leviathan
security group

3223 3rd Ave S., Suite 100
Seattle, WA 98134

Before the National Institute of Standards and Technology.

July 7, 2020
Leviathan Security Group submits these comments in response to the National Institute of Standards and Technology's request for public comment on version 2 of the NIST Special Publication (SP) 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as announced on April 29, 2021.

Background

Leviathan Security Group ("Leviathan") is a Security Consulting firm based in Seattle, WA with two specialty areas, Risk & Advisory Services, and Testing Services. Our teams regularly conduct activities with HIPAA Covered Entities and Business Associates of various sizes, across a range of industries. The Risk & Advisory team regularly performs Risk Assessment services and measures the efficacy of organizations' compliance with the Security Rule. Similarly, the Testing Services team has conducted numerous penetration tests on applications and systems of such organizations. Our customers range from large hospital and clinic systems to small technology service providers to medical equipment manufacturers.

Our comments include general commentary on Revision 2 of SP 800-66 overall, and specific feedback on many of the Security Rule subsections in Section 4 of SP 800-66. As some of our methodology in assessing implementations is proprietary in nature, our comments apply to the content of the guidance and our experience in evaluating how our customers have used this and other guidance, with a focus on improving the guidance and ease of implementation.

In our experience evaluating clients' implementation of the HIPAA Security Rule and performing risk assessments, common problem areas are:

- **Risk Assessment and Risk Management**
  Smaller clients often have limited skills in this area and do not understand their obligations, nor do they have subject matter experts in risk who can readily implement recommendations in this space, such as those in SP800-30 and 800-39.
- **Incident Handling**
  Incident Handling is a wider industry problem, but given HIPAA breach determination and reporting requirements, robust incident handling is very important to this audience. Common pitfalls are incomplete plans, failure to follow plans, failure to maintain audit trails and other evidence, and failure to act with urgency to meet reporting obligations, often due to internal communication problems or unclear escalation paths.

- **Audit controls, logging, and monitoring**
  The lack of detailed logging and retention of logging records often makes it difficult to fully determine root cause and impact of incidents; it can also be beneficial to conduct thorough access reviews. The lack of monitoring and alerting, particularly through automated means, leads to missed early warnings of incidents, or leads to unproductive staff time manually reviewing logs looking for, and often missing, anomalous events.

General Commentary on SP 800-66

These comments apply generally to the document and overall content rather than a specific section.

Most language refers to Covered Entities (CEs) as the targets of requirements or in examples, while the Security Rule also applies to a number of Business Associates (BAs). The document only refers to BAs in those sections of the security rule which explicitly reference them. In our work, BAs are responsible for many parts, if not all, of the Security Rule as delegated from CEs; some BAs we work with process and hold far more ePHI volume than do many CEs.

As organizations continue to outsource computing services of all types and sizes to external providers, it is imperative to understand and manage data flows within an organization and to its external service providers and partners. Examples should include considerations for using a wide range of services and the need to follow applicable guidance from the SP 800 series on topics such as cloud provider-based services. Existing examples primarily describe traditional healthcare delivery models of hospitals and clinics and do not cover the range of supporting services provided primarily by BAs. Many of these smaller service providers have limited security and privacy resources and are in particular need of practical guidance from NIST and others. Often, the most effective guidance for these smaller organizations is to procure services from established providers who can provide the needed controls and expertise to manage them.

Leviathan suggests the addition of a section on data flow mapping and analysis. Understanding data flows between systems, into and out of the organization, and to users is essential in understanding the implications of many of the questions posed in Section 4 and guidance offered there.

Finally, the existing examples primarily depict very traditional Covered Entity models (hospitals and clinics), and to a lesser extent, Business Associates. The current healthcare ecosystem contains a wide range of additional types of providers and processors. Diversity in examples is encouraged to provide examples relevant to a wide range of readers.

Section 4 Comments

Section 4.1, Security Management Process
Leviathan believes more guidance is needed for smaller BAs and CEs who lack expertise in Risk Assessment and Management practices.

Key Activity 2
Where the organization has someone familiar with basic risk management techniques, Appendix E offers a good starting point for assessment activities. However, Leviathan suggests that even simpler guidance may be needed as a starting point; alternatively, the requirement can be outsourced to a party with the qualifications and experience to conduct the assessment.

Key Activities 2 and 3
Leviathan suggests guidance on the timing of Risk Assessment and Management activities. The HIPAA Security Rule does not define expectations for how often these activities are carried out; implementations can vary widely, but suggested minimums should apply:

- Risk Assessment should be performed on all the major systems and areas of the business
- Risk Assessment should be performed while building or buying new services before they are generally available
- Where Risk Assessment has not been consistently or widely performed, the organization should address gaps in their assessment of assets to provide uniform input to the Risk Management Process.
- Risk Management should be performed with regular frequency to examine past decisions, re-evaluate risk likelihood and impact levels, and assess the effectiveness of past remediations.
- Retention of Risk Assessment and Management activities is not covered, but may be crucial for future assessment and management, Incident Response, or Audit activities.
- Risk Assessment and Management activities should be performed regularly. Leviathan suggests at least annually for a thorough assessment and at least quarterly for a management review.
- Appendix E and SP 800-30 describe assessment activities. A simple Risk Management Framework (RMF) is described in Section 3.1 but does not include all of the basic operating requirements of a simplified Risk Management Program. Numerous RMFs exist, including SP 800-39, but tend to be complicated; the process described in section 3.1 could be amended to include:
  - A Risk Management Policy, outlining duties, responsible parties, frequency, and required documentation of the program.
  - A basic risk register that records assessment findings, relative severities, treatment plans, timelines, responsible parties, and dependencies. This could simply be a spreadsheet for smaller organizations.

  - Criteria for risk evaluation and treatment decisions by IT and business leaders.
  - Retention requirements for records of risk treatment activity.

In our experience, many smaller organizations lack experience with Risk Assessment and Management programs, and guidance on starting points will be more useful than pointers to other NIST SPs or outside standards that may pose a barrier to adoption.

Key Activity 4
Leviathan suggests consideration of SaaS and other modern IT System and Service offerings and their respective challenges in acquisition and operation.

Key Activity 7
Leviathan suggests consideration of available automation on cloud service platforms (AWS, Azure, GCP, etc.) as well as SaaS or on-premise logging and SIEM tools to reduce staff time associated with review activities and make them practical to implement. This activity needs guidance on the frequency of system review activity, which varies widely based on technologies in use and an organization's size.

Key Activity 9
Leviathan suggests including more guidance about minimum required activities and their frequency. One potential suggestion is to implement a Plan-Do-Check-Act cycle or similar cyclic process.

Section 4.4, Information Access Management

Key Activity 4
Leviathan believes this activity should place additional emphasis on access reviews. We have frequently found extensive problems related to the lack of timely access reviews. When reviews are performed, often they are tedious and cumbersome as those responsible for the review lack detailed knowledge of individuals and their current access needs. For this reason, we recommend access reviews involve or are delegated to line management familiar with their direct reports' access needs and job duties. Missing from the questions:

- Are access decisions justified, approved, logged, and retained?
- Are review activities logged and retained, including decisions arising from review activities?

Finally, encourage automation in this area to simplify the activity logging and overall effort.

Section 4.5, Security Awareness and Training

Key Activities 1-3
Leviathan feels that feedback and analysis of past events should be included in determining training needs, a training plan and content, and delivery of training. Leviathan suggests that

organizations should conduct a review of behavior issues, past incidents, and breaches to determine what training is missing or needs reinforcement, improvement, or periodic reminders.

Key Activity 4
Leviathan feels that HIPAA/HITECH has become extremely dated with respect to remote work / telework, even before the pandemic. Guidance around travel should be expanded to include any remote setting, including work from home. We frequently find in our assessments that remote work arrangements are not adequately covered, including worker responsibilities for physical security and protecting information from unauthorized access by other members of the household.

Key Activity 7
Leviathan recommends the inclusion of feedback and regular review of attendance data (in person or LMS delivered) to determine if the plan is reaching intended audiences successfully.

Section 4.6 Security Incident Procedures

Leviathan feels that Risk Management should be more integrated with the Incident Response process.

- Incidents caused by or influenced by known risks should feed back into the Risk Management process for reevaluation of impact and likelihood.
- Remediation and corrective action plans arising from incidents should be added to the Risk Assessment and Management process for tracking. Often, we find long term corrective actions can be lost or deprioritized when competing with other work, whereas when tracked as active risks are more likely to be successfully remediated.

Section 4.7 Contingency Plan

Key Activity 2
Leviathan feels that this section needs a major update to reflect current service delivery and work location models, where organizations may be largely reliant on service providers for their infrastructure and remote workers. Considerations:

- Do SaaS and other service provider contractors provide needed reliability guarantees?
- If workforces are remote, or contingencies expect remote work (due to weather or unavailability of primary facilities), have factors such as widespread power or telecommunications outages been considered?

Key Activities 5,7
Data backups are critical, and now involve more “shift” of data location than “restore” of data from media. These activities should consider backup recovery testing (however that occurs) as part of the testing process, and periodically evaluate and verify the ability to recover based on

identified scenarios using actual tests; tabletop exercises are not sufficient to prove restoration capabilities.

4.8 Evaluation

This section discusses penetration testing, but does not consider risk assessment, vulnerability scanning (beyond general mention of automated tools), or other processes such as threat modeling. Leviathan suggests that the feedback from and to the risk assessment and management processes should be considered in evaluation. Many organizations rely solely on automated tools of varying quality, operated by staff of varying skill levels. Such tools may have coverage limitations that do not provide all necessary data for evaluation, and should be supplanted by risk assessment processes, and analysis of potential coverage gaps. Finally, "penetration testing" is a widely misunderstood term; some penetration tests are based on automated tools only, with little to no targeted work performed by actual professionals, or the chaining of individual vulnerabilities together that results in successful penetration of a complex system[1].

4.9 Business Associate Contracts and Other Arrangements

Key Activity 1

Many CEs and BAs outsource computing services to cloud and other providers that will directly or indirectly process or store ePHI. Leviathan feels that guidance is needed for audiences to understand their contractual obligations and procure appropriate service levels to ensure providers are able to meet HIPAA Security Rule obligations. In some cases, this may require procuring a certain level or tier of service from provider offerings, such as a tier that offers a Business Associate Agreement with the service. Additionally, contracts must be reviewed carefully to determine if the provider's standard terms meet needs or are amendable to meet needs; for example, a BA has reporting obligations to a CE within a limited time upon discovery of an incident, but the BA's service provider only offers terms that do not meet that timeframe.

Key Activity 2

Leviathan suggests that this activity include review for specific contract terms around data ownership and disposal at end of contract.

Key Activity 3

The area of Third-Party Assurance is large and cumbersome, in part due to the lack of an effective standard for the evaluation of BA compliance with the Security Rule, leaving organizations to create many disparate processes for this evaluation, with different implementation expectations for security controls. Larger organizations understand this; Leviathan feels that many smaller BAs do not understand their obligations in this area nor how

[1] It is well beyond the scope of this document to resolve the widespread misunderstanding and generalization of penetration testing; more description of what constitutes a reasonable evaluation at breadth and depth might be better comprehended by readers, with mention of (but less reliance on) penetration testing as a component.

to fulfill them. Additional guidance would be helpful. Other NIST publications, such as NIST SP 800-53 revision 4 or NIST SP 800-161, provide detailed guidance for assessing third parties, but the guidance in these may be too heavyweight for smaller BAs. Presented with complex suggested controls, these organizations may default to not performing any assessments or only the most cursory reviews of partner security marketing materials.

4.10 Facility Access Controls

Leviathan suggests that this section explain an organization's obligations when its physical facilities are entirely outsourced to providers, as is increasingly common (i.e., the need to obtain assurances and include contract terms that the terms of § 164.310(a)(1) are met by their suppliers.

4.11 Workstation Use

Leviathan feels that the workstation sections of HIPAA are very dated. Workstations now include a range of mobile devices, all of which may no longer be owned by the CE or BA (BYOD), particularly in remote work situations.

Key Activity 1

Leviathan feels that the focus should be primarily on the user rather than the device.

- Are the inventory details assigned, associated with and tracked by the primary users?
- Are appropriate permissions or restrictions (e.g., remote access or other specific location parameters, use of device by type or capability) associated with users?

Key Activity 3

Leviathan feels physical access controls are increasingly irrelevant to remote workforces. Instead of focusing on the location of the workstation, focus on the location of the work. Many organizations have moved back to a central processing model using virtual desktops and other access technologies to keep ePHI processing centralized and away from the risks of mobile workstations and portable media. Modern work scenarios require additional evaluation criteria:

- Where is work on ePHI occurring?
- What assets are involved in the work?
- What users are involved in the work?
- What controls are relevant to the current assets, users and locations?
- Are appropriate policies and controls in place where physical controls are unavailable or irrelevant?

4.12 Workstation Security

As above in 4.11, Leviathan feels HIPAA's treatment of workstations is out of date and current guidance should broadly consider mobile devices, some of which may be individually owned (BYOD) and user capabilities to access or modify covered data from any device they are able to use.

Key Activity 1
Leviathan feels physical siting and facility controls for access to workstation areas is increasingly irrelevant. Device capability (where laptop, phone or tablet, in addition to desktop workstations), and user permissions to interact with ePHI on the device are more relevant measures. Unfortunately, HIPAA and the OCR Audit Protocol do not consider mobile computing; guidance here could help implementers evaluate current scenarios.

Key Activity 2
Leviathan suggests consideration should be given to mobile devices and remote workers in evaluating access risks.

Key Activity 3
Leviathan suggests additional safeguards should be considered based on limitations to physically securing device locations:

- Whole disk/device encryption
- Limitations on local storage and processing on mobile devices
- Multifactor access controls
- Screen timeout
- Strong Device Management: Mobile Device Management (MDM), Endpoint Detection and Response (EDR)
- Workforce education on mobile and remote computing risks to ePHI, working within established safeguards, and related user responsibilities

4.13 Device and Media Controls

Key Activity 1
Leviathan suggests implementers consider cloud storage, and the need to ensure disposal where backup and versioning of stored data may happen automatically.

Key Activity 3
Leviathan suggests access and audit controls and regular review of shared storage environments to ensure that data stored there is not available to unauthorized parties.

Key Activity 4
Leviathan suggests evaluating available levels of redundancy and geographic distribution of storage service providers to evaluate risks to availability and time to restore.

4.14 Access Controls

Key Activities 1,2,3

Leviathan suggests references to centralized directory services and Single Sign-on and federation as ways to implement the required standard.

Key Activity 6
Leviathan suggests encouraging the use of automation and tooling from service providers where applicable. In our experience, access reviews are weak, infrequent or nonexistent in many circumstances we encounter in the field. This is often due to a lack of available data about necessary and unnecessary access patterns, or a reviewer's unfamiliarity with those access patterns.

Key Activity 7
Leviathan suggests that Emergency Access Procedures only be considered when regular access availability is not fully redundant and/or geographically dispersed. In organizations reliant on highly capable service providers, this should be unnecessary.

4.15 Audit Controls

Key Activity 1
Leviathan strongly encourages the tracking of all access to and movement of ePHI. The existing text suggests a process for identifying activities based on risk and vulnerability. While we are not discussing the HIPAA Data Breach rule in this document, implementors should keep in mind that the lack of detailed audit records contributes to the ability to determine the size of a data breach, and that many breaches reported must consider maximum impact as the exact number of records is often undeterminable by available audit records. The retention of such audit records is also a major consideration.

Key Activities 3-4
Leviathan strongly suggests implementors consider automation to assist in the monitoring and review of information system activity to reduce staff time required and improve the timeliness of critical review information.

4.17 Person or Entity Authentication

Leviathan feels that this section should be expanded to include service or API authentication. In an increasingly distributed service provider and automation model, audiences need guidance on API authentication. Guidance in these areas is still emerging in standards-based form; consider references to NIST SP 800-204 or the OWASP ASVS project.

Key Activity 2
Leviathan suggests inclusion of guidance for common implementation considerations:

- Current multifactor authentication solutions (e.g., based on mobile device applications) as mandatory whenever feasible
- End user account self-registration and verification processes
- Password reset processes

- Resilience against credential stuffing attacks

4.18 Transmission Security

Key Activity 4
Leviathan suggests further reference to encryption standards in the SP 800 series for guidance on the selection and use of acceptable methods. These documents are more likely to provide current guidance in a changing threat landscape, in particular, the lifespan considerations for encryption algorithms and key lengths in SP 800-131A. Bullets 1-3 should be deprecated in favor of a recommendation to implement strong encryption in all internal and external environments; where infeasible, additional risk assessment and compensating controls should be undertaken.

4.22 Documentation

Key Activity 1
Leviathan suggests the inclusion of feedback from risk assessments and contingency plan tests as part of the question about when to consider updating documentation.

In conclusion, Leviathan Security Group thanks NIST for the opportunity to strengthen and improve the protections offered by the HIPAA Security Rule through the Implementation Guidance covered by SP 800-66 Rev. 2. We appreciate the opportunity to share our views on this evolving area and thank NIST for their leadership in this important area.

Sincerely,
Leviathan Security Group