access review standard requires organizations to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incidence tracking reports [2]. Depending on the complexity of the covered entity, a full time security log auditor may be required to review all information system access logs on a regular basis. In some cases it will also be beneficial to offload log monitoring to separate business owners of systems producing logs. Most times these business owners will better know which events are of concern.

Contractual Agreements

Most, if not all, healthcare organizations have business associations with other organization in which they share e-PHI either for the treatment of the patient or payment of service to the patient. The HIPAA Security Rule states that every covered entity is required to sign contractual agreements recognizing that the business associate will abide by the following terms:

- Administrative, physical, and technical safeguards will be implemented to ensure the security of e-PHI that it creates, receives, maintains, or transmits on behalf of the covered entity.
- Assurances that any hired agent, which comes in contact with e-PHI, will take necessary and appropriate actions to secure that e-PHI.
- Any security incidents involving the business associate must be reported to the covered entity.
- The contract may be terminated at any time if the covered entity discovers that any part of the contract has been dishonored unless specific laws force contractual negligence.

Group health plans must amend plan documents to include assurance that the plan sponsor is responsible for safeguarding all e-PHI related to the plan. The amended documents must include the same provisions that the above business associate contracts include as well as a provision stating that the plan sponsor will adequately separate e-PHI received from the group health plan and other organizational information using necessary and appropriate security practices.

Documentation

The security rule states that it's not enough to define the policies, you must maintain written documentation of the policies and procedures defined to comply with the security regulation. Any action on those policies and procedures including assessments must also be documented. All documentation must be maintained for a period of six years from the latest date the policy or procedure was in effect. All documentation must be available to any individual that will be

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

held responsible for following the policies and procedures defined. As updates to policies and procedures become necessary, the documentation should also be reviewed on a periodic basis to assure that new policies and procedures are not missing from the documentation.

Assign Security Officer

Healthcare organizations are required assign a security official. This employee would be responsible for performing the risk analysis and the definition and implementation of necessary policies and procedures to manage those risks. Because of the complexity and volume of work to comply, for most organizations, hiring a full time employee for this position will be more cost effective than having a current employee split time with current duties. This security office should be someone at and executive level who understands the core business processes. It would also be beneficial to most organizations that this person be somewhat technical in nature so they understand the technical aspects of securing electronic information.

Security Incident Procedures

Healthcare organizations will be required to have policies and procedures in place that give them the ability to identify and respond to security incidents. Polices and procedures are required for how known or suspected security breaches are identified, analyzed and dealt with. Also, there must be policies and procedures on how security events are documented. The following list of questions should be answered in any security event documentation:

What is the security breach?
How did the security breach happen?
What information is affected?
What are the steps to mitigate the security breach?
What are the steps to recover from the security breach?
What are the steps that can prevent the security breach from re-occurring?
What is the cost of the security breach?
What is the cost of prevention?
Was this type of breach acceptable?

Answering these questions will provide you with better information, which leads to better decisions regarding the cost involved to prevent a similar breach in the future.

Contingency Plan

For e-PHI to be secure, it must be remain confidential, integrity must be kept, and the information must be available. In the event of a major system failure or natural disaster, healthcare organizations are required to have polices and procedures in place that define an electronic information contingency plan. This plan must include electronic data backup plans. Data backup plans will grow in complexity paralleled to the organization, but the “plans should be formatted to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

provide quick and clear direction in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations".[4] The purpose of the plan is to be able to recover electronic patient information at any time, at any place. For smaller organizations backing up e-PHI to CD's is perfectly acceptable, provided the CD's are stored in a safe and secure place and the data can be retrieved at a later time. This introduces the need for a recovery plan. Policies and procedures need to be defined on how the backed-up e-PHI will be recovered. The policies and procedures must also define how this plan is tested and revised accordingly. A contingency plan must also define how the security of e-PHI will be maintained operating in contingency mode. Separate policies and procedures may need to be written specific to dealing with certain extreme circumstances.

Evaluation
Every covered entity is required to evaluate both technical and non-technical security polices on a regular basis and adjust them based on technical or operational changes to the environment. Covered entitles should not try to evaluate themselves. Doing so will lead to oversights and excuses. An extremely cost-effective way of evaluation is to enlist the help of a peer organization or business associate to review your security policies. This is beneficial to both parties because it will be an unbiased opinion and an opportunity for the evaluator to possibly take something from the experience that they were unaware of.

In addition to the required standards mentioned above there are two addressable standards regarding workforce security, and security awareness training.

Workforce Security
Each healthcare organization should address the procedures for authorizing and supervising employees that use or may come in contact with e-PHI. That employee's supervisor and the requested data's business owner prior to access being granted should first authorize each employee that requires access to e-PHI. In some cases training should also be a requirement for access. Procedures to determine if requested access to e-PHI is necessary and appropriate must be addressed. This is easily accomplished, but sometimes hard to define, through role-based access. Covered entities must also address procedures for terminating an employee's access to e-PHI. The HR department's communication with the account administrator is critical in the termination process to make sure accounts are deactivated in a timely manner.

4. NIST Publication 800-34 p. 31

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security Awareness Training

All covered entities are required at some level to address the needs for security awareness to its employees. At a minimum, employees should be made aware of the importance of security in terms that they understand. Using examples of downtime or monetary penalties raises the level of importance to non-technical people. Employees should understand the need for basic security procedures, such as login monitoring, and password management. Most end users want things to work fast and easy. To add security to processes, usually makes the process slow and/or hard. Educating a user that he/she will be responsible for any inappropriate use of e-PHI under his/her user account, regardless of actually performing the act, usually convinces them not to share the passwords. Users can be a security team's best ally when educated correctly.

Physical Safeguards

The HIPAA Security rule defines required and addressable standards regarding physical security as it relates to the need for the confidentiality and availability of e-PHI. Required standards include workstation use and security as well as disposal and re-use of media containing e-PHI.

Workstation Use and Security

The security rule requires covered entities to implement policies and procedures that define how workstations that access e-PHI are used. These standards should define the functions that are preformed to secure a workstation from unauthorized access to e-PHI including the physical surroundings of the workstations. Examples of this may be facing monitors away from public or high traffic areas or "locking" workstations when left unattended. The workstation security standard requires covered entities implement policies and procedures to restrict access to workstations with access to e-PHI to authorized users only. Use of usernames and passwords should be implemented at a minimum level. The National Institute for Standards and Technology (NIST) provide very good guidelines for securing workstations at http://www.nist.gov.

Media Disposal and Re-Use

Each healthcare organization must define and implement polices and procedures for disposing of e-PHI and the device or media that stored e-PHI. Deleting data from a drive is not enough to adequately dispose of e-PHI. There are relatively cheap tools to completely erase data from hard drive media according to DoD standards. All other types of media should be physically destroyed when the media is no longer in use. Pay close attention to hard drive vendor contracts regarding replacement of damaged media. To protect against un-authorized disclosure of information, most vendors now support the destruction of drive platters before returning the damaged drive.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In addition to required physical security standards, covered entities must address suggested physical security standards including facility access controls and other media controls.

Facility Access Controls

Covered entities should address standards relating to facility access controls. A facility security plan should be implemented to safeguard the facility and equipment related to the transmission or storage of e-PHI from un-authorized access, damage, or theft. Included in this plan should be provisions for access control including validation of the access requested based on the duties assigned to an individual requesting access. This standard is geared toward establishing "key" management policies and procedures. Distribution of keys, cards or tokens that provide access to physical systems that access e-PHI must be carefully managed. Comprehensive inventory of keys, cards, and tokens must be kept to know who has the access and logs should be kept at each location to account for when each key, card, or token was used. Maintenance records should be well documented for all repairs or modifications to any security component of the facility or its information systems. Contingency operations must be addressed. In the event of a disaster, access to the facility must be allowed for the restoration of e-PHI according to the organization's contingency plans.

Media Controls

Covered entities must address the need to account for all movement of hardware and media that stores e-PHI, along with any individual responsible for the movement of that hardware. Also covered entities must address the need to create a recoverable copy of e-PHI before the movement of hardware or other electronic media that stores that e-PHI. This standard supports the data backup plan defined under the Administrative Safeguards section.

Technical Safeguards

This section of the HIPAA Security Rule defines both required and addressable standards. In my opinion, all of the standards defined in this section should be required. If these most basic technical security best practices are not followed, the e-PHI of a covered entity will not be secure. This section is potentially the most costly section of the security rule due to the cost associate with technical solutions, whether it is financial or operational. Again, depending on the organization, complying with these rules may require more expensive technical solutions. However, if the risks are completely analyzed, that cost should be kept to a minimum.

Access Control

Access to e-PHI must follow standards to provide the confidentiality, integrity, and availability as prescribed by the HIPAA Security Rule. All users of e-PHI must have unique identification and policies and procedures must be in place to assign and maintain this identification. Covered entities should follow industry

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

best practices on assigning usernames to all employees and agents of the organization as well as assigning special accounts for automated process. These processes should never be run under a generic administrative level account. Policies and procedures must be established to provide for emergency access to information. These polices may contradict other "normal circumstance" policies, but are necessary to access e-PHI in an emergency when there is no time to follow the normal policies. This policy should allow for the quick action of a system administrator, but only after proper written (emails are ok) authorization by a senior management official. The policy should also define what constitutes an emergency. Systems that access e-PHI should automatically logoff after certain period of idle time. This may vary on the location of the system, but a good idle timeout is 5-10 minutes. While the security rule does not require encryption, due current technologies embracing encryption, e-PHI should be encrypted at any point in transit and should be encrypted while in storage. With the advent of online applications and SSL encrypting data in transit can be done relatively easy. Most organizations require VPN's for remote access and some variety of file encryption software if e-PHI must be transferred via FTP, or email. Encryption is built into most operating systems now where it is easy and cheap enough to do at a minimal level.

Audit Controls

Every covered entity must implement processes to record activity with e-PHI. Periodic reviews of these records must occur to look for un-authorized access or disclosure of the information. Log management will be critical to being able to identify security breaches. "Failure to enable the necessary data collection mechanisms will greatly weaken or eliminate your ability to detect suspicious behavior and intrusion attempts and to determine whether or not they were successful." [5]

Integrity

The integrity of e-PHI must be maintained with the use of strict procedures for approving permissions for modification or deletion of e-PHI is necessary and appropriate. These procedures will take shape in the form of strict role based access permission levels that clearly define what roles need the ability to change or delete e-PHI according to their organizational duties.

User Authentication

Each employee, agent, or business associate that accesses e-PHI must be authenticated as the person they claim to be before access is granted. This can be strongly enforced with strict password policies at very little cost. The password policy should require users to have passwords of at least 8 characters (14 if using Windows NT LM hashing) including letters and numbers. All passwords should expire in no more than 90 days. Passwords should never be shared and there should be heavy penalties if it becomes known that a user shared their password. Digital signatures can also be used to verify the identity

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

of a user. Digital signature architectures can be complex to setup and maintain, but add great security value to your electronic transmission processes.

Transmission Security

Transactional systems that transmit e-PHI must have procedures in place to verify the integrity of the data that is in transit has not been compromised. The use of checksums and possibly the use of digital signatures are important in verifying data integrity is maintained during transit. Encryption must be used whenever e-PHI is transmitted through un-trusted systems to ensure the confidentiality of the data in transit. An example of un-trusted systems might be systems on the Internet communicated with via HTTP or email.

Conclusion

The HIPAA Security Rule, which was finalized in February of 2003 (effective April 21, 2005), will have a significant impact on healthcare organizations in America. There are administrative safeguards, physical safeguards, and technical safeguards which covered entities must address, if not be required to follow, that were defined by The Department of Health and Human Services (D.H.H.S.) as necessary and appropriate to adequately secure protected health information in electronic form. For some organizations complying with these standards may be a costly endeavor. By following the security rule's guidelines and thoroughly studying the business' critical processes and how those processes are affected by the proposed standards, organizations can implement a strong security plan that fulfills the requirements of HIPAA at a minimal cost.

---

5. The Cert Guide to Systems and Network Security Practices p. 216

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES

Matthew J. Flanary. "HIPPA Security Standards Checklist". Davis & Kuelthau, s.c. URL: http://www.dkattorneys.com/pdf/HIPAAsecuritychecklist.pdf (February 2003)

"What Health Information Is Protected by the Privacy Rule". HIPAA Privacy Rule and Its Impact on Research. The Department of Health and Human Services. URL: **http://privacyruleandresearch.nih.gov/pr_07.asp** (August 2003)

"Security Operations Guide for Windows 2000 Server". Microsoft Corporation. March 2002. 9-13

"Contingency Planning Guide for Information Technology Systems". National Institute for Standards and Technology (NIST). June 2002 URL: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf (July 2003)

Allen, Julia H. "The CERT Guide to System and Network Security Practices". Addison Wesley. May 2001 p 216

Tim Ferrell. "Impact of HIPAA Security Rules on Healthcare Organizations". October 2001 URL: http://www.sans.org/rr/paper.php?id=495 (July 2003)

"HIPAA Security Final Rule". WEDI SNIP. February 2003. URL: http://www.wedi.org/snip/public/articles/HIPAA_Security_Final_Rule_official_version.pdf (May 2003)

Deborah S. Birnbach and Mayeti Gametchu. "How HIPAA's Security Rule could effect IT". April 2003 URL: http://www.computerworld.com/securitytopics/security/story/0,10801,80816,00.html (August 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS