WHITEPAPER

# HEALTHCARE CYBERSECURITY

## IGNYTE ASSURANCE PLATFORM™

Life Sciences and Health Care Security & Privacy

## CONTENTS

**Introduction to Cyber Security in Healthcare** **3**
**Healthcare Regulatory Agencies & Standards Bodies** **3**
- The Food and Drug Administration (FDA) 3
- The Department of Human & Health Services (HHS) 4
- The Centers for Medicare and Medicaid Services (CMS) 4
- The Office of the Inspector General (OIG) 4
- The National Institutes of Health (NIH) 4
- The Federal Risk & Authorization Management Program (FedRAMP) Program Management Office (PMO) 5
- The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) 5
- The College of American Pathologist (CAP) 5

**Healthcare Regulations & Standards that Impact Information Systems** **6**
- HIPAA Privacy Rule 6
- HIPAA Security Rule 6
- Health Information Technology for Economic and Clinical Health Act (HITECH Act) 7
- Meaningful Use 7
- Federal Information Systems Management Act (FISMA) 7
- FDA Title 21 CFR Part 11 7
- Medical Device Cybersecurity Act of 2017 8
- Internet of Medical Things Resilience Partnership Act (2017) 8
- Payment Card Industry – Data Security Standard (PCI-DSS) 8
- GDPR 8
- FTC Red Flags Rule 9

**NIST RMF: Gold Standard & Backbone of All Security & Privacy Requirements Provided by U.S. Government** **9**
- Free Tools Provided by U.S. Government 10
  - NIST Privacy Overlay 10
  - NIST HIPAA Security Rule Toolkit 10

**The Primary Drivers behind Increasing Regulations & Standards** **10**
- The Growth of Digital Healthcare 10
- Healthcare Industry's Large Attack Surface 10

**How Ignyte Can Help** **11**
- The Service-Enabled Ignyte Assurance Platform™ 12
  - Leverage Subject Matter Expertise 12
  - Comprehensive & Unified Security Platform 12
  - Consortia & Standards Driven Platform 12
- Ignyte Helps Healthcare Security Governance Leaders Take Strategic Approach 13
  - Controlled Security Investment 13
  - Proactive Risk Management 13
  - Do More With Less Resources 13
- Integrate Harmonized Healthcare Compliance & Privacy Requirements directly into your Cyber Operations 14
  - Enable Cross Functional Collaboration 14
  - Controls Instrumentation for Continuous Diagnostics Mitigation (CDM) 14
  - Operationalize Compliance Requirements 14
- Streamline Business Associate Agreements & Data Sharing Agreements 15
  - Respond to High Risk Business Associates 15
  - Reduce Vendor Management Burden 15
  - Consolidate Vendor & Business Associate Portfolio 15

**References** **16**

# INTRODUCTION TO CYBERSECURITY IN HEALTHCARE

**Today, cybersecurity has become a concern for all industries. Healthcare organizations hold some of the most sensitive personal information about people, such as names, dates, places of birth, social security information, and medical records. The healthcare industry is under attack from cybercriminals who seek access to this sensitive personal information. Most healthcare organizations are easy targets because they use legacy systems and lack sufficient financial resources to deploy adequate cyber protection.**

## KEY HIGHLIGHTS

Here are some key highlights about cybersecurity in the healthcare sector:

1. Cybersecurity in healthcare is a patient trust and safety concern.
2. Healthcare information is richer in volume and value than financial or retail services data.
3. Healthcare sector is vulnerable to cybercrime due to historic lack of investment in cybersecurity.
4. Cybersecurity maturity is still at an early stage in the healthcare industry.

U.S. FOOD & DRUG ADMINISTRATION

To clearly understand the healthcare network's cybersecurity attack surface, it is imperative to note that the network includes clinics and doctor's offices, as well as internet-based consulting with remote healthcare providers, cloud-based environments, and connected medical devices deployed both at the facility and patients' private locations. Healthcare networks are largely distributed and dependent on information sharing across disparate care providers and facilities. At the same time, patients and other healthcare stakeholders demand instant access to medical services and information. Ready access provides hackers numerous opportunities to steal valuable information in healthcare networks. Astonishingly, recent findings from an independent security lab revealed that healthcare organizations experience more than double the number of attacks as compared to information owners in other industries. [1] As such, cybersecurity must be an integral part of the care pathway.

## HEALTHCARE REGULATORY AGENCIES & STANDARDS BODIES

The healthcare industry is one of the most regulated industries in the U.S. There are many laws and federal statutes that apply to almost every aspect of healthcare, from a medical device to the safety of patients and how the staff is to be trained and educated. In a study published in Pharmacy and Therapeutics, a peer-reviewed journal, the author notes that "almost every aspect of the field is overseen by one regulatory body or another, and sometimes several bodies,"[2]. Clearly, the broad scope of health care regulations illustrates the fundamental concerns for health and life. By the same token, protecting health-related information is a national priority.

### The Food and Drug Administration (FDA)

One oversight body in the federal sector is the Food and Drug Administration (FDA), which enforces the Food Drug and Cosmetic Act to regulate foods, drugs, cosmetics, and other devices, with a primary aim of protecting the public health by assuring that these products are safe, wholesome, sanitary, and properly labeled.[3] To manage cybersecurity, the FDA has released a draft of Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. This guidance document is designed to address security concerns for achieving a 510K Premarket approval.

### The Department of Human & Health Services (HHS)

The Department of Health and Human Services (HHS) is a cabinet-level agency in the executive branch of the government created to protect the public health and to provide essential human services.[4] HHS is responsible for administrating health, welfare, and health information programs. The body provides guidance for healthcare application development and protection against cyberattacks. In addition, HHS investigates new technologies and actively administers a health IT infrastructure.  The Office for Human Research Protections (OHRP) provides oversight to all federally funded research.[5]  The Office of Civil Rights (OCR) enforces the HIPAA regulations, including the Privacy and Security Rules.[6] The oversight body enforcement strategies have yielded significant findings that have been used to improve privacy practices in the healthcare. OCR has received more than 186,000 HIPAA violation complaints and initiated more than 900 reviews.

### The Centers for Medicare and Medicaid Services (CMS)

Centers for Medicare and Medicaid Services (CMS) assures the health care security and quality for beneficiaries.[7] CMS supports innovative approaches aimed at improving quality and accessibility while exploring suitable ways to securely deploy technology to support patient-centered care services.

### The Office of the Inspector General (OIG)

The Office of the Inspector General (OIG) is responsible for protecting the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries.[8] Since its establishment in 1976, OIG has been at the forefront of the country's effort to eliminate abuse, fraud, and waste in Medicare and Medicaid, among other HHS programs. Currently, HHS OIG is the largest inspector general's office in the Federal Government equipped with sufficient resources to meet its objectives.

### The National Institutes of Health (NIH)

The National Institutes of Health (NIH) is the steward of medical and behavioral research in the country.[9] In fact, the oversight body is one of the world's foremost medical research centers and a focal point for health research. As a steward of medical research in the country, NIH seeks fundamental knowledge about the nature of living systems with the aim of using such findings to enhance the quality of health, reduce disability and illness, and lengthen life.

### The Federal Risk & Authorization Management Program (FedRAMP) Program Management Office (PMO)

The Federal Risk and Authorization Management Program (FedRAMP) is managed by the General Services Administration (GSA) and was developed through a close collaboration with cloud and cybersecurity experts to guide cloud service providers in implementing security requirements in their environment. This includes healthcare providers and researchers working with NIH, HHS, and other federal agencies. Almost all federal healthcare agencies are shifting to the cloud to drastically reduce costs while improving patient care. As such, they can adopt NIST-based FedRAMP controls to offer secure cloud computing services.

### The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)

Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) sets the standards by which health care quality is measured for performance improvement.[10] The development of JCAHO standards is based on input from healthcare professionals, service providers, experts, customers, and government. JCAHO has also published cyber emergency preparedness guidance to aid in protecting healthcare information.

### The College of American Pathologist (CAP)

College of American Pathologists (CAP) is a leading organization of board-certified pathologists that serves patients and the public by fostering excellence in the practice of pathology and laboratory medicine globally. CAP has comprehensive accreditation guidelines for laboratory quality assurance. In particular, the CAP General Laboratory Checklist has a section for system security. The standard outlines explicit policies that focus on access to patient data, computer access codes, unauthorized software installation, and public network security.

## HEALTHCARE REGULATIONS & STANDARDS THAT IMPACT INFORMATION SYSTEMS

The healthcare industry is characterized by a collection of agencies and standards organizations that regulate and enforce technology delivery within the healthcare sector, creating a patchwork of often redundant requirements. In fact, it is overwhelming to establish and understand all regulations applying to the healthcare sector or to determine which regulatory body is responsible for enforcing given requirements. Below are some of the many regulations and standards the healthcare industry faces when managing cybersecurity requirements.

**HIPAA Privacy Rule**

Most people are aware of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule due to the consent that they have to sign and notices they receive for healthcare services. Health organizations across the country now integrate privacy with their digital security program. Privacy is a cyber concern and the National Institute of Standards and Technology (NIST) is currently developing standards to properly integrate privacy and security risks into a singular framework.

Overall, the Privacy Rule contains roughly 30 requirements and controls. The controls are put in place to protect a patient's medical records and other personal health information. It applies to health plans, health care clearinghouses, and those healthcare providers that conduct certain health care transactions electronically. The rule calls for safeguards to be implemented in order to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients' rights over their health information, including rights to examine or obtain a copy of their health records, and to request corrections.

Within the Department of Health and Human Services (HHS), the Office for Civil Rights (OCR) has the responsibility for implementing and enforcing the Privacy Rule with respect to compliance activities and potential monetary penalties. See the Combined Regulation Text of All Rules and Understanding HIPAA for additional guidance.

**HIPAA Security Rule**

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule establishes a national set of security standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity or business associate. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This is one of the more prescriptive frameworks of security legislation and breaks down the requirements for organizations into four clear areas:

- **164.308 (administrative safeguards)**
- **164.310 (physical safeguards)**
- **164.312 (technical safeguards)**
- **164.316 (policies and procedures and documentation requirements)**

A risk assessment helps organizations ensure they are compliant with the administrative, physical, and technical safeguards and assists in identifying areas within an organization where protected health information (PHI) could be at risk. The Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) have developed a tool for small and medium sized health care practices and business associates to help with conducting risk assessments. The HIPAA Security Risk Assessment Tool, provides guidance in performing a risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Promoting Interoperability (PI) Programs.

### Health Information Technology for Economic and Clinical Health Act (HITECH Act)

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.  Embedded within HITECH is the enforcement of HIPAA and explicitly defines monetary fines as prescribed by OCR for both business associates and covered entities.

This act authorizes the Centers for Medicare and Medical Services (CMS) to offer reimbursement incentives for healthcare providers for use of certified electronic health record (EHR) technology. The HITECH Act gives the Department of Health and Human Services the legal mandate to manage regulations that promote development and implementation of an “interoperable, private, and secure nationwide health information technology infrastructure through the Office of the National Coordinator of Health Information Technology,”[11].  The adoption of this act has created an important legacy systems overhaul in the healthcare sector.

### Meaningful Use

The American Recovery and Reinvestment Act of 2009 (ARRA) was enacted on February 17, 2009. As part of ARRA, the Centers for Medicare & Medicaid Services developed the EHR Incentive Program - also referred to as Meaningful Use.  The program provided incentive payments to eligible professionals (EPs), eligible hospitals, critical access hospitals (CAHs) and Medicare Advantage Organizations to support the adoption and meaningful use of interoperable health information technology (HIT), and qualified electronic health records (EHRs).  The program's goals were part of a larger effort under the HITECH Act to accelerate HIT utilization of qualified EHRs & health IT.

HITECH promoted the meaningful use of interoperable and secure electronic health records throughout the U.S. health care delivery system as a critical national goal. Meaningful Use also reinforced existing the HIPAA Security Rule along with specifically requiring a risk assessment around EHR systems. Meaningful Use is defined by the use of certified EHR technology in a meaningful manner (for example electronic prescribing); ensuring that the certified EHR technology is connected in a such way that it provides for the electronic exchange of health information to improve the quality of care and enhance privacy.

### Federal Information Systems Management Act (FISMA)

The Federal Information Security Management Act (FISMA) is U.S. legislation that provides recommended security controls for federal information systems to achieve adequate security for multi-layered, risk-based activities involving management and operational personnel within the organization. Signed into law part of the Electronic Government Act of 2002, FISMA applies to all government agencies and healthcare systems funded by the government in order to conduct research. FISMA applies to many research institutions that have received funding or assistance from federal government through a grant. The government implements FISMA through the NIST risk management framework using NIST special publication as its defacto implementation guidance.

### FDA Title 21 CFR Part 11

There isn’t a consistent framework to do complete security mapping of the CFR to an existing control set.  Sometimes this requirement is segmented to clearly document applicability to medical devices and systems directly tied to EHRs and research.

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the U.S. Food and Drug Administration (FDA) requirements for electronic records and electronic signatures. Part 11 details the criteria for electronic records and electronic signatures to be considered reliable and comparable to paper records.

### Medical Device Cybersecurity Act of 2017

The Medical Device Cybersecurity Act of 2017 (S. 1656) was proposed in July 2017 to provide oversight to the medical device manufacturers who hadn't been adequately protecting their products against cybersecurity risks and vulnerabilities. The bill is designed to increase the responsibilities of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to include the cybersecurity of medical devices. At its core, the bill recommends developing a "report card" for medical devices to check their resiliency to cyberattacks. The report card would be generated from testing conducted prior to sale. The legislation is intended to strengthen the healthcare network overall against attacks that put patient's health and personal information at risk of being exploited.

**Other provisions to the bill include:**

- **Strengthen remote access protections for medical devices both inside and outside of hospitals.**
- **Ensure critical cybersecurity updates and patches remain free and do not require recertification by the Food and Drug Administration (FDA).**
- **Offer guidance and recommendations for end-of-life devices, such as secure disposal and recycling instructions.**

### Internet of Medical Things Resilience Partnership Act (2017)

To increase the security of medical devices connected to the internet, Congress proposed a bill in the House of Representatives on October 5th, 2017. The new bill called the "Internet of Medical Things Resilience Partnership Act of 2017," H.R. 3985 - is under review by the House Committee on Energy and Commerce's Subcommittee on Health.

The bill proposes establishing a working group of public and private entities led by the Food and Drug Administration (FDA) and the National Institute of Standards and Technology (NIST). The group would recommend voluntary security frameworks and guidelines that would apply to networked medical devices sold in the U.S. The affected devices store, receive, access or transmit information to an external recipient or system for which unauthorized access, modification, misuse, or denial of use may result in patient harm.

### Payment Card Industry – Data Security Standard (PCI-DSS)

In the early 2000s, online payments were becoming more common and security breaches were increasing rapidly. To combat this, in 2004, all the major credit card companies worked together to develop a comprehensive set of security standards for merchants.

The latest version, PCI-DSS 3.2 includes over 300 individual requirements. Most healthcare organizations are processing standard credit card payments to some degree. Sometimes information security professionals, will segment the environment to reduce the PCI requirements and lower the effort to becoming compliant. However, the requirements remain applicable as long as credit card data is involved.

### GDPR

The General Data Protection Regulation (GDPR) applies to Healthcare organizations that work with European citizens. GDPR came into effect on May 25th, 2018. GDPR is designed to help customers gain more control over their data by offering added transparency throughout the data collection and use process. It also aims to simplify the regulatory environment for businesses so both businesses and citizens in the European Union will fully benefit from the digital economy. For the most part, GDPR consolidates principles from part of the UK's Data Protection Act. However, there are elements of GDPR, such as breach notification and ensuring that someone is responsible for data protection, which organizations now need to address, or run the risk of a fine.

At its core, the laws are designed to bring existing legislation including those around personal data, privacy and consent across Europe up to par with the digital age. GDPR applies to any healthcare organization operating within the EU, as well as any organizations outside of the EU which offer goods or services to customers or businesses in the EU.  Almost every major global healthcare corporation in the world must comply with GDPR.

**FTC Red Flags Rule**
Healthcare organizations that meet the rule's definition of "creditor" must comply with the Red Flags Rule. Organizations count as creditors if they do the following, in addition to deferring payment for goods and services or billing customers:

**The Red Flags Rule defines "Covered Accounts" as either:**

- **Receive or use consumer reports in connection with a credit transaction.**
- **Give information to credit reporting companies in connection with a credit transaction.**
- **Advance funds to or for someone who must repay them, either with funds or pledged property. This excludes incidental expenses in connection to services the business provided to the consumer.**

The Red Flags Rule requires healthcare organization to execute a written identity theft prevention program designed to detect the "red flags" of identity theft in day-to-day operations, take measures to prevent a potential crime, and mitigate its damage if necessary. The Federal Trade Commission (FTC) enforces the Red Flags Rule along with several other agencies.

## NIST RMF: GOLD STANDARD & BACKBONE OF ALL SECURITY & PRIVACY REQUIREMENTS PROVIDED BY U.S. GOVERNMENT

Overall, there are numerous cybersecurity frameworks in the healthcare sector created to help organizations to keep their network secure. Even if some of them might not have the same scale such as HIPAA and HITECH, they are all critical tools that cannot be ignored by entities in the industry. They are intended for organizations to utilize to protect their patient information. As cybersecurity standards become required, it is critical that organizations understand how best to implement them to create a comprehensive and effective approach to critical information security.

The National Institute of Standards and Technology (NIST) issues one of the most common cybersecurity frameworks, NIST CSF, which was first published in February 2014.  The framework is currently being adopted in the healthcare sector among others. NIST also reworked the CSF to make it easier to use. The framework remains voluntary and flexible to implement.  The NIST CSF advises proper implementation of cybersecurity measures to help an organization align its cybersecurity controls with business requirements and resources.

Federally funded healthcare research institutions that are working collaboratively with high education & national university systems are mandated to follow FISMA and/or DFARs. Both of these regulations extend into full implementation of NIST RMF and sometimes FedRAMP depending on the exact implementation of the healthcare technology and specific enforcement agency.

### Free Tools Provided by U.S. Government

To aid in the adoption of various standards, the U.S. Government has provided several free tools which are available to healthcare organizations. Some of these tools come pre-configured for healthcare right out of the box. Healthcare organizations with minimal resources are encouraged to use these tools to help them getting started.

#### NIST Privacy Overlay

As mentioned above, in 2002, Congress passed the Federal Information Management Act to develop and implement computer security plans that follow the standards set by the National Institute of Standards and Technology (NIST). In turn, NIST implemented the Risk Management Framework (RMF), which is a set of interconnected security standards detailing processes and specific technical requirements.

NIST offers a mapping overlay authoritatively developed by the legal teams from a NIST, HHS, OCR, and NIH for general public release. The Privacy Overlays identify security and privacy control specifications required to protect personally identifiable information (PII), including protected health information (PHI).

The Privacy Overlay utilizes the existing NIST framework to apply the necessary security and privacy controls for protecting PII.

#### NIST HIPAA Security Rule Toolkit

The NIST HSR Toolkit is used by organizations to better understand the requirements of the HIPAA Security Rule (HSR), implement those requirements, and assess those implementations within their own operational environments.

## THE PRIMARY DRIVERS BEHIND INCREASING REGULATIONS & STANDARDS

### The Growth of Digital Healthcare

Today, connected medical devices have become common in patient care as customers play an active role in monitoring their health. The adoption of technology allows patients to access their medical information and track their treatment process remotely, a trend that has led to a boom in the connected medical devices industry. Unfortunately, the same technology is introducing increased cyber risks, especially in situations where medical devices and systems are not initially developed with cybersecurity in mind.

Increased digital care has led to an increased number of regulations to protect patient information from cyberattacks. Unfortunately, digital capabilities in the sector are evolving and innovating at a fast pace, making it difficult for regulatory bodies to catch up with an effective list of security rules and recommendations. Routine standards for regulating health information technology will continue to grow as the sector aims to catch up with emerging technologies and capabilities.

### Healthcare Industry's Large Attack Surface

However, despite being one of the most regulated industries, a benchmark against other highly regulated industries, such as financial and banking services, reveals that healthcare is far behind in its cybersecurity practices. This is a critical observation for the second largest sector of the U.S. economy, accounting for 18 percent gross domestic product (GDP), according to 2017 statistics. In fact, the health sector is only rivaled by the U.S. Federal Government that accounts for a 20 percent share of GDP. In 2017, information technology spending in healthcare reached $100 billion.[1] This increased growth also indicates increased activities in the cybersecurity attack surface.

The healthcare sector was the victim of 88 percent of all ransomware attacks in the U.S. in 2016. According to CSO Online,[1] 81 percent of cybersecurity incidents are caused by employee negligence, such as the use of weak administrative credentials, loss of digital devices, accepting phony attachments, emails, and other ways hackers use to expose users to malicious software or phishing scams.[12] Despite these findings, only 27% of healthcare security executives feel confident about safeguarding patient data. Additionally, the healthcare industry invests only 6 percent of its budget to cybersecurity.[13]

**Other crucial study findings include:**

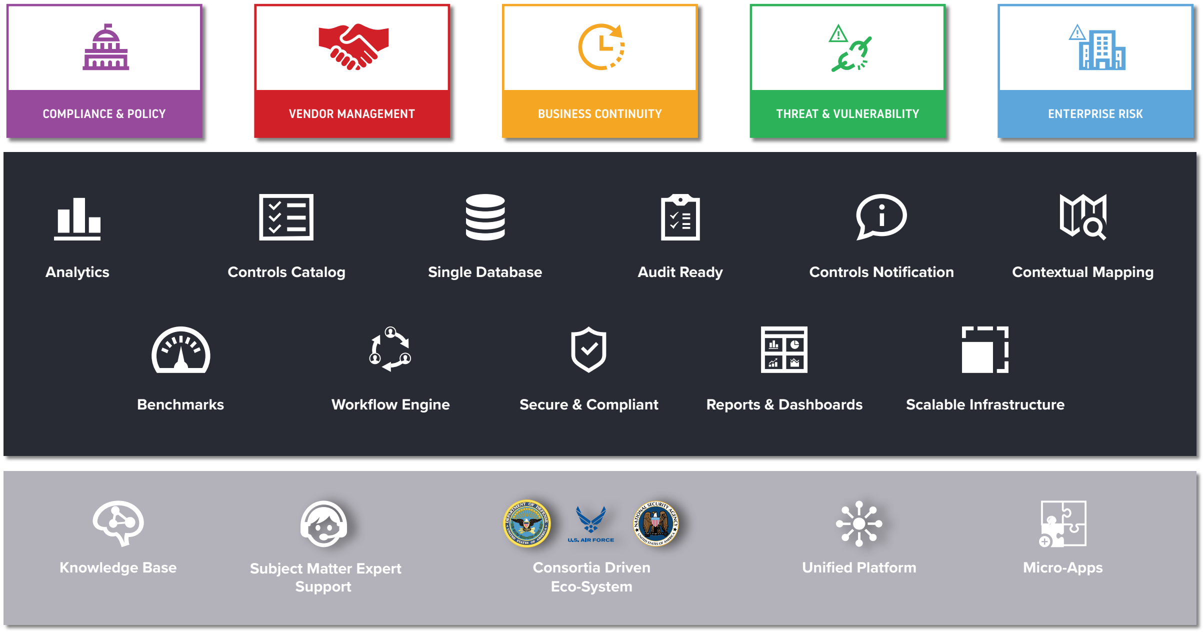
1. **Over 75% of the entire healthcare industry has been infected with malware within the last 12 months.**
2. **88% of all healthcare manufacturers have had malware infections.**
3. **96% of all ransomware affecting the healthcare sector targeted medical treatment facilities.**
4. **Healthcare ranks 15th out of 18th in social engineering among industries, an indication that personnel and staff lack security awareness.**
5. **63% of the biggest U.S. hospitals have less than a C in patching cadence.**
6. **Past-breached organizations have been found to have 242% as many C's or lower in social engineering compared to non-breached companies.**

## HOW IGNYTE CAN HELP

Working with Ignyte Assurance Platform, organizations in the healthcare industry will efficiently manage various frameworks, implement consistent cyber practices across the firm, address diverse cyber threats, and ensure full regulatory compliance. Ignyte offers world-class risk and compliance management to help businesses safeguard customer and corporate interests. Overall, Ignyte provides organizations with the capabilities for strengthening their reputation and brand while avoiding fines from regulatory non-compliance. In other words, working with Ignyte can help free up resources for use in exploring new investment prospects by turning compliance and risk into a business opportunity. Ignyte has the ability to see the entire landscape from end-to-end and top-to-bottom through its integrated compliance and risk management service offering.

### The Service-Enabled Ignyte Assurance Platform™

Using the Ignyte Assurance Platform™ provides a robust security management platform that consolidates several siloed operations into a dashboard.



COMPLIANCE & POLICY
VENDOR MANAGEMENT
BUSINESS CONTINUITY
THREAT & VULNERABILITY
ENTERPRISE RISK

Analytics
Controls Catalog
Single Database
Audit Ready
Controls Notification
Contextual Mapping
Benchmarks
Workflow Engine
Secure & Compliant
Reports & Dashboards
Scalable Infrastructure

Knowledge Base
Subject Matter Expert Support
Consortia Driven Eco-System
Unified Platform
Micro-Apps

### Leverage Subject Matter Expertise

Ignyte provides dedicated software support and dedicated subject matter expertise to help you to build your environment to comply with competing healthcare requirements. The SMEs are certified and have years of experience working for many healthcare organizations.

### Comprehensive & Unified Security Platform

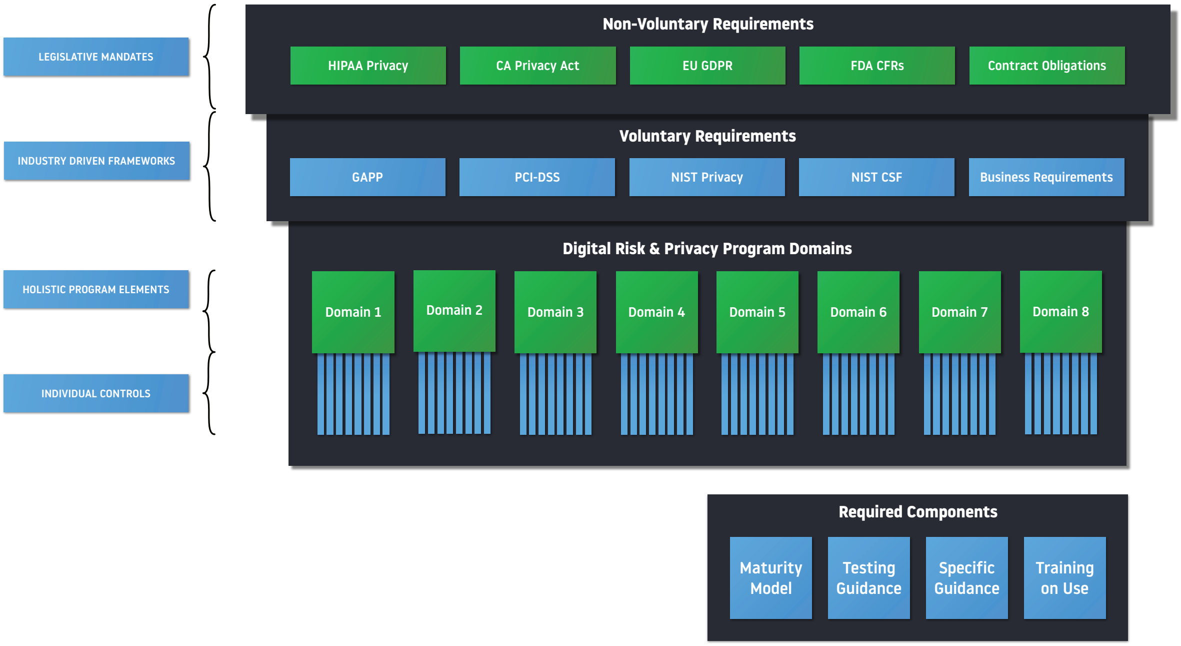
Ignyte Assurance Platform™ is a unified platform built on microservices architecture with a proprietary connector framework. This allows organizations to quickly configure the platform based on healthcare-specific use cases along with data ingest capabilities.

### Consortia & Standards Driven Platform

Ignyte Assurance Platform™ is built on collaboration within a healthcare consortium led by the largest healthcare systems and federal organizations in the country. The Ignyte team closely follows all national and international standards and continuously collaborates with healthcare risk and compliance teams. This allows us to build a platform that is truly driven through standards bodies on how to proactively govern risk and compliance issues specific to the healthcare industry.

### Ignyte Helps Healthcare Security Governance Leaders Take Strategic Approach

Security governance leaders are constantly responding to individual requirements. Ignyte allows teams to step back and develop a strategic governance framework that captures both voluntary and non-voluntary requirements. Requirements are then baked into various security programs leading to a comprehensive set of integrated and harmonized controls.



### Controlled Security Investment

Security leaders are often being asked the fundamental value question of “is this worth it?” Ignyte's platform answers this question by providing a cost analysis baked right into the software so that benefits can be measured along with associated risks.

### Proactive Risk Management

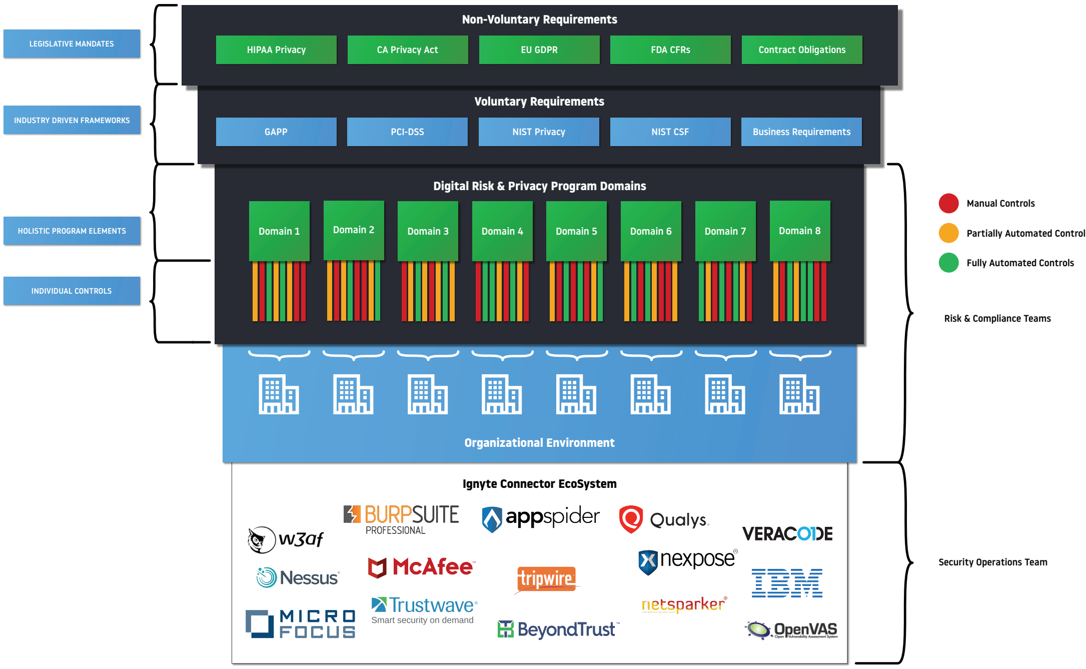
Proactively managing risk in healthcare is the key to staying ahead of emerging requirements and fast changes in technology. Ignyte allows you to manage several types of risks simultaneously in individual risk registers and then link them all to a single strategic objective.

### Do More With Less Resources

One of the most significant challenges facing today’s CISOs is the lack of sufficient resources. Security is most often under-funded by many organizations. The Ignyte platform serves as a force multiplier leveraging product-enabled services. Automating helps Ignyte reduce thousands of man-hours normally spent on copying and pasting data to-and-from different spreadsheets.

### Integrate Harmonized Healthcare Compliance & Privacy Requirements directly into your Cyber Operations

Compliance teams and operations teams are often separated into their own silos making end-of-month executive reporting a difficult and time-consuming task. Ignyte integrates any management framework into operations through our zero-code connector framework bringing control automation to a whole new level. Ignyte offers proper continuous diagnostics monitoring (CDM) strategy through its control instrumentation approach to properly align all cybersecurity products reporting into a singular management framework.  CDM offers a real time approach to managing cybersecurity properly and holistically from the executive management's viewpoint.



### Enable Cross Functional Collaboration

Security operations and compliance management teams are often at odds with each other in terms of execution. Ignyte allows both teams to collaborate in a single platform to provide executive management confidence in the organization's security posture. Ignyte enables this by providing a connector framework for the operations team to feed data into risk and compliance operations.

### Controls Instrumentation for Continuous Diagnostics Mitigation (CDM)

Our Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of healthcare networks and systems. The CDM Program provides organizations with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. All vulnerabilities and threats are received from various sensors or security operations teams and tied directly to each instrument control to bring visibility in the organization.

### Operationalize Compliance Requirements

Ignyte integrates into your existing business processes so that it becomes part of how you conduct your business. Ignyte starts with using your data to improve internal processes and boost decision-making quality about security and privacy initiatives.

### Streamline Business Associate Agreements & Data Sharing Agreements

Ignyte's vendor risk and third-party risk management module provides an integrated approach to managing your vendors. Our vendor risk management module offers the ability to separate business associates from general vendors and those requiring specialized data sharing agreements. Organizations can also import shared assessment SIGs to quickly develop customized questionnaires. Self-onboarding reduces the administrative burden and automated scoring features allow your team to focus on high-risk vendors.

#### Respond to High Risk Business Associates

Identifying high risk and non-compliant business associates is a critical part of a vendor risk management program. Organizations can accelerate decision-making across stakeholders and facilitate cross-functional remediation and risk mitigation processes.

#### Reduce Vendor Management Burden

Ignyte transforms the way you manage business associates through vital reporting of risks and issues, a consistent assessment and remediation process, and automated assessment procedures. We provide a means to facilitate stakeholder interactions, drive transparency and accountability, and effectively monitor vendor-related risks.

#### Consolidate Vendor & Business Associate Portfolio

The vendor portfolio is your database of vendors and business associates. This includes the contacts you interact with, the business services and products that the business associates fulfill, assessment records and documentation, along with other general information. A self-service portal is available so business associates can maintain and update their own information.

## REFERENCES

[1] L. Adefala, "CSO Online," Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries, 2018. [Online]. Available: https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

[2] R. I. Field, "NCBI," Why is health care regulation so complex? Pharmacy and Therapeutics, 33(10, 2005. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2730786/.

[3] "What does FDA do?," 2018. [Online]. Available: https://www.fda.gov/aboutfda/transparency/basics/ucm194877.htm.

[4] "The Department of Human and Health Services," [Online]. Available: https://www.hhs.gov/.

[5] "HHS.gov.," [Online]. Available: https://www.hhs.gov/ohrp/.

[6] "HIPAA," [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

[7] "Home - Centers for Medicare & Medicaid Services," 2018. [Online]. Available: https://www.cms.gov/.

[8] "Office of Inspector General, Department of Health and Human Services," [Online]. Available: https://oig.hhs.gov/about-oig/about-us/index.asp.

[9] "National Institutes of Health (NIH)," About the NIH, 2015. [Online]. Available: https://www.nih.gov/about-nih/what-we-do/nih-almanac/about-nih.

[10] "Joint Commission on the Accreditation of Healthcare Organizations," Facts about Joint Commission accreditation standards | Joint Commission, 2018. [Online]. Available: https://www.jointcommission.org/facts_about_joint_commission_accreditation_standards/.

[11] R. H. C. D. &. G. J. Behara, "The evolving regulatory framework for health information technology in the U.S. Twentieth Americas Conference on Information Systems, Savannah," 2014.

[12] T. Armerding, "CSO Online," Humans cause many of the healthcare breaches, 2015. [Online]. Available: https://www.csoonline.com/article/2871215/data-breach/healthcare-breaches-need-a-cure-for-human-errors.html.

[13] "Cyberpolicy," 4 Healthcare Cybersecurity Stats That'll Raise Your Blood Pressure, [Online]. Available: https://cyberpolicy.com/cybersecurity-education/4-healthcare-cybersecurity-stats-thatll-raise-your-blood-pressure.