How Deception Technology Helps HIPAA Compliance

A TrapX Security Guide

by Moshe Ben Simon
Founder and Vice President, TrapX Security
Contents

Notice.......................................................................................................................................................... 3
Disclaimer.................................................................................................................................................. 3
HIPAA Overview .................................................................................................................................... 4
HIPAA Compliance Penalties .................................................................................................................. 5
  Table 1 - Civil Violation Penalties ........................................................................................................ 6
Who Must Comply with HIPAA? ............................................................................................................. 7
  Health Care Providers ............................................................................................................................. 7
  Health Plans ........................................................................................................................................... 7
  Health Care Clearinghouses .................................................................................................................. 7
  Business Associates .............................................................................................................................. 7
Privacy Rule and PHI ............................................................................................................................... 8
Security Rule ............................................................................................................................................ 9
  Administrative Safeguards ..................................................................................................................... 9
  Physical Safeguards .............................................................................................................................. 10
  Technical Safeguards ............................................................................................................................ 10
Supporting Specific HIPAA Requirements with TrapX Deception Technology ...................................... 11
  Table 2 - §164.306 - Security Standards: General Rules .................................................................... 11
  Table 3 - §164.308 - Administrative Safeguards ........................................................................... 12
  Table 3 - §164.308 - Administrative Safeguards (Continued) ......................................................... 13
  Table 4 - §164.312 - Technical Safeguards .................................................................................... 14
Notes: TrapX Security Compliance Support ............................................................................................. 15
Deception Technology and HIPAA Compliance ...................................................................................... 17
Appendix A: HIPAA Resolution Agreements and Civil Monetary Penalties ... ................................. 18
  Resolution agreements reported in 2016 year-to-date include the following: ................................ 18
Appendix B: Ransomware Implications for HIPAA ............................................................................. 19
  July 11 Guidance by HHS OCR on HIPAA With Respect to Ransomware .................................. 19
Appendix C: Medical Device Hijack (MEDJACK) and HIPAA Compliance ............................................. 20
Notice

TrapX Security reports, white papers, and position papers are made available for educational purposes and general information only. Although the information in our reports, white papers, and updates is intended to be current and accurate, the information presented herein may not reflect the most current developments or research.

These materials may be changed, improved, or updated without notice. TrapX Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Disclaimer

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is complex legislation. This document is not meant to substitute for legal advice with respect to this legislation. It is meant only to provide supplemental information for HIPAA experts (Privacy Officer, Security Officer, General Counsel or Outside Counsels, or HIPAA Information Technology Specialists) to review in support of a decision to utilize Deception Technology as part of a cyber-defense strategy.
HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), also identified as Public Law 104-191, required the U.S. Department of Health and Human Services to define national standards for electronic health care transactions and security procedures. The legislation outlined how protected health information (PHI) should be safeguarded by the entities that hold it.


HHS published a final Security Rule in February 2003, with compliance required as of April 20, 2005 for large entities and on April 20, 2006 for smaller health plans.

HHS enacted a final Omnibus rule, implementing a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act to strengthen the health information privacy and security protections established under HIPAA. The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 and signed into law on February 17, 2009.
HIPAA Compliance Penalties

Financial penalties are designed to act as a visible and strong deterrent. The goal is to hold covered entities accountable for their actions and help to ensure that they take necessary steps as stipulated by the HIPAA regulations to protect the privacy and confidentiality of health care information.

Financial penalties for failure to comply with HIPAA can be severe. Subtitle D of the HITECH Act includes several provisions that strengthen the civil and criminal enforcement of the HIPAA rules to allow a penalty of up to $1.5 million for all violations of an identical provision. In 2016 alone, a cursory review of the public resolution agreements (see Appendix A) reveals many millions of dollars in fines levied against health care organizations.

Table 1 lists civil violations and the prescribed range of associated penalties. Civil violation penalties are administered by the Department of Health and Human Services, Office of Civil Rights.

Criminal penalties are generally prosecuted by the Department of Justice. Individuals that “knowingly” disclose or obtain protected health information can be fined up to $50,000 and be imprisoned for up to one year. The addition of “false pretenses” can increase the fine to $100,000 and the length of imprisonment to five years. Offenses committed with the intent to use or sell the protected health information can further increase the fine to $250,000 and extend the length of imprisonment to 10 years.
Table 1 - Civil Violation Penalties

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>DESCRIPTION</th>
<th>HIPAA PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1</td>
<td>Unaware.</td>
<td>The minimum penalty is $100 per violation, with an annual maximum of $25,000 for repeat violations.</td>
</tr>
<tr>
<td></td>
<td>The covered entity or business associated was unaware of the violation and could not have avoided it, even if reasonable care had been taken to comply with the HIPAA regulations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum penalty can be $50,000 per violation, with an annual maximum for this violation category of $1,500,000.</td>
</tr>
<tr>
<td>Category 2</td>
<td>Reasonable cause.</td>
<td>The minimum penalty is $1,000 per violation, with an annual maximum of $100,000 for repeat violations.</td>
</tr>
<tr>
<td></td>
<td>The covered entity or business associate should have been aware but committed the infraction due to reasons other than “willful neglect.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum penalty can be $50,000 per violation, with an annual maximum for this violation category of $1,500,000.</td>
</tr>
<tr>
<td>Category 3</td>
<td>Willful neglect but corrected within time period.</td>
<td>The minimum penalty is $10,000 per violation, with an annual maximum of $250,000 for repeat violations.</td>
</tr>
<tr>
<td></td>
<td>The covered entity or business associate violation was due to “willful neglect,” and an attempt was made to correct the violation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum penalty can be $50,000 per violation, with an annual maximum for this violation category of $1,500,000.</td>
</tr>
<tr>
<td>Category 4</td>
<td>Willful neglect and uncorrected within time period.</td>
<td>The minimum and maximum penalty is $50,000 per violation, with an annual maximum of $1,500,000 for repeat violations.</td>
</tr>
<tr>
<td></td>
<td>The covered entity or business associate violation was due to “willful neglect,” and no attempt was made to correct the violation.</td>
<td></td>
</tr>
</tbody>
</table>
Who Must Comply with HIPAA?

HIPAA applies to health care organizations that are defined as covered entities or business associates. Individuals, organizations, and agencies that meet these legislative definitions must protect the privacy and security of health information. Covered entities include health care providers, health plans, and health care clearinghouses.

Health Care Providers
Health care providers include clinicians such as doctors, dentists, nurses and other individuals who must comply with the provisions of HIPAA. Other examples of health care providers include organizations such as hospitals, surgical centers, MRI/CT centers, urology centers, diagnostic laboratories, and skilled nursing facilities (SNFs).

Health Plans
Individual and group plans that provide or pay the cost of medical care are also covered entities. They include health, dental, vision, and prescription drug insurers; health maintenance organizations (“HMOs”); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies).

Health Care Clearinghouses
Health care clearinghouses are entities that process nonstandard information received from other covered entities into a standard (i.e., standard format or data content), or vice versa. Typical examples include billing services, health information systems, and value-added networks that process health information or transactions.

Business Associates
Covered entities do not perform all of their own health care activities and often outsource these services and functions to other entities. These entities are referred to as business associates for purposes of defining their responsibilities in support of HIPAA. Covered entities can allow business associates access to the protected health information as long as the requirements for the protection of the data under HIPAA are passed to the business associates through a contract document that explicitly restricts and guides the business associated in the protection of the data. This contract must contain the provisions stipulated by 45 CFR 164.504 (e). ¹

Examples of business associates include a consultant that performs various studies using hospital data, and an attorney that provides legal services to a health plan and must access protected health information.

¹ http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf
Privacy Rule and PHI

The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity (or related business associates), in any form, whether electronic, paper, or oral.

This information is defined as “protected health information” (PHI) and is subject to regulation under HIPAA. PHI can include information about the individual’s history or current state of physical or mental health, the nature of health care provided to the individual, and information relating to payment for health care, identifying the individual by name, address, social security number, date of birth, etc.

Certain types of data are excluded from being classified as protected health information, including certain types of employment records, education records, and certain other records. These data types are defined in the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA is a Federal law that defines the confidentiality, and protects the privacy, of student education records. FERPA generally applies to schools that receive funding under U.S. Department of Education programs and projects.

The Privacy Rule applies to electronic records, written records, telephone conversations, webinars, etc. Covered entities may only release PHI as permitted by the privacy rule or with the written consent of the individual whose information is to be released. The Privacy Rule also contains administrative, notification, and records-maintenance information, all focused on maintaining records correctly. The Privacy Rule also takes steps to ensure that individuals are aware of their rights under HIPAA.
Security Rule

The Security Rule focuses on the management and protection of Electronic Protected Health Information (ePHI). Three types of security safeguards are defined and required for compliance: administrative, physical, and technical. The Security Rule identifies various security standards and the associated implementation specifications. Required specifications must be implemented and administered as dictated by the Security Rule.

Required specifications must be adopted and administered as dictated by the Security Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situations and determine how best to implement addressable specifications.

Administrative Safeguards

Administrative Safeguards are the policies and procedures designed to show clearly how the entity will comply with the act:

» Covered entities that must comply with HIPAA requirements must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.

» The procedures must address all facets of access, including authorization, establishment, modification, and termination.

» Entities must manage and document a training program regarding the handling of PHI for all employees.

» Covered entities that outsource some of their business processes to third parties must ensure that their vendors also have a framework in place to comply with HIPAA requirements. This business associate agreement, in turn, requires that the third party manage all information in a HIPAA-compliant manner.

» A comprehensive contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place.

» Internal audits play a key role in HIPAA compliance by reviewing operations, with the goal of identifying potential security violations.

» Procedures should exist to address and respond to security breaches identified either during audits or in the normal course of business operations.
Physical Safeguards

Physical Safeguards control against inappropriate access to protected data:

» Controls address and govern the introduction and removal of information technology assets, both hardware and software, from the health care network.

» Any access to hardware, software, and networks containing health information must be carefully managed and monitored.

» This access must also be granted to properly authenticated and authorized individuals only.

» Access controls manage the facility, including facility security plans, maintenance records, and visitor sign-in and escorts.

» Policies must address the use of workstations, personal computers, and other computing endpoints. Workstations should be placed in secure areas only. On-screen visibility of patient data must be limited to authorized personnel.

Technical Safeguards

Technical Safeguards control access to computer systems to protect communications containing ePHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient. These safeguards must protect data in cloud-based systems, telephone voicemail, and webinar infrastructure; almost any application using ePHI data is required to be compliant with the stipulated technical safeguards:

» Information systems housing ePHI must be protected from intrusion.

» Information should be encrypted, especially when it flows across networks.

» Each covered entity must ensure that the data within its systems has not been modified or deleted in an unauthorized manner.

» The use of checksums, double-keying, message authentication, and digital signature are important for data integrity.

» Covered entities must also authenticate every user, using authentication technologies such as single and multi-factor passwords, biometrics, authentication token based systems and more.

» Documented risk analysis and risk management are required. Everything must be documented and embedded in day-to-day practices.
Supporting Specific HIPAA Requirements with TrapX Deception Technology

Table 2 - §164.306 - Security Standards: General Rules

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENT</th>
<th>DOCUMENT SPECIFICATION</th>
<th>TRAPX SECURITY COMPLIANCE SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.306 (a) general requirements (1) (2)</td>
<td>1) Ensure the confidentiality, integrity, and availability of all electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.</td>
<td>In today’s environment, “reasonably anticipated threats” now include sophisticated cyber attackers that will, at some time, successfully penetrate the network. TrapX Security DeceptionGrid™ addresses this by identifying, at very high accuracy and in near real-time, that an intruder has penetrated the network. <strong>NOTE 4.</strong></td>
</tr>
<tr>
<td>§164.306 (b) flexibility of approach (1) (2)</td>
<td>(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (iv) The probability and criticality of potential risks to electronic protected health information.</td>
<td>TrapX DeceptionGrid brings high flexibility to existing security solutions in order to address the broad range of attacks that will penetrate the perimeter and gain access to internal networks. DeceptionGrid addresses targeted attacks on medical devices, targeted ransomware attacks on hospital operations, targeted attacks which seek to compromise internet of things (IoT) devices, general purpose systems and assets that contain critical health data. DeceptionGrid targets and identifies bad actors that utilise a wide variety of techniques including MEDJACK, which is a widespread attack vector currently residing in a large percentage of medical devices. <strong>NOTE 1.</strong> DeceptionGrid also has specific support to protect Internet of things (IoT) connected components. <strong>NOTE 2.</strong> DeceptionGrid includes ransomware protection capabilities that enable security personnel to address these requirements with a solution that ties up and delays the attacker with false data so that the ransomware attack can be stopped, ideally without damage to ePHI data, and normal operations can be resumed promptly. <strong>NOTE 3.</strong></td>
</tr>
</tbody>
</table>
### Table 3 - §164.308 - Administrative Safeguards

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENT</th>
<th>DOCUMENT SPECIFICATION</th>
<th>TRAPX SECURITY COMPLIANCE SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308 (5) (ii) (B)</td>
<td>(B) Protection from malicious software (addressable). Procedures for guarding against, detecting, and reporting malicious software.</td>
<td>TrapX DeceptionGrid provides operational capabilities to guard against, detect, and report malicious software tools used by sophisticated cyber attackers. DeceptionGrid targets and identifies MEDJACK, which is a widespread attack vector currently residing in a large percentage of medical devices. <strong>NOTE 1</strong> TrapX also has specific support to protect Internet of things (IoT) connected components. <strong>NOTE 2.</strong> DeceptionGrid includes ransomware protection capabilities that enable security personnel to address these requirements with a solution that ties up and delays the attacker with false data so that the ransomware attack can be stopped, ideally without damage to ePHI data, and normal operations can be resumed promptly. <strong>NOTE 3.</strong> DeceptionGrid reduces risk and protects core assets by the widespread deployment of Traps (decoys), which are fake health care assets, and, by the further widespread deployment of Tokens (lures), which are fake data assets designed to lure the attackers to the traps. <strong>NOTE 4.</strong></td>
</tr>
<tr>
<td>§164.308 (6) (i)</td>
<td>(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.</td>
<td>TrapX DeceptionGrid improves your security incident process by providing early breach detection and comprehensive reporting inclusive of all the forensics indications of compromise (IOC) to find, locate, and terminate attacker activity within the network. Automated workflows identify attacker activity, collect forensic intelligence and remediate attack sources which ensure policies and procedures are streamlined to significantly reduce risk.</td>
</tr>
<tr>
<td>§164.308 (6) (ii)</td>
<td>(ii) Implementation specification: Response and reporting (required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.</td>
<td>TrapX DeceptionGrid improves your security incident process by providing early breach detection and comprehensive reporting inclusive of all the forensics indications of compromise (IOC) to find, locate, and terminate attacker activity within the network. DeceptionGrid updates all security devices with the details and information of a current threat using the ECO system module, thus providing automated workflow and remediation.</td>
</tr>
</tbody>
</table>
### Table 3 - §164.308 - Administrative Safeguards (Continued)

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENT</th>
<th>DOCUMENT SPECIFICATION</th>
<th>TRAPX SECURITY COMPLIANCE SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308 (a) (1) (ii) (D) Information System Activity Review</td>
<td>(D) Information system activity review (required). Implement procedures to review regularly records of information system activity, such as audit logs, access reports, and security incident tracking reports.</td>
<td>TrapX DeceptionGrid provides comprehensive reporting inclusive of all the forensic indications of compromise (IOC) in order to support the regular review of information system activity and related security incident data. The data that supports these reports is based upon visibility of lateral movement within the network after an attacker has successfully bypassed perimeter, endpoint, and authentication-based defenses. DeceptionGrid Traps and Tokens are tempting targets for attackers and create a visible path and audit trail that shows their activity throughout the entire network and identifies the compromised resources.</td>
</tr>
<tr>
<td>§164.308 (a) (3) (ii) (A) Authorization and/or supervision (addressable)</td>
<td>(A) Authorization and/or supervision (addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.</td>
<td>DeceptionGrid deploys Tokens, which are fake data within the workstation endpoints, that point attackers back to the deployed Traps. Anything that touches the fake assets or fake data is an immediate indication of malicious activity because any normal user should not be accessing resources on the health care endpoints for which they are not authorized. The fake data provides attractive information to an attacker searching the workstation for passwords, authentication, access to databases, and more.</td>
</tr>
</tbody>
</table>
### Table 4 - §164.312 - Technical Safeguards

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENT</th>
<th>DOCUMENT SPECIFICATION</th>
<th>TRAPX SECURITY COMPLIANCE SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.312 (e) (1) Standard: Transmission security</td>
<td>(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</td>
<td>TrapX DeceptionGrid deploys Traps, which are fake assets, and Tokens, which are fake data, across the entire infrastructure, including the network, switches, servers, and endpoints. Anything that touches the fake assets or fake data is an immediate indication of malicious activity because any normal user should not be accessing resources on the health care endpoints for which they are not authorized. Once detected, forensics and indications of compromise (IOC) records can enable a detailed understanding of data access, alteration, and deletion. NOTE 4.</td>
</tr>
</tbody>
</table>

### Table 5 - §164.314 - Organizational Requirements

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENT</th>
<th>DOCUMENT SPECIFICATION</th>
<th>TRAPX SECURITY COMPLIANCE SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.314 (b) (2) (iv) Implementation specifications - report to group health plan</td>
<td>(2) Implementation specifications (required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to - (iv) Report to the group health plan any security incident of which it becomes aware.</td>
<td>TrapX DeceptionGrid provides comprehensive reporting inclusive of all the forensic indications of compromise (IOC) in order to find, locate, and terminate attacker activity within the network and support subsequent reporting by the plan sponsor to the group health plan.</td>
</tr>
</tbody>
</table>
Notes: TrapX Security Compliance Support

**Note 1: Medical device hijack (MEDJACK)**
DeceptionGrid provides specific support to identify, help remediate, and reduce the risk to ongoing operations and ePHI data due to an attacker hijacking medical devices (MEDJACK).

**Note 2: Internet of Things (IoT)**
DeceptionGrid provides specific support to identify, help remediate, and reduce the risk to ongoing operations and PHI data due to the attacker compromising Internet of Things (IoT) devices. DeceptionGrid identifies attacker communications traffic when they are hidden and using “backdoors” within existing IoT devices. One touch or look (a ping against the IP address) at our Traps identifies the attacker as they attempt to move laterally through health care networks in search of ePHI data targeted for theft.

**Note 3: Ransomware**
DeceptionGrid with ransomware protection delivers specific functionality and support to identify, delay, and stop ransomware attacks before they can critically damage health care data and impact health care operations. DeceptionGrid surrounds real data with a virtual barrage of fake SMB data shares. Once ransomware starts the attack and begins encrypting the fake data share, it is conclusively identified. DeceptionGrid delays the attacker with fake data shares while the cyber defense team observes behavior, determine the extent of the ongoing attack, safely shuts it down and then resumes normal operations.

**Note 4: DeceptionGrid**
Our production product, DeceptionGrid, deployed deception technology to the health care market in February, 2014. In developing our methods for deception, it was important to spend time considering the point-of-view of the human attacker and the attacker’s methodology for exploiting and navigating health care networks to identify and exfiltrate data. Deception technology fills the gap and extends the power of traditional cyber defense. DeceptionGrid integrates with existing technologies to provide new visibility into internal networks and share our high-probability alerts and threat intelligence with existing health care infrastructure. Our Traps and Lures are mixed among and within existing IT resources to provide a blanket of protection from attackers that have successfully penetrated the network.

The technical innovation of deception technology has been well received by the health care market. Gartner identified ten top technologies for information security in 2016, including deception technology. Gartner predicts that “by 2018, 10 percent of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers.”

Outside of health care, our research team issued research on other prominent threats including Zombie Zero (pre-installed malware in newly manufactured barcode readers in China) and targeted vulnerabilities within Internet of things (IoT) devices, such as the NEST™ thermostat.

DeceptionGrid was developed to overcome the limitations of both traditional perimeter defense and signature based tools and forms of intrusion detection, as well as the limitations of honeypots. First, the architecture included automation for scalability. It was essential to support large health care institutions without requiring the manual configuration of each

---

individual deception node. The cost of manual deployment was too high as a function of acquiring and maintaining individual operating systems.

Emulation became part of our patent-pending architecture and remains essential to our strategy to support broad-scale deployment and maintenance. Emulation is very powerful when combined with deception technology deployment. We can emulate almost any operating system and application mix.

Emulation remains a powerful differentiator. It enables us to deploy a broad portfolio of traps and lures. We can emulate devices that are targeted to the challenges of industry verticals, such as health care, where we enable customers to deploy emulations for blood-gas analyzers, PACs systems (picture archive servers), MRI systems, and much more. This is a big advantage both for us and our customers. Emulation also brings the advantage of faster, automated deployment and a lower overall cost of deployment. Further, manufactured decoys and traps are generated by software automation, and so we continue to add ways to add, augment, change, modify and “shape shift” them at will.

Emulation gives us a comprehensive and scalable model that can address a small deployment and scale to the largest enterprise. Further, our emulations uniquely cover components in the network, endpoint, applications, and even data. We can emulate switches, routers, and many other network components.

We also use our automation to deploy Tokens which are decoy information technology artifacts (fake shares, credentials, files etc.) that are scattered within the real information technology resources. This creates a tempting environment for an attacker within the network. The sooner we can find these attackers, and reduce the critical time to detection, the sooner we can terminate the attack and reduce the risk to ePHI data.

Traditional cyber-defense technologies, such as firewalls and endpoint security, generate many alerts. In a large enterprise, the alert volume may reach thousands, hundreds of thousands or, in some cases, millions of alerts per day. Security operations personnel cannot process most of the activity, and yet it only takes one successful penetration to compromise an entire network.

DeceptionGrid takes a very different approach. DeceptionGrid ALERTS are the end product of a binary process. Probability is all but reduced to two values: 0% and 100%. Any party that seeks to identify, ping, enter, or view any of our traps is immediately identified by this behavior. This is a binary process, not probabilistic. If you touch these traps this is clearly a violation - you should not be doing so. This is a huge advantage over heuristics and probability-based approaches and the many thousands of extraneous alerts these techniques generate.

Our strong research and development team has brought us to market very quickly. We have assembled a broader product mix of product capabilities than most of our direct competitors. Our automated forensics analysis in our traps, both static and dynamic, provides security operations personnel with accurate data that would take many hours to find using manual processes among disparate systems. This analysis can identify the location of the attacker’s back door within the enterprise and may often help locate the possible origin of the attacker. Further, this analysis often finds trails or links to other components within the networks, such as an endpoint which may be infected or compromised.

Our Air Module takes advantage of this data; it reaches out to the suspect endpoint, performs a complete memory analysis, and then enables shutting down and isolating the infected endpoint.

Our Ransomware protection capability uses our emulation and automation to directly address ransomware. We are able to detect ransomware attacks, distract the attack using our proprietary techniques, and then help shut it down. This is a very recent and important technical innovation in the deception technology marketplace, bringing very high value to our prospects and customers, and can substantially reduce the risk to health care networks from the ongoing barrage of ransomware attacks.
Deception Technology and HIPAA Compliance

Deception technology can impact operations positively and reduce the risk of HIPAA data breaches by rapidly identifying attackers moving laterally within networks. By reducing the time-to-breach-detection to nearly real-time, deception technology can defeat attackers before they can access ePHI data.

Specialized deception technology solutions such as DeceptionGrid enable covered entities to address HIPAA compliance requirements more directly and effectively. Recent clarifications, such as the July update from HHS OCR on ransomware, make specialized cyber-defense products such as DeceptionGrid timely and highly compelling for health care cyber defense.

Increased enforcement of HIPAA with strong penalties is, unfortunately, concurrent with rapid increases in the volume and sophistication of cyber attacks on health care institutions. Within the past few years, cyber attackers have accessed more than 30% of the patient data records in the United States. New attack vectors, such as medical device hijack (MEDJACK), continue unchecked, hidden within medical devices in a majority of our health care institutions.

TrapX Security has the tools to support HIPAA compliance initiatives. We can help you better assess the risk to your health care environment, and we provide you with deception that will help you manage and reduce risk to the lowest levels possible. For more information, please reach out to our health care support team. We look forward to hearing from you.

Deception technology provides new increased visibility into internal networks so that health care entities can answer these critical questions:

- How will I know if my network has been penetrated?
- What can I do to identify cyber attackers rapidly?
- How can I stop ransomware before it encrypts my data?
- How can I reduce or eliminate the risk to my network from attackers that have penetrated my network?
Appendix A: HIPAA Resolution Agreements and Civil Monetary Penalties

A resolution agreement is a settlement agreement signed by Health and Human Services and a covered entity or business associate. The covered entity or business associate must agree to perform in accordance with the agreement and report on their status to HHS. This may continue for a period of up to three years. A resolution agreement may include the payment of penalties, which can be substantial. The examples from 2016 below show some significant settlements.

Resolution agreements reported in 2016 year-to-date include the following:

» UMass settles potential HIPAA violations following malware infection – November 22, 2016

» $2.14 million HIPAA settlement underscores importance of managing security risk – October 17, 2016

» HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016

» Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million – August 4, 2016

» Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) – July 21, 2016

» Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University – July 18, 2016

» Business Associate’s Failure to Safeguard Nursing Home Residents’ PHI Leads to $650,000 HIPAA Settlement – June 29, 2016

» Unauthorized Filming for “NY Med” Results in $2.2 Million Settlement with New York Presbyterian Hospital – April 21, 2016

» $750,000 settlement highlights the need for HIPAA business associate agreements

» Improper disclosure of research participants’ protected health information results in $3.9 million HIPAA settlement – March 17, 2016

» $1.55 million settlement underscores the importance of executing HIPAA business associate agreements – March 16, 2016

» Physical therapy provider settles violations that it impermissibly disclosed patient information – February 16, 2016

» Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800 – February 3, 2016
Appendix B: Ransomware Implications for HIPAA

July 11 Guidance by HHS OCR on HIPAA With Respect to Ransomware

One of the greatest current threats to health information privacy is the rapid growth in malicious cyber attacks on electronic health information systems. Ransomware is the newest and most visible type of attack vector.

To help health care entities better understand and respond to the threat of ransomware, the HHS Office for Civil Rights has released new Health Insurance Portability and Accountability Act (HIPAA) guidance on ransomware. HHS effectively requires that covered entities address ransomware as an issue directly in HIPAA operating procedures, risk assessment, and risk mitigation. Entities must:

» Conduct a risk analysis to identify threats and vulnerabilities, including ransomware, to ePHI and establish a plan to contain and manage those risks

» Implement procedures to safeguard against malicious software, where ransomware must be addressed directly

» Train users in the detection of malicious software

» Maintain an overall contingency plan that maintains data backup and recovery

The guidance states that a ransomware attack usually results in a “breach” of health care information under the HIPAA Breach Notification Rule. For more information, refer to the HHS OCR note in http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf Under the Rule, entities experiencing a breach of ePHI must notify individuals whose information is involved in the breach, HHS, and, in some cases, the media. All of this is incentive to have new technology, and the best practices to support it, to address and defeat ransomware.

Organizations must take steps to protect their data from ransomware attacks. HIPAA covered entities and related business associates are required to develop procedures and deploy technologies that can anticipate, detect, mitigate, and recover rapidly from ransomware attacks.
Appendix C: Medical Device Hijack (MEDJACK) and HIPAA Compliance

Cyber attackers remain a significant and unresolved threat to medical devices and health care networks. Attackers that have embedded “backdoors” within these medical devices are very difficult to detect. They can navigate from these locations within the internal network to identify and steal health care data. These attackers are not easily visible, if at all, to most perimeter and endpoint defense technologies. Probabilistic tools such as intrusion detection will not detect them either. Just one successful attacker accessing ePHI can create a large liability for the health care institutions involved.

“Deception technology enables major health care institutions, such as hospitals, to directly address the risk associated with MEDJACK and enables a much more comprehensive plan for successful risk management and HIPAA compliance. Deception technology can uniquely detect these attackers as they emerge from the medical devices and move laterally out onto the network. Health care cyber defense teams can find the attackers rapidly, ideally mitigate the attack before ePHI can be breached, and then rapidly enable the hospital to resume normal operations.”

Moshe Ben Simon  
Co-Founder and Vice President  
TrapX Security, Inc.

The FDA is wrestling with the problem of integrating modern, safe medical devices with up-to-date cyber defense techniques. To the best of our knowledge, any cyber security software agent or executable from a third party that would be placed within the medical device is absolutely not approved for use at this time. Medical devices are closed devices and, hence, highly vulnerable to the medical device hijack or MEDJACK attack vector.

Attackers, without generating any alert, can distribute their most sophisticated toolkits and establish backdoors within major health care institutions. The attackers have put considerable research and development into the creation of these new tools. Smart malware can now hop laterally across networks to exploit virtually any information within the health care institution.

This makes things much more complex for health care cyber defenders. Cyber defense teams cannot install their local suites of cyber defense software. There is no real protection offered by any third party or pre-installed cyber defense suites. Medical devices cannot be scanned using any sort of agent or intrusive software. In many ways, these medical devices are virtual black holes to the hospital cyber support team. There are many technical reasons and manufacturer restrictions that limit hospitals from installing software within the medical devices. Technical limitations aside, when you speak with them they will tell you directly that the issue is liability. Tampering with an FDA-approved device might impact its operation in some unknown way. No clinician or health care administrator wants to take that risk. All of this makes HIPAA compliance that much more difficult.
As noted in the initial MEDJACK report, hospitals install medical devices “behind the firewall” where they were believed to be secure and protected. This is no longer the case. We know from all of our MEDJACK and MEDJACK.2 case studies that firewall strategies do not work. Modern attackers and their malware have defeated this strategy in the three health care institutions highlighted in the MEDJACK report, in the three additional institutions cited within the MEDJACK.2 report, and in many other health care institutions that we interact with daily. The emergence of MEDJACK creates a very difficult situation in terms of both risk management and threat mitigation.

The MEDJACK and MEDJACK.2 attack vectors present a highly vulnerable target to attackers. The defenders cannot easily get in to detect or remediate an attack. The attackers seem to have a wide open door. Medical devices are “black boxes,” and their internal software is not visible to the hospital cyber defense team. They run out-of-date operating systems, such as Windows 2000, an early version of Windows 7, or Windows XP all of which are highly vulnerable and nearly completely unprotected.

The list of devices vulnerable to MEDJACK and MEDJACK.2 is long, including diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers), life-support equipment (heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines), and more. As noted above, most of these devices run standard and, oftentimes, older operating systems and the medical devices’ proprietary internal software.

About TrapX Security

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our field proven solution deceives would-be attackers with turn-key decoys (traps) that “imitate” your true assets. Hundreds or thousands of traps can be deployed with little effort, creating a virtual mine field for cyberattacks, alerting you to any malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.

TrapX Security, Inc.
1875 S. Grant St., Suite 570
San Mateo, CA 94402
+1–855–249–4453
www.trapx.com
sales@trapx.com
partners@trapx.com
support@trapx.com

TrapX, TrapX Security, DeceptionGrid and CryptoTrap are trademarks or registered trademarks of TrapX Security in the United States and other countries. Other trademarks used in this document are the property of their respective owners. © 2016 TrapX Security. All Rights Reserved.