IMAGINARY COMMUNITY HEALTH CENTER
COMPUTER SECURITY RISK ASSESSMENT

MAY 26, 2020

Prepared By:
Mike Owens
mowens@eagleconsultingpartners.com

Eagle Consulting Partners, Inc.
6779 Memphis Ave. #7 | Cleveland, Ohio 44144
216.503.0333 | www.eagleconsultingpartners.com

Table of Contents

Appendices

DOCUMENTATION OF MANAGEMENT REVIEW

An important component of the Security Risk Assessment and Risk Management process is the review of Assessment results by an organization's senior management, those with decision-making responsibility for the organization. If management does not understand and manage the exposures to the organization from system downtime, data loss, and/or data breach, the organization could face crippling costs, regulatory actions, or both.

Regulatory enforcement agencies, such as the HHS Office of Civil Rights, the federal agency responsible for HIPAA enforcement, seek proof of Risk Assessment acknowledgement and of Risk Management actions during audits and investigations.

Organization management may sign and date below to document their review of this report. Eagle recommends saving a signed copy of this report with the organization's compliance or risk management files.

I/We, as senior management of Imaginary Community Health Center with decision-making responsibility for the organization, affirm that I/we have received and reviewed this security risk assessment report. I/We understand the risks, findings, and recommendations documented herein.	
Signed: **Name:** **Title:** **Date:**	**Signed:** **Name:** **Title:** **Date:**
Signed: **Name:** **Title:** **Date:**	**Signed:** **Name:** **Title:** **Date:**
Signed: **Name:** **Title:** **Date:**	**Signed:** **Name:** **Title:** **Date:**

This page is provided as a courtesy to Imaginary Community Health Center for their own record-keeping purposes in case of future incident, audit, or regulatory review. The signed page should not be returned to Eagle Consulting Partners. Eagle takes no responsibility for maintaining a copy of this documentation, unless otherwise established via contract.

EXECUTIVE SUMMARY

Introduction

Eagle Consulting Partners conducted a HIPAA Security Risk Assessment for Imaginary Community Health Center (ICHC) using the methodology specified in NIST SP 800-30. The Assessment identifies and measures risks by looking at both the probability that an event will occur, and if it does occur, what the impact will be on the organization. Eagle uses the Factor Analysis of Information Risk (FAIR) model for providing quantitative estimates of possible financial losses and loss event frequencies.

Management should prioritize addressing the scenarios with the highest risk levels first, particularly those highlighted in the "Top Findings" section below. Other risk-reducing activities may be undertaken as time and resources allow.

This Assessment should not be construed as a scorecard, grade, checklist, or criticism of the organization or security or IT personnel. Eagle does not expect or suggest that an organization should have no risks or a "perfect score."

The presence or absence of security controls may be a function of budgetary considerations and management directives to security personnel, IT support, and other relevant staff and contractors. This Assessment is designed to identify and highlight the risks to the organization's electronic Protected Health Information so that organization management can make informed choices about information security priorities and investments.

Our report includes a summary of top findings, a more detailed review of our methodology, an overview of the cybersecurity threat landscape, an update on HIPAA enforcement, and important takeaways relevant to the organization. In Appendix 1 – Risk Register, we explore a range of possible loss event scenarios and estimate the annualized loss amounts for each. Appendix 3 includes a more detailed impact analysis of a major data breach on the organization. Appendices 4 and following document ICHC's existing practices to protect against security incidents, the best practices, and our recommendations for corrective action.

Mike Owens of Eagle Consulting Partners was the lead information security consultant on this engagement.

Top Findings

For Imaginary Community Health Center, our top findings include:

Financial Impacts

1) The cost of total data loss is estimated at between $290,000 and $415,000. Additionally, we forecast a four- to six-week cash flow disruption of $350,000-$530,000 while systems capabilities are being replaced. While we have technical recommendations to reduce this risk, it will never be zero, so we recommend that you review your insurance coverage to protect the practice. The organization's current cyber insurance policy provides only $100,000 for business income loss and another $100,000 for data recreation costs. Since the probability of data loss is very low, additional coverage for this type of loss is inexpensive. See Appendix 3B for breakdown of this analysis.
2) We estimate that the breach response cost of a worst-case data breach would range from $65,000 to $120,000. This impact estimate does not include the risk of HIPAA regulatory penalties, which are issued to roughly 2% of major breaches and could be as high as $300,000 for an organization your size. There are multiple recommendations in the report to

reduce this risk. While there are technical measures to reduce this risk, these measures cannot eliminate it. The organization's data breach insurance covers many of the projected cost categories. However, our high-end projections for regulatory penalties exceed the coverage amount in the organization's existing policy. See Appendix 3A for breakdown of breach-related financial impacts.

3) Extended downtime of the network and EHRs of one week would cause estimated financial impacts of $2,000 to$4,000. These impacts are primarily based on reduced patient volume and staff productivity losses.
4) Ransomware is a special case that the organization should be aware of. Ransomware – a type of malware that encrypts computer data and demands payment before providing the decryption keys – has been a frequent and effective form of attack over the last two years. Healthcare organizations have been particularly common targets for these attackers. Ransomware infection is considered a data breach – in addition to the extended downtime it causes – because hackers have begun posting the stolen data online when victims refuse to pay the ransom. Even providing payment is no guarantee against the data's publication.

Recommendations

5) **Insurance Coverage Review.** As noted above and based on the financial impact estimates in Appendices 3A and 3B, worst-case scenario financial impacts would exceed ICHC's cyber-insurance coverage in two specific areas.
    a. First, a regulatory penalty following a data breach could exceed the current coverage. Current regulatory penalty coverage is limited to $100,000. However, organizations of similar size to ICHC have received regulatory penalties of around $300,000. These financial penalties are issued for roughly 2% of major HIPAA data breaches.
    b. Second, business income losses following a catastrophic data loss scenario are estimated to exceed the existing coverage, which is limited to $100,000.

    In both cases, ICHC management may choose to accept the risk of losses greater than insurance coverage, may acquire increased insurance coverage, and/or may take further steps to reduce the likelihood of these scenarios occurring.
6) **Expand Telework Security.** Much of the world transitioned to telework over the last two months due to the COVID-19 pandemic, resulting in three overlapping challenges. First, organizations rapidly implemented and/or expanded remote work technologies. Often, and understandably, urgency of implementation resulted in imperfect security configuration. Second, employees were thrust into remote work situations without training in the additional considerations and security risks related to working from home. Third, criminal actors – seizing upon the increased volume of remote connections and employee emotional vulnerabilities related to the pandemic – launched widespread COVID-19 themed attacks including phishing, RDP attacks, and others. ***Brute force RDP attacks have increased 600% in the U.S. since the beginning of March***, according to a recent report from endpoint protection vendor Kaspersky.[1] Now, with the initial "reaction" phase past, organizations can and should revisit their telework security capabilities. Key safeguards to consider include:
    a. ***Physical Security of Home.*** Exterior doors and windows should be locked. For full-time home workers, a dedicated room for the home office is best. If there are other household members, such as children, a lockable door may be considered.

[1] "Remote spring: the rise of RDP bruteforce attacks," Kaspersky. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

For workers with highly sensitive information, such as senior leaders, home security systems should be considered.

b. ***Home Router Security.*** A checklist for router security should be employed. This may include minimum technical specifications for the router and/or a list of required models, changing default admin password, enabling two-factor authentication whenever possible, enabling WPA/2 encryption, selecting a secure DNS, and ensuring that firmware updates are applied.
c. ***Device Security.*** Security of laptops, smartphones, and even printers should be addressed. Mobile device management systems can be used to centrally manage and enforce secure configuration of both company-owned and employee-owned (BYOD) devices, including encryption. Security patches/updates should be applied. IT departments should evaluate risks of any solutions which require the employee to connect their device to the home office network for these updates to occur.
d. ***Data in Motion.*** Security of data in motion is a top concern. Potential security measures include requiring VPNs to connect to the home network and/or prohibiting the use of public Wi-Fi.
e. ***Data Protection.*** Safeguards to protect data include the use of an organization-approved and managed file sharing service, such as Box or Citrix Sharefile, prohibiting the use of personal file sharing services, such as Google Drive or Dropbox, and attending to backup if the employee's work involves files stored on the local device.
f. ***Paper Documents.*** Policies should specify standards for secure transport and storage of paper documents. A home office shredder should be considered if sensitive paper documents are used or created.
g. ***Household Members.*** Policies should prohibit household members from any inappropriate access to the organization's assets – computers, smartphones, or paper records.

Additional resources, including an industry best practice guide for telework network security, are available from the Eagle website.[2] See also Appendix 4 control 1150.

7) **Password Policies.** Password policies for ICHC systems and applications do not align with best practice recommendations. Especially because of the increased use of (and attacks on) remote network connections like VPN and external Remote Desktop access, we recommend establishing policies for stronger passwords. This should also include training staff in secure password creation, such as using 12+ character passwords and employing "passphrases" wherever possible. See Appendix 4 control 1430 and Appendix 6.
8) **Multifactor Authentication.** For the same reason strong password policies (above) are so important, we recommend implementing multifactor authentication (MFA, also known as two-factor authentication or 2FA) for the VPN, external Remote Desktop access, and Microsoft 365. Implementation of MFA is regularly cited by security professionals and penetration testers as the number one recommendation for reducing an organization's susceptibility to common attack methods such as phishing, brute force attacks, and other credential compromise methods. See Appendix 4 control 1430.
9) **Implement DNS Filtering.** Implement a DNS-based internet filtering service such as Cisco Umbrella, Webroot, WebTitan, or similar, to provide additional defenses against malware. This

[2] "Telework Security: Securing Home and Remote Workers," Eagle Consulting Partners. https://eagleconsultingpartners.com/general-news/telework-security/

is especially valuable in the current COVID-19 work-from-home situation as agency workstations are on unmanaged home networks and not protected by the agency firewall.

10) **Security Awareness Training.** Social engineering attacks on employees, such as phishing and business email compromise, are common forms of attack on organizations. Eagle tested ICHC staff through a simulated phishing attack and determined that **16% of employees clicked the link in the test phishing email**. Analysis of data breaches reported to HHS during 2019 indicated that 40% of incidents involved email in the attack chain vs. 13% during the previous 8 years. Security awareness training, which educates staff in recognizing and avoiding these online traps, is generally one of the most cost-effective security improvements an organization can take. We recommend ICHC implement a modern security awareness training program for all staff that incorporates the best practices from latest research and addresses practical skills necessary for effective security awareness. Such a program should:
    a. Include brief, engaging, relevant, and practical training modules delivered regularly throughout the year.
    b. Provide coverage of significant attack vectors that employees may experience, including phishing, spear phishing, drive-by downloads, business email compromise, and other methods of social engineering.
    c. Conduct regular assessment of employee knowledge through brief training quizzes/knowledge checks and through periodic phishing assessments.

    See additional information in Appendix 4 controls 1260 and 1265.
11) **Expanded, Outcomes-Driven IT Support.** ICHC's current IT support contract does not include a clear scope of work, delineation of responsibilities, SLAs, performance standards, etc. Additionally, Eagle identified confusion regarding responsibility for and frequency of key items such as server patching. Based on the information assets and infrastructure managed by ICHC, we recommend an IT support package with a clearly defined scope of work and appropriate SLAs. For example, scope and frequency of patching, of network configuration, of firewall management, of endpoint protection software and monitoring, of backup process management and verification, etc. This could be achieved through a different/expanded contract with Techwin or with another IT managed services provider. See Appendix 4 control 1110, 1731, and others.
12) **Telehealth Systems.** Due to rapid adoption of telehealth because of COVID-19, ICHC providers currently use multiple telehealth platforms for patient interactions. As of this assessment, none are explicitly managed by the organization, though we understand the organization to be reviewing Zoom. We strongly recommend ICHC consolidate all providers into a single telehealth solution for proper compliance and better management. Whatever platform is chosen, ICHC should establish a managed company account, provide appropriate access to providers & staff, and ensure a BAA is in place. Additionally, ICHC should implement best practice security configuration, including requiring meeting passwords and waiting rooms, and attending to secure delivery of access information to patents. See Appendix 6 and Appendix 4 control 1825.
13) **Patch Management.** Patch management is a challenge in any organization but tends to be even more prone to problems in organizations that rely on manual patching processes. Unpatched systems and applications create vulnerabilities to attack, and in many cases those vulnerabilities are being exploited "in the wild", i.e. attackers are actively exploiting the vulnerabilities. Currently at ICHC, workstations, servers, and network gear are patched through a combination of manual, on-site updates and some enabling of built-in auto-update features. ICHC has limited visibility or reporting capabilities into the patch status of its IT equipment, and Techwin was not able to provide Eagle with confirmation of the patch

status of all servers and network gear. Based on all of this, we have two recommendations for patch management:

a. **Explicit Patch Management Expectations and Monitoring for Techwin.** Extending recommendation #11 above, ICHC should define specific expectations for Techwin (or any other IT service provider) regarding the patching of servers and network gear, including the QNAP device. We recommend these expectations include monthly patching of all servers (including the firmware, operating systems, and applications), monthly review and firmware checks for all network gear, reporting and confirmation of patch status to ICHC monthly, alerting of ICHC when high priority or actively-exploited vulnerabilities are identified, and recommendations of off-cycle patching for high-priority vulnerabilities when appropriate.
b. **Automated Patching Tools for Workstations.** Particularly with more workstations off-site more frequently, ICHC can improve the ease and reliability of workstation patching by implementing a small-business-focused patch management application. These applications monitor workstations for patch level compliance, automate the process of applying Microsoft and 3rd-party patches, provide centralized reporting & validation, and in most cases will function even when workstations are not on the local ICHC network. Many of these applications have free or low-cost offerings for small businesses. Example SMB patch management applications include SolarWinds, Manage Engine, PDQ Deploy, and Itarian, among many others. Kaspersky SMB endpoint protection also includes a patching tool. After initial setup, an automated patch management tool would significantly reduce the time Dr. Browne spends manually patching workstations each month.

For more information, see Appendix 4 control 1731.

14) **Develop a Disaster Recovery Plan.** A Disaster Recovery Plan (DR Plan) is a written, detailed, and tested plan for restoring the IT capabilities and critical electronic information of an organization when a disaster scenario occurs. Specifically, a good DR Plan specifies the actions an organization will take prior to a disaster and the actions during and after the disaster to recover quickly. We recommend the Board develop a DR Plan which prepares for a variety of disaster scenarios from pandemic to natural disaster to ransomware corruption of the network. Documenting the efforts made and lessons learned from the current COVID-19 pandemic response would be a good place to start. See Appendix 4 control 1720 and 2210.
15) **Managed Security Services Provider and/or SOC.** Many of the recommendations in this list and priority items from Appendix 1 highlight a broad theme for the organization to implement more robust security-focused information system security monitoring capabilities. Based on our current understanding of the organization's systems, there is high probability that the organization would be unable to determine if an attacker were present in their infrastructure and/or if a breach had occurred. According to general cybersecurity research, it takes six months or more on average for most organizations to determine they've been breached. Often this discovery only happens because the organization is notified by law enforcement or some other third party. We recommend the agency consider proactive security monitoring by experts who can identify early warning signs and respond to security issues. This security management capability could be developed in-house, but for an organization of ICHC's size, generally the most efficient and effective solution is to partner with a specialized Managed Security Services Provider (MSSP) and/or Security Operations Center (SOC) company. MSSPs have the expertise, personnel, tools, and systems in place to

implement security monitoring effectively and with efficiencies of scale which would be difficult for the agency to achieve in-house. See Appendix 4 controls 1110 and 1760.

Additional recommendations and best practices are documented in Appendix 4 and elsewhere in the appendices to this report. These recommendations and best practices should be implemented to the extent practicable, prioritized based on the degree they would impact the organization's levels of information security risk.

Maturity of Security Controls

The security control maturity was assessed for ICHC using the CMMI Cybermaturity Model. Each of the control groups in the Controls Assessment Detail and Facility Security Review appendices were assessed using the 0 to 5 scale of CMMI. These rankings were then averaged for each of the ISO 27001 / 27002 Control Domains. See Appendix 2 for more detail and Appendix 4 for individual control maturity ratings.

About the Risk Assessment

Purpose and Scope

The purpose of this Risk Assessment is to determine the severity of threats to the confidentiality, integrity, and availability of electronic protected health information (PHI) maintained by Imaginary Community Health Center.

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. Conducting a Risk Assessment as required by §164.308(a)(1)(ii)(A) is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.

This Risk Assessment addresses the security of all electronic PHI (ePHI) used or maintained by ICHC. The scope includes all information systems which use ePHI, the list of which is detailed in the IT Asset Inventory. Consequently, this Risk Assessment meets HIPAA requirements.

Methodology

Eagle Consulting Partners used the methodology detailed in *NIST Special Publication 800-30 Risk Management* for this engagement. This Assessment is designed to address regulatory requirements of the federal HIPAA regulations and included a survey based on the 45 required controls specified in the HIPAA Security regulation. In addition, the Assessment explored the presence or absence of controls recommended by authoritative security frameworks, including ISO 27001/2 and the Center for Internet Security. To complete this Assessment, Eagle Consulting Partners:

1) Provided initial survey instruments which were completed by ICHC
2) Conducted telephone interviews with Bonnie Raitt, Executive Director, and Dr. Jackson Browne, HIPAA Security Officer.
3) Conducted a virtual review of the organization's facility and systems
4) Conducted additional interviews with the following:
    a. Neil Stephenson of Techwin Systems
5) Reviewed major attributes – including major security features, data characterization, and data quantification – for key information systems, including the electronic record software and other identified systems
6) Documented detailed findings and recommendations in the included appendices
7) Identified top findings for the Executive Summary of this report
8) Provided this report to ICHC and reviewed the findings with them

The Cybersecurity Threat Landscape

General Trends

The Threat is Real, The Numbers are Staggering: "In the last eight years, more than seven billion online identities have been stolen in data breaches, which is almost the equivalent of one for every person on the planet."[3]

Financial Impact of Cyberattacks: "The fear of breaches is founded in the financial cost of attacks, which is no longer a hypothetical number. Breaches cause real economic damage to organizations, damage that can take months or years to resolve. … More than half (53 percent)

[3] Symantec, Internet Security Threat Report, Vol. 22, April 2017.

of all attacks resulted in financial damages of more than US$500,000, including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs."[4]

Evolving Threat Actors: In addition to the threats from insiders and criminal groups, attacks from nation-states and state-sponsored hackers are affecting hundreds of thousands of people across the globe.

Ransomware: "Ransomware attacks, in which hackers encrypt an organization's vital data until a ransom is paid, have become a billion-dollar cybercrime industry according to the FBI. Ransomware is now widely seen as the single biggest cybersecurity threat to both business and government organizations."[5]

Phishing: Starting in 2016, malicious phishing emails have become "the weapon of choice for a wide range of cyber-attacks, … used by everyone from state-sponsored cyber espionage groups to mass-mailing ransomware gangs." [6]

Cloud and IoT: IT Security Teams struggle to adapt to these emerging environments and keep up with their accelerating growth.

Healthcare Trends

"Healthcare records contain some of the most detailed personal information available, and healthcare organizations are not doing enough to protect this information."[7]

Cyberattacks on healthcare providers increased significantly in 2016 and continue to increase through the present. According to the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, in 2016 there were 327 reported healthcare breaches of over 500 individuals; 359 breaches in 2017; 366 breaches in 2018; and 430 reported so far in 2019[8]

Drilling into the 2019 data breaches reveals the following statistics, major trends are an increase in hacking incidents, with involvement of email and network servers. More specifically, based on the 2019 HHS-reported data breaches so far, compared to the average from the previous 8-year period:

Based on asset involved in the attack chain, we have the following:

- 40% involved email, compared to 13%
- Network server breaches slightly increased, from 16% to 22%
- Laptop-related breaches are down sharply, from 12% to 3%
- Desktop-related breaches are down from 6% to 3%

When evaluating the mechanism of breach, we see:

- Hacking/IT incidents represent most, 57%, up sharply from 22%
- Unauthorized access is steady at 30% for 2018, versus 28%
- Theft is down significantly, from 33% to only 7%.
- Improper disposal is a small factor, only 1% in 2019, down from 3%

---

[4] Cisco, 2018 Annual Cybersecurity Report.
[5] AlienVault, 2017 Ransomware Report.
[6] Symantec, Internet Security Threat Report, Vol. 22, April 2017.
[7] SecurityScorecard, 2018 Healthcare report: A Pulse on the Healthcare Industry's Cybersecurity Risks.
[8] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Major findings from recent healthcare cybersecurity studies further outline the healthcare industry's cybersecurity weaknesses:

1) Healthcare is one of the lowest-ranked U.S. industries in terms of cybersecurity.
2) "Healthcare organizations overall have struggled to keep up with growing cybersecurity demands and have increasingly fallen victim to sophisticated attackers."[9]
3) Over half of all healthcare breaches involved insiders – the only industry where this was the case.
4) "Basic security measures are still not being implemented. Lost and stolen laptops with unencrypted PHI continue to be the cause of breach notifications." [10]
5) "Healthcare organizations, even top performers, struggled with patching cadence and network security." [11]

Compounding these issues is the fact that healthcare companies are not spending enough on security, averaging just 3 percent of their IT budgets. For comparison, the average for the finance industry is 10-12 percent of IT budget. The combination of extensive private data and an inadequate security focus has made healthcare organizations attractive targets for attackers and, all too often, victims of their own errors.

HIPAA Enforcement

The Federal HHS Office of Civil Rights (OCR), along with State Attorneys General, handle enforcement of the HIPAA regulations. Effective in 2009, the HITECH Act increased financial penalties for HIPAA violations dramatically: per-incident violations increased from $100 to as much as $50,000; annual incident-type maximums increased from $250,000 to $1.5 million.

HIPAA Enforcement Continues under Trump. While President Trump has widely communicated his dislike for regulations, HIPAA enforcement under his administration has continued at a steady pace, and even hit a new record in 2018 with $28.7M in settlements and penalties:

Year	Total Actions	Total Fines	Average Fine
2019	11	$15.3 million	$1.4 million
2018	10	$28.7 million	$2.9 million
2017	10	$19.4 million	$1.9 million
2016	13	$23.5 million	$1.8 million
2015	6	$6.2 million	$1 million

Right of Access Initiative. The Trump Administration began in 2019 its "Right of Access" Initiative. The HIPAA Privacy regulation guarantees patients the right of access to their records, including access in electronic formats. While HIPAA Privacy is not in scope of the Security Risk Assessment, we note that in 2019 there were two settlements, both for $85,000, for failures of health providers

[9] SecurityScorecard, 2018 Healthcare report: A Pulse on the Healthcare Industry's Cybersecurity Risks.
[10] Verizon, 2018 Protected Health Information Data Breach Investigations Report.
[11] SecurityScorecard, 2018 Healthcare report: A Pulse on the Healthcare Industry's Cybersecurity Risks.

to provide timely right of access to their records and/or in the electronic format that they preferred.

Ongoing Emphasis on Risk Assessment and Risk Management. In its frequent public statements about enforcement, OCR repeatedly and continually emphasizes the importance of the Security Risk Assessment as the foundation of an effective compliance program.

Other Enforcement Actions. State attorneys general have increased HIPAA enforcement actions, including a 16-state settlement in June of 2019 with Medical Informatics Engineering for $900,000 relating to a 2015 data breach affecting 3.9 million individuals. Data breach victims also employ class-action lawsuits against healthcare organizations for harm caused by data breaches. In 2019, Banner Health settled a class action lawsuit for $6M to resolve claims of 2.6 million patients affected by a 2016 data breach. In 2018, Aetna settled a class-action lawsuit for $17.1 million after a Business Associate inappropriately disclosed the HIV status of thousands of individuals.

Threat Actors

Insider Threats

"Security is all about people, and people are often the weakest element."
Martin Holste, FireEye Chief Technology Officer for Cloud

Insiders are responsible for over a quarter of recent data breaches across all industries. In healthcare, insiders cause over half of the data breaches – the only industry in which this is the case. Of these insider threats, the largest percentage come from non-malicious insider error, including misdelivery of both paper and electronic PHI, disposal errors, loss, publishing errors, and database misconfigurations.

Malicious insider incidents, though less common than errors, should be an equally significant concern within organizations. Motives behind these incidents range from inappropriate curiosity to financial, grudge, or espionage-driven reasons. "Regardless of the motivation of the actor, over 80% of incidents are comprised of people simply utilizing established logical (privilege abuse 66%) or physical (possession abuse 17%) access to sensitive data in an unauthorized manner."[12] These results emphasize the importance of core principles such as physical asset management controls, minimum-use access privileges, and regular internal auditing.

Cyber Criminals

Cyber criminals outside of organizations account for almost three quarters of recent breaches across all industries. These criminals fall into three broad categories. Organized cyber-crime groups represent the largest category, responsible for around half of all recent breaches. These groups carry out a wide variety of primarily financially motivated attacks, including large-scale email malware/ransomware attacks and sophisticated financial heists.

Nation-states, primarily Russia and North Korea, and state-sponsored hackers are responsible for a growing number of attacks and breaches – around 12% as of recent reports. Motivations include espionage, political disruption, and financial gain. Recent high-profile attacks include:

1) The compromise of Hilary Clinton campaign manager John Podesta's email during the 2016 U.S. Presidential Campaign. (Russia)

[12] Verizon, 2018 Protected Health Information Data Breach Investigations Report.

2) The WannaCry ransomware that affected over 300,000 computers in 150 countries in May 2017. (North Korea)
3) The June 2017 NotPetya data destroyer disguised as ransomware, which primarily targeted Ukraine's infrastructure but also spread globally and caused over $1.2 billion in damages. (Russia)
4) The cyberattack on the 2018 Winter Olympics opening ceremonies. (Russia)
5) The long-term hack of Starwood Hotels (acquired by Marriott in 2015) and breach of information on 500 million guests from 2014-2018. (China suspected)[13]

The third category of criminal threats is opportunistic hackers. These individuals or smaller-scale groups execute attacks for a wide variety of reasons, from malicious enjoyment, to "hacktivism," to financial gain.

Common Vulnerability Areas

Ransomware

Ransomware is the fastest-growing cyber threat in recent years, with names such as WannaCry and Petya now reaching public attention. One in three organizations has experienced a ransomware attack, and over 85 percent of all malware attacking healthcare organizations is ransomware. Ransomware attacks are easy and inexpensive for criminals to launch. By relying on email, phishing, and social engineering for delivery, ransomware avoids many network security protections. Furthermore, organization size has little impact on ransomware risk. As an example, in late 2017 we at Eagle Consulting Partners worked with a small doctor's office whose electronic medical records server had been encrypted by ransomware. Shortly thereafter, in January 2018, EHR vendor Allscripts was also infected with ransomware, crippling many of their customers for the better part of a week.

Most ransomware infections start via email attachments, phishing, or users accessing malicious websites. The most important protections against ransomware are quality user-awareness training, effective endpoint security, and rapid patching regimens. Data backup and recovery systems are the only reliable means of recovering from a ransomware attack.

Phishing & Social Engineering

Phishing and other email-delivered attacks have grown rapidly over the last few years, in part because email "doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials." Furthermore, "targeted spear-phishing campaigns, especially in the form of Business Email Compromise (BEC) scams, rather than the mass-mailing phishing campaigns of old, are now favored by attackers."[14] The FBI estimates that over 7,400 businesses are targeted daily by spear-phishing and BEC emails, resulting in losses over $3 billion.

Although technical security controls are important to combat phishing and social engineering attempts, regular and ongoing end-user training remains the most important and effective protection against these attacks.

---

[13] See https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/ and https://bgr.com/2018/12/12/china-hack-marriott-state-security-ministry/.
[14] Symantec, Internet Security Threat Report, Vol. 22, April 2017.

Cloud

The rapid growth in use of cloud technologies has resulted in significant vulnerabilities for organizations. Most have limited understanding of what cloud applications are being used by their employees. According to recent analysis by Symantec, "most CIOs think their organizations only use around 30 or 40 cloud apps" yet the real number is closer to 1,000. [15] Over two-thirds of an organization's information in the cloud is "shadow data," unknown to management and IT, and of that data, 25 percent is "'broadly shared,' meaning it is shared internally, externally, and/or with the public."

Not surprisingly, IT security teams "are having difficulty defending evolving and expanding cloud and IoT environments. One reason is the lack of clarity around who exactly is responsible for protecting those environments."[16] One of the most important cloud security controls an organization can take is to "implement smart data governance practices in your business so that you know what business data is being stored on cloud services."[17] This is best done through a combination of policy, user training, technical controls, and ongoing monitoring.

Internet of Things (IoT)

The Internet of Things, like the cloud, is a significant vulnerability area that organizations struggle to manage. The number of IoT devices has exploded in recent years to over 20 billion devices. In most attack cases, IoT devices are networked to create massive botnets that then conduct other attacks. Mirai in 2016, Reaper in 2017, and others like them have infected and repurposed hundreds of thousands of IoT devices globally to engage in distributed denial-of-service (DDoS) attacks that have taken down websites, including Netflix and Twitter. Vulnerable IoT devices can also allow malicious hackers to penetrate deeper into an organization's network, as in the case of the casino whose high-roller database was stolen via the lobby fish tank's internet-connected thermometer.

Security is not a manufacturer priority for most of these IoT devices. Firmware updates are infrequent, rarely easy to install, and almost never automatic. Few users change default usernames and passwords. Users generally forget about the devices once installed and fail to perform any patching or upkeep. Four out of five IoT devices are not patched against common vulnerabilities, according to a recent study. Finally, IoT devices are frequently procured and installed without the knowledge of an organization's IT department. IT security teams should audit their network for IoT devices, update device credentials, track the devices in IT asset management and patching/maintenance programs, use strong wifi encryption and/or hardwire the devices where possible, and use other hardening techniques.

Business Associates

Organizations also need to pay attention to vulnerabilities present in their HIPAA Business Associates. Based on recent data, almost one in five breaches was reported by or involved a Business Associate or third party. Third parties are vulnerable to all the other items described in this report, yet an organization has limited visibility or control of a third party's information security protocols without engaging in intentional due-diligence processes with its existing and potential Business Associates. Ultimately, "healthcare organizations who leverage third-party providers also

[15] Symantec, Internet Security Threat Report, Vol. 22, April 2017.
[16] Cisco, 2018 Annual Cybersecurity Report.
[17] Symantec, Internet Security Threat Report, Vol. 22, April 2017.

need to vigilantly monitor the security posture of these vendors and partners to limit exposure and ensure compliance."[18]

KEY TAKEAWAYS

Integrated Security Management Approach (People + Policies + Technology): Information security must be treated as a core business area – and risk – by organization management. It cannot be isolated to the IT department. Security-aware organizations will take an integrated approach to security management that includes a combination of intelligent policies, secure technology practices, and conscientious, well-informed staff. Within this environment, IT teams must shift perspective beyond physical infrastructure to all business-critical systems and data, wherever they may be.

Personnel Training: Regular training for staff is an important part of preventing PHI-handling errors and reducing computer vulnerabilities. All providers and staff should understand their responsibilities under the HIPAA Privacy, Security, and Breach Notification rules, including practical examples of inappropriate behaviors and possible corrective actions. They should also be familiar with safe computer practice, including safe web browsing, responsible email use, recognizing phishing and social engineering, password security, and responding to malware attacks. We recommend HIPAA and computer security trainings be conducted annually at minimum, with quarterly refresher training and discussions.

Complete Environment Visibility: IT security teams must have a thorough inventory of all information assets, systems, and data locations, especially including all cloud applications, IoT devices, and shadow data. Complete visibility also involves understanding the security of any Business Associates, what systems they access, what information they have, and how they protect it.

Importance of Basic Network Security Best Practices: The basics still matter. All workstations, servers, mobile devices, and NAS should have full disk encryption. The importance of regular patching of all systems and assets cannot be overstated. Networks should be appropriately segmented, and data isolated to limit access and provide resilience in case of penetration, ransomware, or other attack. Business-critical systems and data should be backed up to multiple locations with appropriate backup retention schedules. Restoration procedures, incident response plans, and disaster recovery plans should all be tested regularly, at least annually.

Security Monitoring: Organizations should regularly monitor access to protected information, as well as the health and status of the network and all endpoints. They should also conduct periodic technical assessments as appropriate to their size and circumstances, such as vulnerability scans and penetration testing. Ongoing monitoring of Business Associate security is another important aspect of this recommendation.

[18] SecurityScorecard, 2018 Healthcare report: A Pulse on the Healthcare Industry's Cybersecurity Risks.

REFERENCES

- AlienVault, 2017 Ransomware Report.
- BGR, "Authorities think agents from China's Ministry of State Security hacked Marriott," 12/12/2018. https://bgr.com/2018/12/12/china-hack-marriott-state-security-ministry/.
- Business Insider, "Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank," 4/15/2018. https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4.
- Cisco, 2018 Annual Cybersecurity Report.
- FireEye, Looking Ahead: Cyber Security in 2018.
- Healthcare Informatics, "Risk Management is Maturing, But Cybersecurity Gaps Still Loom, Report Finds," 3/2/2018. https://www.healthcare-informatics.com/news-item/cybersecurity/risk-management-maturing-cybersecurity-gaps-still-loom-report-finds.
- HIPAA Journal, "Aetna Settles Class Action Lawsuit Filed by Victims of HIV Status Data Breach," 1/18/2018. https://www.hipaajournal.com/aetna-settles-class-action-lawsuit-filed-victims-hiv-status-data-breach/.
- Krebs on Security, "Marriott: Data on 500 Million Guests Stolen in 4-Year Breach," 11/30/2018. https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/.
- Protenus, 2017 Breach Barometer Annual Report.
- SecurityScorecard, 2018 Healthcare Report: A Pulse on the Healthcare Industry's Cybersecurity Risks.
- Symantec, Internet Security Threat Report, Vol. 22, April 2017.
- Verizon, 2018 Data Breach Investigations Report.
- Verizon, 2018 Protected Health Information Data Breach Investigations Report.
- The Washington Free Beacon, "White House: Russia's Cyber Attack on Ukraine Most 'Destructive and Costly' in History," 2/15/2018. http://freebeacon.com/national-security/white-house-russias-attack-ukraine-destructive-costly-cyber-attack-history/.

Risk Register - *A Summary Analysis and Prioritization of Potential Loss Event Scenarios*

Organizational Risk Tolerance	
Maximum Capacity for Loss	**$2,000,000**

RISK RATING SCALE		
(5) Critical	*Greater than*	$2,000,000
(4) Very High	*Up to*	$2,000,000
(3) High	*Up to*	$1,000,000
(2) Medium	*Up to*	$500,000
(1) Low	*Up to*	$100,000
(0) Very Low	*Less Than*	$20,000

Key Term	Definition
Risk	A measurement of the probable frequency and probably magnitude of future loss.
Loss Event Scenario	The scenario which would result in financial loss if it occurred. Includes the asset at risk, the threat, and the effect.
Single Event Loss	Estimates of the financial losses if the Loss Event Scenario were to occur.
Threat Event Frequency	The estimated number of times that the organization experiences an attempt by a threat to cause a loss.
Effectiveness of Controls	Estimate of effectiveness of existing controls in preventing a threat event from becoming a loss and/or reducing the impact of the loss.
Annualized Loss Expectancy	The range of expected financial losses from a scenario over a one-year period. A quantitative expression of risk.
Risk Rating	A qualitative assessment of the average Annualized Loss Expectancy based on the organization's risk tolerance.

ID	Loss Event Scenario	Asset at Risk	Effect	Single Event Loss LOW ESTIMATE	Single Event Loss HIGH ESTIMATE	Threat Event Frequency	Effectiveness of Controls	Annualized Loss Expectancy	Risk Rating	Significant Risk Factors and Relevant Controls:
001	Breach of EHR Databases by malicious external actors	Allscripts & DentalEHR databases	Confidentiality	$65,000	$420,000	Low (Between once every 10 years and 1 time per year)	50%	$3,300 to $210,000	(2) Medium	1) Remote network access & authentication, including password strength and 2-factor auth (1430, 1150) 2) Employee security & phishing awareness (1265) 3) IT security responsibilities and accountability (1110, 1731) 4) Network security monitoring (1760)
002	Loss/Destruction of data in EHR Databases for any reason	Allscripts & DentalEHR databases	Availability	$290,000	$415,000	Low (Between once every 10 years and 1 time per year)	75%	$7,300 to $100,000	(1) Low	1) All listed for scenario 001, plus 2) Backup validation, disaster recovery planning and testing (1720, 2210)
003	Extended outage of ICHC Network or EHR systems for any reason	Network, including all hosted applications	Availability	$880	$4,000	Moderate (Between 1 and 10 times per year)	25%	$650 to $30,000	(0) Very Low	1) Same as scenario 002
004	Breach of PatientIntake by malicious external actors	PatientIntake Data / content of Allscripts Database	Confidentiality	$65,000	$260,000	Low (Between once every 10 years and 1 time per year)	50%	$3,300 to $130,000	(1) Low	1) Authentication, including password strength and 2-factor auth (1430)
005	Confidentiality breach of telehealth systems due to lack of centralized management and/or improper configuration and use	Zoom, Doxy.me, Doximity	Confidentiality	$10,000	$300,000	Low (Between once every 10 years and 1 time per year)	50%	$500 to $150,000	(1) Low	1) Multiple unmanaged telehealth systems in use (see notes in Appendix 6) 2) Authentication, including password strength and 2-factor auth (1430) 3) Considerations for patient texting and emailing of telehealth meeting info (1825)
006	Ransomware infection of the local network, resulting in both data breach and extended network downtime	Network, including all hosted applications	Any/Multiple	$100,000	$450,000	Low (Between once every 10 years and 1 time per year)	75%	$2,500 to $110,000	(1) Low	1) All listed for scenarios 001 and 002.

Security Control Maturity Ratings

Security Controls Domain	Current Maturity
Information Security Policies	3
Organization of Information Security	1.5
Human Resources Security	1.7
Asset Management	1.8
Access Control	1.7
Cryptography	2
Physical and Environmental Security	1.3
Operational Security	1.1
Communications Security	1.2
System Acquisition, Development, and Maintenance	N/A
Supplier Relationships	1.5
Incident Management	1
Business Continuity Management	0
Compliance	2.5

Security control maturity was assessed using the CMMI Cybermaturity Model. Each of the control groups in the Controls Assessment Detail and Facility Security Review appendices were assessed using the 0 to 5 scale of CMMI. These rankings were then averaged for each of the ISO 27001 / 27002 Control Domains.

The CMMI Cybermaturity Model is available at https://cmmiinstitute.com/getattachment/439bd454-ccfe-4285-9407-e7f7a48d810d/attachment.aspx.

CMMI Cybermaturity Ratings	
0: Incomplete	Control activity is ad hoc, unknown, or nonexistent.
1: Initial	GENERAL: Represents a minimum standard of care. Basic functions may be performed. These functions are performed informally and may not be prioritized commensurate with risk. PEOPLE: General personnel capabilities may be performed by an individual, but are not well defined PROCESS: General process capabilities may be performed by an individual, but are not well defined TECHNOLOGY: General technical mechanisms are in place and may be used by an individual
2: Managed	GENERAL: Basic functions are achieved with relative consistency. Subset of the organization has developed plan, but formal organization strategy or documented plan has not been developed. PEOPLE: Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization PROCESS: Adequate procedures documented within a subset of the organization TECHNOLOGY: Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place
3: Defined	GENERAL: Formal plans and strategies define the consistent achievement of functions across the organization. Lagging indicators provide understanding of the work performed. PEOPLE: Roles and responsibilities are identified, assigned, and trained across the organization PROCESS: Organizational policies and procedures are defined and standardized. Policies and procedures support the TECHNOLOGY: Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization
4: Quantitatively Managed	GENERAL: Achievement of outcomes is measured and reported. Leading indicators contribute to proactive risk management and continual improvement PEOPLE: Achievement and performance of personnel practices are predicted, measured, and evaluated PROCESS: Policy compliance is measured and enforced. Procedures are monitored for effectiveness. TECHNOLOGY: Effectiveness of technical mechanisms are predicted, measured, and evaluated
5: Optimized	GENERAL: Mechanisms for outcome achievement are integrated into organizational activities PEOPLE: Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external) PROCESS: Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured. TECHNOLOGY: Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

Financial Impact of a Major Breach

ASSUMPTIONS:	
Number of Patients in Allscripts	**7500**
Number of Patients in DentalEHR	**3100**
% of DentalEHR patients also in Allscripts	**25%**
Cost of Mitigation Offer (per individual):	**$10**
Percent accepting mitigation offer:	**10%**

ESTIMATE OF RECORDS BREACHED		Low Estimate	High Estimate
	Based on the variety of systems and their relative number of records per system, a major system compromise could result in a data breach of a range of records across one or more systems.	**7,500**	**9,825**

INTERNAL COSTS:		Low Estimate	High Estimate
Legal and Consulting Fees	Cost to investigate a breach, review federal and state legal requirements, conduct required "risk of harm" test, provide PR advice and handle required regulatory filings. Outside forensic investigators may be required.	$50,000	$100,000
Mandated breach notification	Letter to all individuals , including letter, envelope, first class postage and labor (Assume $1.00/letter)	$7,500	$9,825
Mitigation	HIPAA Privacy requires covered entities to mitigate the damages caused by breaches. The customer must decide how to mitigate -- no specific mitigation is prescribed. Many organizations choose to offer one year of identity theft protection to all affected adult individuals. Estimation formula: *Number of Individuals in System* *x Cost of Mitigation Offer* *x % of Individuals who Accept Mitigation Offer* ---------- *= Estimated Mitigation Cost*	$7,500	$9,825
ESTIMATED TOTAL BREACH RESPONSE COST:		***$65,000***	***$120,000***

ADDITIONAL FINANCIAL IMPACTS		Low Estimate	High Estimate
Regulatory Penalties	Estimated 2% Risk of HIPAA penalties (based on enforcement actions to date in major breach cases). Penalties have ranged from $35K to $16M, and generally include a costly 3-year compliance agreement. For an organization of this size, we estimate $300K worst case scenario, including both a negotiated settlement amount plus costs of a compliance agreement.	$35,000	$300,000
Reputation Damage	Some damage to reputation is expected although difficult to quantify in dollar terms	Not Quantified	Not Quantified
ESTIMATED ADDITIONAL FINANCIAL IMPACTS:		***$35,000***	***$300,000***
ESTIMATED TOTAL FINANCIAL IMPACT OF MAJOR BREACH:		**$100,000**	**$420,000**

Financial Impacts of Downtime and Data Loss

ASSUMPTIONS:	
Annual Revenue:	**$4,400,000**
Accounts Receivable:	**$300,000**
Annual Cost of Admin Staff Person:	**$40,000**
Number of Admin Staff	**5**

AMOUNT OF DOWNTIME:	IMPACTS:	LOW ESTIMATE	HIGH ESTIMATE
1 Hour of Downtime	1) Schedule delay for remainder of day 2) Minimal financial impact	Minimal	Minimal
1 Day of Downtime	1) Significant disruption of operations 2) Estimated 5-15% fewer patients seen 3) Clinical staff would handwrite notes which would need to be keyed in later	$880	$2,640
1 Week of Downtime	1) Estimated 10-20% reduction in patient volume due to operational problems	$800	$2,400
	2) 30-40% productivity loss of administrative staff; Unpaid overtime/life disruption for physicians	$1,200	$1,600
	3) Other operational disruption - temporary delays in collection, some cash flow impact		
	4) Some minor clinical impact due to unavailability of patient chart		
	5) Reputation damage		
	Estimated Financial Cost of 1 Week of Downtime:	**$2,000**	**$4,000**

DATA LOST FOREVER:	IMPACTS:	LOW ESTIMATE	HIGH ESTIMATE
	1) Loss of 25-33% of Accounts Receivable	$75,000	$99,000
	2) 25% reduction in monthly billing for 2-3 months due to multiple operational problems while systems are rebuilt.	$183,000	$275,000
	3) Additional staff costs for rebuilding patient record database. Assume 1 additional person for 9 to 12 months.	$30,000	$40,000
	4) Cash Flow Disruption. Delay in billing of 4-6 weeks following the disaster, resulting in a corresponding delay in collections.	$350,000	$530,000
	5) Reputation damage	Not Quantified	Not Quantified
	ESTIMATED FINANCIAL LOSS:	**$290,000**	**$415,000**
	ESTIMATED CASH FLOW DISRUPTION:	**$350,000**	**$530,000**

Controls Assessment Detail *Review of Security Controls Implementation and Maturity*					
Control #	**Control Title**	**Control Description**	**Existing Controls and Comments**	**Maturity Level**	**Additional Resources**
1000	**DOMAIN: INFORMATION SECURITY POLICIES**	**Controls For The Writing And Review Of Policies**			
1010	**Information Security Policies**	1) Information security policies are created to address compliance with the HIPAA Security regulations and security best practices articulated in authoritative security frameworks such as NIST, CIS, OWASP, and ISO 27001/2. 2) Policies are approved by management and/or the board. 3) All employees are trained and sign-off that they understand and will follow policies. 4) Management and the board demonstrate a commitment to information security through allocation of management time and budget.	1) Comprehensive policies: Yes. HIPAA Privacy and Security Policies created and periodically revised by Eagle. 2) Management approval: Yes. All policies are approved by management and the board of directors. 3) Employee sign-off: Yes. For new hires and whenever substantive changes are made to policies.	3: Defined	
1100	**DOMAIN: ORGANIZATION OF INFORMATION SECURITY**	**Controls For Assignment Of Responsibilities, Including Management Of Mobile Devices And Teleworking**			
1110	**Security Responsibilities**	All information security responsibilities are clearly documented: 1) An Information Security Officer is named, 2) Job duties are documented in job description 3) The scope of the security duties includes both technical and people/process matters. 4) The security officer may delegate and/or use contractors to complete these duties.	1) Information Security Officer: Dr. Jackson Browne 2) Job Description includes information security responsibilities. 3) Authority is appropriate. 4) Aspects of information security responsibilities are outsourced to Techwin Systems, who manages network, firewall, backups, and antivirus/antimalware software. 5) The contract with Techwin is for a fixed number of hours of on-site support from a network adminsitrator. The most recent contract has conflicting information whether 4 or 8 hours of support per month are included. 6) The Techwin contract includes suggested on-site activities but does not include a clear scope of work, delineation of responsibilities, SLAs, performance standards, etc.. Additionally, neither the Trend Micro antivirus nor the Azure cloud backup storage, both services apparently provided by Techwin, are documented in the contract. Recommendation: Based on the information assets and infrastructure managed by ICHC, we recommend an IT support package with a clearly defined scope of work with appropriate SLAs. For example, scope and frequency of patching, of network configuration, of firewall management, of endpoint protection software and monitoring, of backup process management and verification, etc. This could be achieved through a different/expanded contract with Techwin or with another IT managed services provider.	3: Defined	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1120	**Risk Assessment**	Risk assessments are conducted to identify, quantify, prioritize, and manage risks. The prioritization is accomplished by identifying actions which provide the greatest benefit in reducing overall risk. Risk assessment should be formalized and ongoing. Individuals who need to act on the risk assessment are given access to, and they review, the risk assessment findings.	1) Eagle has conducted multiple previous security risk assessments for the organization. 2) This 2020 assessment is a comprehensive analysis of the organization.	2: Managed	
1130	**Risk Management**	1) Organizations systematically manage risks and document management actions via formal processes. Risk management is performed either by reducing the risk, transferring the risk, or accepting the risk. 2) Organizations establish risk tolerances and manage any excess risk by transferring risks that exceed the risk tolerance. Security risks can be transferred with: a) Business interruption insurance to protect against system downtime, data corruption, data loss, personnel loss, or other business continuity failure b) Data Breach Insurance to protect against data breach costs, including costs of investigation, remediation, mitigation, and potential regulatory penalties c) Employee Dishonesty Insurance to protect against insider threats Alternately, risks can be transferred contractually through outsourcing arrangements.	1) Risk management process: Yes. The organization has contracted Eagle for risk management support. 2) Insurance: Yes. $2 million for both single and aggregate, including: a) $250k for Forensic IT review b) $250k for Legal review c) $250k for regulatory fines & penalties d) Service to affected individuals (notification, credit monitoring, help line) - up to the plan limit e) Computer attack response - up to the plan limit f) $100k business income loss g) $100k data recreation h) $1M Cyber extortion (e.g. ransomware) 3) Based on the financial impacts estimated in Appendices 3A and 3B: a) A regulatory penalty following a data breach could exceed the current coverage. b) In a data loss scenario, business income losses are estimated to exceed existing coverage.	1: Initial	
1140	**Separation Of Duties**	Best practice is to have one individual (or vendor) implement and manage the computer system, and a separate individual (or vendor) to validate that appropriate security is in place.	1) This risk analysis is conducted by a company different from the company implementing/managing the network, which provides an appropriate "separation of duties".	2: Managed	
1150	**Remote Worker Policies**	Appropriate policies are used for remote workers, including: 1) Clear instructions regarding the use or prohibition of using personally-owned equipment such as home computers 2) Established procedures and training for secure remote connection to the organization's network 3) Policies regarding physical security of equipment in an employee's home 4) Clear policies and training regarding the secure use of mobile devices	1) Due to COVID-19, the organization has increased use of staff work-from-home. All staff are on-site at least one day per week. 2) The global increase in remote work arrangements has led to a significant increase in cyberattacks targeting remote workers, VPNs, RDP connections, and using COVID-19 / coronavirus themes. 3) Employee home networks are unmanaged by the agency and likely have weak security as compared to the organization's internal network. 4) It is likely that a significant number of employees are increasing personal usage of their company laptops and/or are allowing others in the household to use the company laptop as well.	1: Initial	1) Telework Securely: Securing Home and Remote Workers. https://eagleconsultingpartners.com/general-news/telework-security/

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1160	**Mobile Device Management**	Best practices are employed to manage mobile devices, including: 1) Use of a mobile device management system, which enforces security controls, including: a) Encryption of mobile device hard drive/memory with appropriate key management b) Remote location and remote wiping c) Strong authentication, such as a certificate c) Enforcement of secure configuration d) In BYOD environments, separation of personal and business data 2) Policies and procedures which detail technical management processes 3) Policies and procedures for end-users which clearly specify their responsibilities, appropriate for the environment (BYOD or organization-owned devices) 4) A strong user agreement, including that addresses BYOD and/or organization-owned devices	1) By policy, company PCs are required to access the organization's network and assets. 2) No technical measures were identified which would prevent non-company-managed devices to connect to the organization's network or assets, e.g. over VPN or RDP. Username and password are all that is required. Example of asset-level restrictions would be use of device certificates.	0: Incomplete	1) Telework Securely: Securing Home and Remote Workers. https://eagleconsultingpartners.com/general-news/telework-security/
1200	**DOMAIN: HUMAN RESOURCES SECURITY**	**Controls For Prior To, During, And After Employment**			
1220	**Background Checks**	1) Background checks are performed on all candidates for employment and contractors based on business requirements and in accordance with relevant laws, regulations, and ethics. 2) Special attention is given to users who will have a high level of access to information systems, e.g. system administrators. a) Criminal background screening b) Credit check 3) For healthcare organizations, the National Practitioner Data Bank Continuous Query is used for all applicable staff.	1) A background check process is in place, including drug screens and physicals.	3: Defined	
1230	**Employment Agreements**	Employment agreements and/or other written agreements are in place with employees, contractors, and other third-party users in which they agree to the terms and conditions of computer system use and their responsibilities for information security.	1) HIPAA Policies include an "Acknowledgement of HIPAA Policies and Procedures" sign-off; this was implemented 4/1/2015; signed statement kept in employee files. 2) Policies were updated in 2018. 3) It is not known if all employees have signed acknowledgement forms and/or reviewed the 2018 policy updates. **Recommendation:** Ensure all staff have reviewed updated policies and that signed acknowledgement forms are on file.	1: Initial	
1250	**Policies And Procedures Training**	A training curriculum for employees has been established to educate and train users in the organization's policies and procedures. This curriculum includes periodic, ongoing reminders.	1) Eagle provided HIPAA policies training materials to ICHC in 2015 for ongoing use.	2: Managed	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1260	**Security Awareness Training**	1) A security awareness training curriculum for employees has been established to educate and train users regarding: a) The secure usage of applications, internet, email, and other technology solutions b) Safe web browsing, safe email practices, and protecting against social engineering. c) Common threat actors and attack methods 2) The training curriculum is ongoing throughout the year, including a comprehensive annual training session and brief monthly or quarterly "refresher training" on relevant topics.	1) A security awareness presentation is provided to all staff periodically by Eagle. 2) Ongoing training throughout the year is not used.	1: Initial	1) Eagle Security Awareness Training: https://eagleconsultingpartners.com/security-awareness-training/ 2) CIS Control 17: https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/
1265	**Security Awareness Evaluation**	1) Employee security knowledge and behavior is evaluated to identify and score employee security posture. For example: a) Comprehension checks following training sessions b) Periodic simulated phishing attacks. 2) Corrective action is taken to educate employees with weak security skills.	1) A simulated phishing attack was conducted as part of this assessment. 2) The test resulted in a 16% failure rate, with 3 of 19 employees clicking the phishing link. 3) ICHC does not conduct periodic security knowledge and behavior evaluations (other than the one-time assessment above). 4) If the simulation had been real, the clicked links could have resulted in ransomware or other malware being downloaded onto the network or compromise of user credentials. 5) Phishing and related social engineering techniques are one of the most common methods used by attackers to gain access to networks and critical systems. 6) Effective ongoing training can reduce the average phishing failure rate to around 3% or less. Recommendation: Implement ongoing security awareness training which includes regular evaluation components including simulated phishing assessments.	0: Incomplete	
1270	**Termination Procedures**	Employee termination procedures are in place clearly defining responsibilities and processes for termination. These procedures include: 1) Return of assets, such as smartphones, laptop computers, and keys. 2) Access privileges to application systems are revoked in a timely process. Separately, procedures are in place to manage termination of contractors and other third parties who may have access privileges to IT systems.	1) Employee termination is covered under policy 3010 and includes appropriate procedures to retain equipment and disable systems access.	3: Defined	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1300	**DOMAIN: ASSET MANAGEMENT**	**Controls For Inventory Of Assets, Acceptable Use, Information Classification, And Media Handling**			
1310	**IT Asset Inventory**	An inventory of IT Assets is maintained. Best practices include: 1) Automated asset discovery tools are used to conduct a real-time inventory of systems connected to the network. 2) All internet-of-things (IOT) devices are inventoried and policies are in place prohibiting employees from attaching unapproved IOT devices on the organization's network. 3) If DHCP is used, then enable DHCP server logging to improve the asset inventory and help detect unknown systems. 4) New equipment acquisitions automatically update the inventory as new, approved devices are connected to the network. 5) An asset inventory of all systems connected to the network is maintained. 6) Network-level authentication via 802.1x is used to permit only authorized systems, in the inventory above, to connect to the network. 7) Periodic physical inventories are conducted so that management knows if any devices are lost, stolen or otherwise missing. (Reference: CIS CSC #1)	1) Up-to-date: Yes 2) Includes all systems: Somewhat. Dr. Jackson Browne manages inventory of local IT assets excluding the servers. Servers inventory is managed by Techwin. 3) Automated: No 4) Prohibit unapproved devices: No. There are no policies in place for this at this point. 5) New asset process: Yes. Manual process by Dr. Browne. 6) Network-level authentication: No 7) Physical inventory: Yes. Performed periodically by Dr. Browne.	2: Managed	1) CIS Control 1: https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/
1320	**Protected Data Set Inventory**	1) A formal inventory of software applications and protected data sets is maintained. This inventory should include: a) An inventory of applications that process protected data sets b) The location of all databases and/or flat files that contain protected data c) A characterization of the data d) Quantification of the data e) The number of application users f) Whether the application is exposed to the internet g) Details of the security controls in place for the application 2) The number of locations that store protected data is minimized	1) Data set inventory: Yes. Documented in Appendix 6. 2) Application inventory: Yes. Documented in Appendix 6.	1: Initial	1) CIS Control 2: https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/
1330	**Media And Device Controls**	Best practices in device/media controls are employed, including: 1) Use of encryption technology and effective key management techniques 2) Labeling and inventory of media 3) Storage of media in secure areas 4) Periodic inventory of media to detect any loss 5) Written procedures documenting handling, storage, and security 6) Attending to the security of the media during transport or shipping	1) Except as noted in Appendix 8, workstation hard drives are encrypted. 2) Servers are not encrypted. 3) QNAP drives are encrypted.	2: Managed	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1340	**Media Disposal**	Best practices in media disposal / wiping are employed. This includes: 1) Formal written policies are in place specifying processes for media disposal 2) Approved methods are used (e.g. NIST SP 800-88, Guidelines for Media Sanitization) prior to repurposing of any media 3) Vendors used for media disposal are properly vetted. Whenever a vendor performs disposal/data wiping, a certificate of destruction is obtained 4) Records and documentation are maintained for any media disposed and/or repurposed 5) Media for disposal/repurposing is kept in a secure location and promptly processed ** Any leased photocopy/printer equipment should be included in this control. **	1) Dr. Browne physically destroys hard drives from retired workstations. 2) Photocopy equipment includes hard disk drives that may store images of PHI. Leased/serviced from ProCopy Inc..	2: Managed	1) NIST SP 800-88 R1: Guidelines for Media Sanitization. https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
1400	**DOMAIN: ACCESS CONTROL**	**Controls Related To Access Control Policy, User Access Management, Systems And Application Access Controls, And User Responsibilities**			
1420	**Unique User ID**	Best practice is to require a unique User ID for all regular users of systems: 1) At the network level, a separate account is established for each employee or authorized user 2) If the application software is not linked to network sign-in, a separate User ID is established for the application software as well 3) Generic IDs, if used, are used sparingly. For example, a generic account might be used in a department that, from time-to-time, had one student. A generic ID could be used in this case, and the password changed when the student left. 4) As part of its software-procurement process, only software that supported appropriate user accounts, access controls and, audit logging is used at the organization	1) Separate user IDs are used for network access, Allscripts, and DentalEHR. 2) Change passwords on Student User IDs after a student leaves (both network and Allscripts ID). 3) Formal HIPAA policies conform with best practices detailed at left.	2: Managed	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1430	**Secure Authentication Methods**	Secure authentication methods are in place: 1) Password policies are enforced a) At minimum, systems enforce password length of at least 8 characters b) For sensitive systems, recommended minimum password length is 15 characters or more c) Longer "pass phrases" should be encouraged 2) Software should check complexity of password and disallow insecure passwords 3) Passwords should be changed only if there is evidence or suspicion of compromise (discontinue forced password expiration timetables) 4) Procedures are in place to deliver new passwords securely so that only the individual knows their password 5) Two-factor and/or single-sign-on technology is used if feasible. 6) Security awareness training, written policies, and a user agreement are all in place 7) Additional safeguards should be in place to protect privileged accounts 8) A transition plan should be created if software does not support best-practice number 2	1) See Appendix 4 for application-specifics. 2) Generally, password requirements meet pre-2017 standards for length and complexity. 3) Two-factor authentication is not used. 4) Recommended authentication best-practices were revised in 2017 and are described at left. Highlights include use of pass-phrases and no longer forcing password resets on a defined schedule. 5) With the current (COVID) transition to work-from-home and remote network connections, the likelihood of a loss event caused by remote login abuse is higher than normal. **Recommendations:** 1) Require minimum password length of 12 characters for remote access. 2) Enforce two-factor authentication for remote access.	1: Initial	1) NIST SP 800-63B (June 2017) 2) Pwned Passwords: https://haveibeenpwned.com/Passwords
1440	**Audit Of Access Privileges**	A formal process is in place to periodically audit all access privileges to ensure that only authorized individuals have access to systems and that privileges are appropriately set.	1) Access lists are updated when employees are hired/terminated. 2) This review process is included in formal HIPAA policies. 3) Ass noted in Appendix 7, the most recent review of user credentials was in March 2020.	2: Managed	1) CIS Control 14: https://www.cisecurity.org/controls/controlled-access-based-on-the-need-to-know/ 2) CIS Control 16: https://www.cisecurity.org/controls/account-monitoring-and-control/
1500	**DOMAIN: CRYPTOGRAPHY**	**Controls Related To Encryption And Key Management**			
1520	**Encryption Best Practices**	Sensitive "data at rest" is encrypted using best practices: 1) Encryption is applied to devices and/or media according to established policy 2) Encryption status of devices is tracked and managed 3) Modern encryption ciphers are used 4) Encryption key management is done per best practices in NIST SP 800-57. Appropriate attention is given to key management procedures to ensure that the encryption keys are available when necessary and are kept confidential. 5) For end-user devices (e.g. laptops, USB Flash drives, smartphones) the guidelines in NIST SP 800-111 are employed for selection of encryption technology, configuration, and key management.	1) Server encryption: No 2) Workstation & laptop encryption: Yes. All but 3 have BitLocker enabled 3) QNAP encryption: Yes 4) Encryption documented: Yes, by Dr. Browne 6) Key management: BitLocker keys are printed and stored in a locked file drawer in Dr. Browne's desk. Digital copies of the keys are also stored on a folder on the public drive. All staff have access to view. Recommendation: Move encryption keys to restricted access digital folder.	2: Managed	1) NIST SP 800-57 2) NIST SP 800-111

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1600	**DOMAIN: PHYSICAL AND ENVIRONMENTAL SECURITY**	**Controls For Securing The Physical Environment, Including Secure Area Separations, Entry Controls, Physical Threat Protection, Equipment Security, Asset Disposal, And Clear Desk/Clear Screen Policies**			
1610	**Facility Security Plan**	A facility security plan is implemented to address information security risks. This plan will include: 1) Assessment of risks based on crime statistics in the area, patient population served, and other environmental factors 2) Use of appropriate technology, such as video monitoring and/or intrusion detection equipment 3) Use of human resources, such as security personnel and/or training of staff 4) Appropriate physical security of data equipment to include physical barriers, such as locked cabinets, rooms, or areas 5) Use of other protective systems, such as fire detection and/or suppression systems 6) Periodic testing of equipment and personnel 7) Use of appropriate safeguards for computer equipment located in publicly accessible areas 8) Attention to the security of cabling and supporting utilities	1) Security plan: Yes 2) Alarms, etc.: Yes. Exterior doors have alarms that are managed by alarm system. Recently added badge scanners to staff entry doors but these are not in use yet. No video monitoring at this time. 3) Locked storage: Yes 4) Fire suppression: No	2: Managed	
1620	**Physical Access Controls**	Physical access controls are employed, as appropriate, including: 1) Appropriate entry/exit controls at the perimeter, as well as at sensitive areas within the facility 2) Assignment of access privileges based on need 3) Visitor control systems and procedures 4) Staff training regarding procedures	1) Not reviewed in detail due to COVID-19 operating conditions. Will be reviewed during ongoing Risk Management support. 2) Generally, per previous assessments, appropriate controls are in place. 3) The organization is in the process of implementing badge readers at multiple doors to manage employee access. 4) Temporary procedures due to COVID-19: a) In-office patient visits significantly decreased from normal. Currently averaging 5-10 patients per week. b) Patients wait in their vehicles until appointment. c) In some cases, provider (in PPE) conducts appointment at patient's vehicle. d) Patients are only physically interacting with the provider(s). No direct contact with support staff.	1: Initial	
1630	**Physical Security Of Workstations**	Attention to the physical security of workstations is employed, for example: 1) Siting of equipment to limit risks from unauthorized personnel 2) Equipment accessible to the public is specified for appropriate physical and/or software protections, such as cable locks, automatic log-outs, and operating system hardening 3) Deterrents, such as labels prohibiting consumer use, are employed to reduce casual unauthorized access 4) Physical measures, such as screen filters, are used to limit viewing from unauthorized personnel 5) Workers using mobile computing devices are trained on procedures for private usage, and secure transport and handling	1) Control not reviewed in detail at this time due to COVID-19 conditions. 2) Per previous risk assessments: a) Tablets are used in patient areas and are not left unattended, so risks here are minimal. b) Workstations in dental area are placed appropriately. c) DentalEHR equipped with "HIPAA view" to hide patient names; staff are trained. 3) To be reviewed in further detail during Risk Management engagement as more-normal in-office operations resume.	1: Initial	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1700	**DOMAIN: OPERATIONAL SECURITY**	**Controls For Management Of Production It Systems: Change Management, Capacity Management, Malware, Backup, Logging, Monitoring, Installation, Vulnerabilities, Etc.**			
1720	**Backup And Recovery**	Backup and Recovery plans are formalized: 1) A data-criticality analysis is documented, 2) Hardware-level redundancy, such as RAID or Mirroring solutions, are employed, 3) For applications requiring high availability, replication to a geographically-remote location is employed. 4) Backup occurs at a frequency no less than daily, 5) Multiple generations (at least 10) are maintained, 6) An off-site backup is maintained, preferably geographically distant, 7) Isolation of backup media to protect from ransomware/attack 8) Backup media is encrypted, and duplicate encryption keys are kept off-site, 9) Verification of proper backup occurs on a daily basis, 10) Backup procedures are documented and multiple personnel are trained and accountable 11) Recovery capabilities are regularly tested. The formal Backup/DR Plan should specify all of the above best practices.	1) Documented critical data: Yes 2) Consistent backup process: Yes. Veeam backups. Saturday full image backups to QNAP of all servers with daily incremental backups. 14 day retention. Additional Azure cloud backup with 1 full weekly and 2 incremental backups. 3) AD/DC included: Yes 4) Fully-automated: Yes 5) Off-site backup: Yes. Microsoft Azure cloud (account in ICHC name, managed by Techwin). 6) Off-network backup: Yes. To the cloud. 7) Completion verification: Yes. Notification (both success and failure) are sent via email daily. 8) Detailed procedures: Yes. Techwin has all details on the backup and multiple users are familiar with the system. 9) DR Plan: No 10) Partial recovery tests: Yes. We regularly run test restore of files. 11) Full recovery tests: No. Database and/or VM restorations have not been conducted.	2: Managed	1) CIS Control 10: https://www.cisecurity.org/controls/data-recovery-capability/
1731	**Patch Management**	A robust patch management program is in place, including the following: 1) IT assets, including network gear and appliances, hypervisors, operating systems, application software, internet-of-things devices, printers, software embedded in medical devices, and other software are reviewed and prioritized for patching. Recommended priorities include: a) Firewall & network gear (as needed) b) Operating systems & hypervisors (monthly) c) Key application software (as needed) d) Microsoft products (monthly) e) Adobe products (monthly) f) Java (monthly) g) All browsers (monthly) h) Remote Monitoring and Management (RMM) tools, if used (as needed) 2) Patch management is performed on a timely basis 3) Threat intelligence is utilized to assist with prioritization 4) Appropriate testing (see Change Management) is conducted prior to patching 5) Documented procedures and tools are in place for patching, including timelines and responsible individuals 6) For organizations performing software development, third-party libraries are monitored for vulnerabilities, and when security updates are provided, recompilation is performed to update executables. See control 39 below. 7) Patch management is institutionalized using status reporting to management	1) Workstations patch management process: Dr. Browne performs this manually on the second Wednesday of the month for all PCs. This includes Windows updates, firmware updates, Adobe Reader/Acrobat, and Chrome browser. 2) Servers patch management process: Responsibility unclear. ICHC understands this to be Techwin responsibility. Techwin POC indicated that he had not reviewed patching during monthly on-site support for at least the past 3 months. Techwin POC did identify that automated OS updates are enabled for at least some of the servers. 3) Automated patching tools: No, neither ICHC nor Techwin use automated patching tools other than setting auto-update on Windows OS. 4) Network equipment checked: Understood to be responsibility of Techwin, to be addressed during on-site service. Frequency of network equipment checks not determined. 5) 3rd party applications: Yes for workstations, unclear for servers. Recommendations: 1) Clarify Techwin patching responsibility, methods, and frequency. 2) Ensure all best practices at left are implemented regarding frequency and scope of patching. 3) Implement a patch management application to simplify, automate, and report on patching & to allow centralized, remote deployment of patches and system updates. ICHC could implement a tool for workstations, request Techwin implement a tool for servers and workstations, or explore whether other IT service providers offer this capability.	1: Initial	1) Example SMB patch management applications include SolarWinds, Manage Engine, PDQ Deploy, and Itarian, among many others. Kaspersky SMB endpoint protection also includes a patching tool.

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1740	**Secure Configuration**	Secure configurations should be used for all IT assets, including cloud environments, networking equipment, server operating systems, databases and other server-based software, workstation operating systems, application software, and third-party cloud applications: 1) When available, authoritative configuration guides should be used for configuring the IT assets detailed above 2) When configuration guides are unavailable, default administrator accounts should be removed, strong passwords should be set, and unnecessary functionality should be disabled 3) Where applicable, standard images shall be used when deploying new assets 4) New assets should not be placed on the network until securely configured	1) VMware is used to enable 9 virtual servers all running Windows Server 2012 R2. 2) Per Neil Stephenson of Techwin, servers are configured using Microsoft best practices to install only appropriate roles and features. 3) Implementing secure configurations and system hardening: a) Decreases the likelihood of compromise or malware infection on an asset. b) Decreases the ability for attackers or malware to move across the network. c) Reduces common vulnerabilities and the network's attack surface.	1: Initial	1) CIS Control 5: https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/ 2) CIS Control 11: https://www.cisecurity.org/controls/secure-configuration-for-network-devices-such-as-firewalls-routers-and-switches/ 3) Azure Security Benchmarks: https://docs.microsoft.com/en-us/azure/security/benchmarks/
1750	**Malware Defenses**	Best practice is to use multiple layers of defenses to protect against malware. Several of these layers are: 1) Use of traditional anti-virus software on workstations. Best practices involve centrally-managed solutions that update and monitor all workstations on the network 2) Malware scanning on email solutions. Many email vendors provide malware scanning 3) Reputation-based whitelisting and/or blacklisting during internet browsing. Firewall vendors provide whitelists and/or blacklists to prevent users from visiting dangerous sites that might serve malware. Other solutions include DNS services that also protect users while browsing 4) "Mobile code," e.g. JavaScript, macros in Microsoft Office products, and/or macros in PDF files, can contain malware. See "Secure Configurations" section above to protect against these threats 5) Utilize threat intelligence from security vendors, government agencies, and non-profits to allow for proactive defense against ransomware and other destructive and disruptive attacks	1) Trend Micro is used for endpoint protection on workstations and Windows servers. 2) Email scanning: No additional malware scanning on email beyond Microsoft 365 defaults. 3) Internet filtering: WatchGuard firewall includes Webblocker internet filtering service, which provides filtering of malicious websites.	1: Initial	1) CIS Control 8: https://www.cisecurity.org/controls/malware-defenses/
1760	**Information System Security Monitoring**	A robust information-system-monitoring program at the network/infrastructure level is in place to detect unauthorized users and/or the presence of malware: 1) Monitoring of the following layers are involved: a) Network-level monitoring, e.g. firewalls and VPNs b) Server-operating systems, server software (e.g. web servers), and workstation operating systems c) Databases d) Administration consoles, key management systems e) Email 4) SIEMs and/or other automated tools are employed, configured, and tuned 5) Log data is captured and protected to deter tampering	1) Logging is generally enabled, but not proactively monitored. 2) During monthly on-site support time, Techwin will sometimes review firewall logs and alerts. 3) Any review is performed primarily for IT administration purposes. Techwin does not offer managed security services. Recommendation: Contract a managed security services provider or cybersecurity operations center to provide active security services, monitoring, and response abilities.	1: Initial	1) CIS Control 6: https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/ 2) CIS Control 12: https://www.cisecurity.org/controls/boundary-defense/ 3) Sysmon Guide: https://github.com/trustedsec/SysmonCommunityGuide

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1765	**Log-In Monitoring**	A robust program of log-in monitoring is conducted. This may occur at multiple levels - the network level and/or the EHR level. Automated tools greatly improve the productivity and effectiveness of this control. Unsuccessful log-in attempts provide evidence of potential password guessing. Successful log-ins are also monitored to determine suspicious behavior by identifying log-ins outside of normal operating hours and/or log-ins from unusual geographic locations. Further, log-ins of privileged users can be monitored to validate that their behaviors are appropriate.	1) Firewall logs are captured but not reliably monitored. **Recommendation:** Contract a managed security services provider or cybersecurity operations center to provide active security services, monitoring, and response abilities.	1: Initial	
1770	**Change Management Policy**	Change management has been formalized in written policies and procedures.	1) ICHC HIPAA policies include formal change management.	1: Initial	
1775	**Change Management Procedures**	Best practices for change management are in place, including: 1) Separate "operational," "test," and, if necessary, "development" environments exist 2) Appropriate testing is conducted prior to implementing any changes 3) Procedures and controls are in place to restrict changes except by authorized individuals with proper approvals 4) Testing is conducted after changes to verify that necessary functionality is maintained	1) ICHC HIPAA policies include formal change management.	1: Initial	
1785	**Cloud Storage Restrictions**	1) Organizations have implemented firewall rules to restrict access to personal cloud storage sites, e.g. Dropbox, Google Drive, Apple iCloud, etc. 2) Policies and procedures prohibit employee use of personal cloud storage sites	1) The Webblocker subscription on the firewall provides multiple site/content filtering options. 2) Personal storage sites are currently allowed.	0: Incomplete	
1790	**Legacy Systems And Data**	1) Organizations manage legacy systems and data: a) If legacy systems are retained, access controls are adjusted to restrict access, safeguards are implemented, and vendor support/patching is continued. b) Alternately, data in legacy systems can be extracted and maintained in different secure, vendor-supported software. c) If data is no longer needed, legacy software and data is deleted.	1) No legacy systems identified.	N/A	
1795	**End-Of-Life Systems**	1) Organizations replace or upgrade end-of-life operating systems, including Windows 7, Windows Server 2008, and older. 2) If replacement of end-of-life systems is not possible due to budget, implement containment/mitigation strategies, including: a) Restrict usage to the specific legacy software. b) Implement network segmentation to isolate the end-of-life system from the rest of the network. c) Block internet access if possible. If internet access is required, implement firewall rules at the network and device level to restrict internet traffic to the extent possible. d) Restrict usage of administrator accounts. e) Enable Data Execution Protection (DEP) f) Use antivirus / antimalware protections.	1) EOL servers: No 2) EOL workstations: Yes. Two PCs are running Windows 7 Pro. These are not in use as of this assessment. They are laptops for use by students. On radar to be upgraded or replaced.	2: Managed	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1800	**DOMAIN: COMMUNICATIONS SECURITY**	**Controls For Network Security And Services, Information Transfer, Electronic Messaging, And Confidentiality Agreements**			
1810	**Secure Network Design**	Principles of secure network design are used. These include: 1) Appropriate placement and configuration of firewalls and other intrusion protection capabilities 2) Isolation of sensitive systems, e.g. location of databases containing PHI, on separate servers and/or separate VLANS for guest wireless access 3) Appropriate use of encryption/authentication/integrity capabilities such as VPNs (see Transmission Security section below) 4) Appropriate documentation, including updated network diagrams, are maintained	1) Commercial firewall is enabled to manage incoming traffic. 2) Guest wireless access is segregated from the internal network. 3) The internal network is flat, with no segmentation or isolation of sensitive systems. **Recommendation:** Implement network segmentation and firewall rules to isolate servers and restrict which workstations & services can contact servers with sensitive data.	1: Initial	
1820	**Data In Motion**	1) For "data in motion", OCR has provided guidance and "safe harbor" to organizations that use VPNs implemented in accordance with NIST Standards: -NIST SP 800-77, Guide to IPsec VPNs -NIST SP 800-113, Guide to SSL VPNs 2) Other technologies (e.g. securely configured RDP) are not expressly prohibited, but do not fall under the safe harbor. 3) When using any third-party services for remote connections involving PHI transfer (e.g. LogMeIn), a Business Associate Agreement is in place. 4) An inventory of all routine data flows which contain ePHI is maintained for management control. This should include end-user initiated data flows.	1) Remote access: Yes. VPN and RD Gateway. 2) VPN: Yes. Through WatchGuard SSL VPN. 3) VPN configuration: Default settings are used. 4) RDP: Microsoft RDS Gateway configured for specific users, so user must have AD credentials and configuration profile in order to connect. 5) Third party remote access software: No. Neither Techwin nor ICHC staff use third party tools to remotely access the network.	2: Managed	1) NIST SP 800-77 2) NIST SP 800-113 3) HHS OCR Guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
1825	**Email And Text Messaging**	Email and cell phone text messaging are also "data in motion" and subject to this requirement. Best practices: 1) A secure email service is used for any email that contains PHI 2) The email system is configured to detect and automatically encrypt PHI, as well as allow the user to select encryption 3) Any certificates used in configuring these systems are signed by a Certificate Authority 4) SMS text messaging is not used, and rather, a secure text-messaging service is used for clinicians and others who require this convenience	1) Microsoft OME is available for email encryption through Microsoft 365 subscription. Low usage -- need is minimal. 2) Due to COVID-19, PatientIntake system has added ability to text patients from the application dashboard. For the limited numbers of patients attending in-office appointments, they wait in their vehicles rather than the waiting room, and this functionality is used to text them when the provider is ready for their appointment. 3) Information for telehealth appointments, such as video access link, may be emailed to patients using standard (unencrypted) email. 4) Both the texting and the emailing of appointment schedule information are not strictly compliant with HIPAA requirements for secure transmission of PHI, however both are common practice and are also covered by the HHS guidance on COVID-19 telehealth and HIPAA compliance.	1: Initial	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
1830	**Wireless Network Security**	Best Minimum Practices for Wireless Network Security include: 1) Commercial-grade WAPs and other networking equipment should be used in the network 2) SSID is enabled 3) Use WPA2 for encryption, WPS is disabled 4) Use an authentication protocol, preferably EAP-TLS with PKI 5) Use authoritative security guides, including: -NIST SP 800-153, and -NIST SP 800-97, Establishing Wireless Robust Security Networks	1) Commercial-grade WAPs managed by Techwin. 2) WPA2 encryption used. 3) Unmanaged devices allowed on internal wifi: Yes. employees can connect to secure wifi but visitors can only connect to our guest wifi. 4) Separate guest wifi: Yes Recommendation: Only allow devices managed by ICHC to connect to the internal wifi. Employees should use the Guest wifi for their phones and any other personal devices.	1: Initial	1) CIS Control 15: https://www.cisecurity.org/controls/wireless-access-control/
1840	**Redundant Connections**	1) Maintain redundant connections from separate ISPs. 2) Regularly test failover procedures Note that even best practices cannot fully mitigate all risks with cloud computing. This model is vulnerable in the event of widespread disruption in the internet, for example, from electronic warfare and/or sabotage by nation-state actors.	1) No change to ISPs. 2) ICHC is less reliant on cloud services now that Allscripts is locally hosted. 3) In previous assessments, ICHC has accepted the risk of infrequent internet outage.	1: Initial	
2000	**DOMAIN: SUPPLIER RELATIONSHIPS**	**Controls For Managing Supplier And Third-Party Relationships**			
2010	**Third Party Contracting Processes**	Third parties whose duties include creating, receiving, transmitting, or maintaining ePHI are placed under an appropriate HIPAA Business Associate Agreement (BAA). 1) Responsibility for contracting is centralized and an appropriate policy is in place, and understood by all in the organization, which documents the contracting process 2) A standard contract form is used, which includes: a) compliance with all elements required by HIPAA regulations b) specific procedures for security-incident reporting, which place the organization in control of the risk assessment process to determine if an incident is a breach c) financial liability for breach response is accepted by the contractor d) the contractor maintains appropriate insurance coverage to ensure the ability to fulfill its obligations 3) Contract forms supplied by the other party are negotiated, to the best of the organization's ability, to ensure the protections detailed above.	1) Contracting responsibility is centralized with management. 2) A standard Business Associate Agreement is used, based on a template provided by Eagle to be compliant with the latest HIPAA regulations. 3) The BAA does not require third parties to accept financial liability for breach response. 4) Of ICHC's third party contractors and services, most are unlikely to agree to financial liability clauses in a BAA.	2: Managed	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
2020	**Third Party Risk Management**	Third-party risk management is systematically handled: 1) Risk management responsibility is assigned in the organization 2) Third parties whose duties involve risk to PHI are identified, whether or not they meet the definition of HIPAA Business Associate 3) Risk assessments are performed to identify the risk level of the various third parties 4) Appropriate risk-management actions are taken, commensurate with the level of risk, which could include: a) Vendor evaluation process, which includes attention to information security practices b) Appropriate contracts, including for vendors/third parties who create data security risk but who do not meet the definition of HIPAA Business Associate, c) Periodic assessments and/or audits to validate that the organization's security posture is consistently maintained	1) All selected contractors are checked for suspension or debarment during contracting process 2) A comprehensive business associates list is not maintained. 3) The organization does not have an ongoing vendor risk management process.	1: Initial	
2100	**DOMAIN: INCIDENT MANAGEMENT**	**Controls For Managing And Reporting Information Security Incidents**			
2110	**Security Incident Procedures**	A documented approach to managing information-security incidents, consistent with applicable law, is in place to handle these events when they are detected. Best practices include: 1) Documentation of all security incidents 2) Training of staff regarding forensic procedures for collection of evidence 3) Established criteria for triaging incidents with established response timeframes and notification procedures for different severity levels 4) Incident Response training and Red Team exercises 5) Proactive network monitoring to detect incidents 6) Procedures to conduct post-mortem analysis of incidents for continuous improvement	1) Have procedures: Yes 2) Procedures detail: Somewhat. ICHC has an incident policy that includes security incidents. Within the policy timelines are established. 3) Incident response training: No. However ICHC has resources through Techwin and EAGLE who can support incident response processes on request.	1: Initial	1) CIS Control 19: https://www.cisecurity.org/controls/incident-response-and-management/

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
2200	**DOMAIN: BUSINESS CONTINUITY MANAGEMENT**	**Controls For Information Security Aspects Of Business Continuity Planning, Implementation, Verification, And Review, Including It Redundancy And Disaster Recovery**			
2210	**Disaster Recovery Planning**	A carefully prepared disaster recovery plan is in place. This plan will include: 1) Specify a Disaster Recovery Team (DRT), establish a protocol for activation, articulate the decision making process during a disaster, specify the communications plan for team members and other stakeholders 2) Identification of likely failure scenarios (e.g. power failure, fire, data corruption due to malware, hardware failure, etc.) 3) Crafting strategies to a) Avoid the failure, b) Mitigate damage if failure does occur, and c) Respond when the failure occurs 4) Prioritize recovery based on criticality of processes to the business 5) For each scenario, include detailed steps necessary to alert stakeholders and to restore operations 6) Repositories of critical documents including emergency contact information for employees / key vendors / other stakeholders, documentation regarding computer infrastructure / cloud accounts, and other information necessary during an emergency are maintained by all members of the DRT in multiple locations.	1) ICHC does not have a comprehensive disaster recovery plan. 2) The organization's contract with Techwin includes 24/7 call support. 3) The two physical servers have 4-hour response contracts (24/7) from the vendors. 4) Established and tested disaster recovery plans differentiate those who recover quickly from network failures, ransomware, etc., and those who do not. Recommendation: Prepare and test disaster recovery plan.	0: Incomplete	1) Disaster Recovery Plan Development: https://eagleconsultingpartners.com/dr-plan/
2220	**Emergency Mode Operations Planning**	An "Emergency Mode Operations" plan is in place that provides the organization the ability to operate during periods of system downtime. An effective plan will include: 1) Backup and alternate copies of critical data, such as patient charts, schedules, and other information 2) Alternate systems, such as paper forms, for use when systems are unavailable 3) Regular training and drills, both to test the plan and train employees in event of need	1) The organization does not have formal emergency mode operations plans. 2) Blank paper charts are available in some departments for use during system outage. 3) Offline schedules or patient contact information are not maintained. 4) Remote work and telehealth capabilities have been expanded during COVID-19.	0: Incomplete	
2300	**DOMAIN: COMPLIANCE**	**Controls For Legal, Regulatory, And Contractual Compliance, Records Protection And Retention, Privacy Of Protected Information, And Reviews Of Information Security**			
2310	**HIPAA Security Policies**	Information security policies are created to address the requirements of the HIPAA Security regulations. The organization regularly monitors changes in regulatory and contractual obligations and updates policies appropriately.	1) ICHC uses comprehensive HIPAA Security Policies customized for ICHC and most recently updated in 2018.	3: Defined	
2320	**Minimum Necessary**	The analysis required by the HIPAA Privacy Rule in the "Minimum Necessary" specification is documented. This documentation is used to establish role-based access controls in software applications.	1) Minimum necessary access requirements are documented in Appendix E of the HIPAA policy manual. 2) Access controls are in place for Allscripts system and DentalEHR.	3: Defined	

Control #	Control Title	Control Description	Existing Controls and Comments	Maturity Level	Additional Resources
2335	**Internal Audit Program**	An internal audit program is in place to monitor and review activity in EHR and other application software that contains ePHI. Best practices include: 1) The organization has identified the most probable type of employee "snooping", e.g. looking at records of co-workers, family, and friends 2) Reporting has been developed to efficiently review these most-likely situations 3) The audit program is coupled with an effective sanction program detailed above.	1) Audit program: Yes. Dr. Jackson Browne does quarterly EHR audits. These are performed manually. 2) ICHC previously reviewed an automated audit review tool, AMS SPHER, and determined it was not within budget.	2: Managed	
2340	**EHR Operating Integrity**	1) Use EHR technology that has been reviewed by third parties for consistent and effective functioning. 2) Ensure interfaces to outside systems, such as test or prescription order transmissions, are correctly configured and functioning. 3) Reliable patient-matching procedures are implemented to ensure that the correct patient record is accessed and/or updated. 4) Conduct regular employee training in EHR-system usage and address concerns about usage challenges. 5) Red-flag and investigate any incidents of EHR errors, such as incorrect medication lists, incomplete recording of treatment notes, failed lab test orders, incomplete prescription orders, etc.	1) Recent studies have identified that failures of EHR applications to provide consistent and effective functioning, both internally and when interfacing with outside systems, had led to issues with patient care. Example cases have included treatment delays, serious injury, and patient deaths. 2) See our recent article about this issue for more information: https://eagleconsultingpartners.com/general-news/ehrs-can-kill-patients/ **Recommendations:** 1) Review the article and the best practices at left. 2) If any errors with the EHR occur, immediately notify the vendor to investigate.	3: Defined	1) "EHRs can Kill Patients": https://eagleconsultingpartners.com/general-news/ehrs-can-kill-patients/
2370	**Website**	An organization's website is included in the formal risk assessment to review for any processing of PHI, as well as segregation of the website from sensitive data.	1) The organization implemented a new website in 2019 with a new hosting provider. 2) The site includes a link to access FollowMyHealth Allscripts Patient Portal. This link redirects patients to the FollowMyHealth website platform -- no patient data is transmitted through the ICHC website. 3) The site includes a "Pay My Bill" link. This link redirects patients to the PatientIntake website for processing payments -- no patient data or financial information is transmitted through the ICHC website. 4) Patient photos are present on the site. Recommendation: Ensure appropriate media release forms were obtained for all patient photos on the website.	3: Defined	
2380	**Evaluations**	Best practices include use of a variety of technical and non-technical evaluations of the adequacy of the controls in place. These evaluations may include: 1) Policy gap analyses to identify any deficiencies in written policies vs. standards and regulations 2) Compliance audits to identify deficiencies in compliance with HIPAA and other standards and regulations 3) Technical evaluations, such as automated vulnerability analyses, firewall audits, and/or penetration tests are conducted to validate the efficacy of technical safeguards 4) The organization subscribes to vulnerability intelligence services in order to stay aware of emerging exposures	1) Compliance assessment: Somewhat. Policy gap analysis was conducted when creating the current HIPAA Policy manual. Compliance assessment (of adherence to policies) has not been conducted. 2) Vulnerability scan: No. ICHC has contracted Eagle for a vulnerability scan of the network to be performed later this year.	1: Initial	1) CIS Control 3: https://www.cisecurity.org/controls/continuous-vulnerability-management/ 2) CIS Control 20: https://www.cisecurity.org/controls/penetration-tests-and-red-team-exercises/

Facility Security Review	
Control Title & Description	**Facility 1**
Name	**Main Office**
SECTION 1: FACILITY SUMMARY	
Purpose	Community Health Center
Address (City & state at minimum)	Small Town, USA
Number of staff based at the facility	45
SECTION 2: PRESENCE OF CRITICAL OR SENSITIVE INFORMATION ASSETS	
Identify whether servers, critical applications, critical digital storage, sensitive data sets, or other critical or sensitive IT is housed in the facility. (Yes/No)	Yes
Briefly summarize the critical or sensitive information assets housed in the facility.	All servers
Identify whether the facility network has regular access/connection to critical or sensitive information assets. (Yes/No)	Yes
Briefly summarize the access to critical or sensitive information assets from the facility.	All servers
SECTION 3: INITIAL FACILITY RISK PROFILE	
Establish the initial facility risk profile: HIGH: Facility houses critical or sensitive information assets. --> Complete Sections 4 and 5 below. MEDIUM: Facility network connects to critical or sensitive information assets. --> Complete Section 4 below. LOW: Facility does not access critical or sensitive information assets. --> No additional information necessary.	High
SECTION 4: EXTERIOR AND INTERIOR SECURITY CONTROLS	
Building description, including: 1) Standalone vs. multitenant. 2) Number of floors in building, and floor(s) occupied by the organization. 3) Exterior access vs. shared internal lobby. 4) Owned or leased. 5) Commentary on possible external threats, e.g. neighborhood, crime rate, etc.	Standalone facility accessed from exterior. Single floor. Previous risk assessments have noted that the regional opiate epidemic increases risk of break-in, though the health center does not store controlled substances. ICHC recently expanded into the ajacent chiropractic space.
How many exterior doors / entry points?	Multiple.
What type of locks are used on the exterior doors? (Ex. Barrel lock, deadbolt, electronic/electromagnetic, padlock, exit-only, etc.)	TBD
Other external access controls? (Ex. badge reader, entry buzzer, security guard, barred windows, etc.)	ICHC is in the process of installing and enabling badge readers.
Are the exterior doors kept locked or unlocked during business hours?	Only main door is unlocked during business hours.
Are any of the locking mechanisms easy to bypass? (Ex. latch accessible to a shim/Shove-it/Slim-Jim tool)	TBD
Are windows latched and secured?	TBD
Is an alarm system in place? Is it used? Who has enable/disable capability? Third-party monitoring?	Yes
Summary interior description, including: 1) General layout. 2) Divisions of public areas vs. controlled access areas vs. employee-only areas.	TBD
Approximate number of visitors per month	TBD
Any access controls / checkpoints between various areas of the facility? (Ex. between waiting room and escorted area, between escorted area and private offices, etc.) 1) Method or technology used for access control?	TBD

Control Title & Description	Facility 1
Name	**Main Office**
Review positioning and visibility of workstations. 1) Can any screens be viewed from publicly accessible areas (ex. waiting room)? 2) Can any screens be viewed through first-floor windows? 3) Are any workstations located in public areas (ex. hallways)? Are they screen-locked / automatic logoff? Any visible PHI on screens?	TBD
Any free-standing copier/multifunction devices? (These generally have internal hard drives.) 1) Owned or leased? 2) Service contract? Get name of company offering lease and/or service.	Yes, leased.
Any IoT devices in the office? (Ex. smart speaker, smart TV, thermostat, internet-connected appliances, etc.) 1) Are these devices on the same network as workstations or on an isolated network/VLAN? 2) Other significant networked devices? (Ex. network-controlled HVAC, medical equipment)	TBD
SECTION 5: ADDITIONAL CONTROLS FOR HIGH PRIORITY FACILITIES	
Video monitoring / recording? 1) Inside? Outside? 2) Is positioning and coverage appropriate? 3) Is it watched live? Reviewed? 4) Where are recordings stored? How long?	No
Review networking equipment & critical assets. 1) Are they stored securely and in an isolated area, such as a network closet? 2) Is the space locked? Any other security? Who has access? 3) Is the “network closet” (in whatever form) used for any other purpose? (Ex. supplies storage, cleaning & maintenance, etc.) 4) Is automatic fire suppression present in the network closet? If so, describe. 5) Are there any water sources in or above the network closet? (Context: risk that water leak causes physical damage to assets & loss of data) 6) Is the network closet near any building exits?	Network equipment stored in locked server area in basement. Water pipes and sump pump present nearby.
Include any other notes and observations related to the security of the facility, physical protection of critical assets, storage of devices, internal and external protections, etc.	In lieu of on-site review by analyst (due to COVID-19 restrictions), this is a limited facility review based on previous risk assessments. On-site review will be conducted when feasible during ongoing Risk Management support.

Inventory of Applications and Information Assets

#	Name	Application or Service Description	Number of Unique Identities	Host Device / Service	# of Authorized System Users	SSO Manager or Password Policies (Length, Complexity, Restrict reuse, Failures before lockout)	Multifactor Authentication?	Are access rights disabled upon employee termination? Approximate timeframe termination to account disabled.	Approximate Date of most recent review of user access credentials:	Are audit logs monitored regularly? Monitored for troubleshooting or incident response reasons only? Approximately when were audit logs last reviewed?
10	**Core Infrastructure**									
11	Active Directory	Local network access and file server	Unknown, see notes	On-Prem, multiple servers	64 total - 50 General, incl. service accts. - 14 Dental	Managed by ICHC. Length and complexity not determined. Passwords do not expire.	No	Yes, within a week	3/1/2020	Periodically during Techwin on-site. Monitoring primarily for IT support, not security.
12	Microsoft 365 (Fomerly Office 365)	Email, including OME for encrypted email	Limited	Microsoft	18	Linked to Active Directory	Optional. Some may have it enabled.	Yes, within a week	3/1/2020	Only monitored when issues arise
13	Phone System & Voicemail		N/A		32	Voicemail PIN is 5 digits set by user	No	When number transferred to new staff		Only monitored when issues arise
14	Trend Micro	Antivirus/antimalware	N/A	Installed on servers and workstations	44	Administrative portal managed by Techwin	N/A	N/A	N/A	Periodically during Techwin on-site.
15	Microsoft Office 2010	Office suite	N/A	PCs	N/A	N/A	N/A	N/A	N/A	N/A
20	**Remote Access Systems**									
21	VPN	VPN connection to office network through Watchguard firewall	N/A	Watchguard Firewall, offsite employee PCs		Linked to Active Directory	No	Linked to Active Directory	Linked to Active Directory	Captured, not generally reviewed.
22	Remote Desktop Gateway	Remote desktop access from off-site (without using VPN)	N/A	ICHCRDGW1		Linked to Active Directory	No	Linked to Active Directory	Linked to Active Directory	Captured, not generally reviewed.

Inventory of Applications

#	Name	Application or Service Description	Is data at rest encrypted? What are key management procedures?	Description of backup: - Frequency - Number of generations - Type: Full, Incremental, or Differential - Date of most recent backup recovery test	Additional Notes	Recommendations
10	**Core Infrastructure**					
11	Active Directory	Local network access and file server	No	Daily -- See Appendix 4 control 1720.	1) File share: Each person has a private folder on server. These may contain PHI, for example care manager registries including patient names, service dates, and goals. 2) User count includes service accounts for PatientIntake, Allscripts, and some consultants who provide peer review. 3) Active Directory credentials are used for VPN and offsite RDP access.	**1) Strengthen Active Directory credential requirements to follow best practice recommendations in Appendix 4 control 1430.**
12	Microsoft 365 (Fomerly Office 365)	Email, including OME for encrypted email	Microsoft responsible.	Microsoft responsible.	1) Managed by Techwin. 2) Only email used for now. Considering use of additional M365 capabilities. 3) Encrypted email is rarely needed or used.	**1) Implement multifactor authentication for all users. 2) Consider use of Advanced Threat Protection (ATP) package if receiving spam or phishing emails. 3) Consider review of security settings against best practices, especially if usage expands beyond email.**
13	Phone System & Voicemail			Unk.	1) Desk phone and voicemail provided to employees. 2) Underlying system/technology unclear.	**1) Assess this system in more detail during risk management.**
14	Trend Micro	Antivirus/antimalware	N/A	N/A	1) Centrally-managed endpoint solution. 2) Managed by Techwin.	**1) Ensure that appropriate individuals are receiving any alerts from endpoints.**
15	Microsoft Office 2010	Office suite	N/A	N/A	1) Office 2010 reaches end of support on October 13, 2020. After that time, Office 2010 will not receive updates or security fixes.	**1) Upgrade MS Office before October 2020.**
20	**Remote Access Systems**					
21	VPN	VPN connection to office network through Watchguard firewall	N/A	N/A	1) Increased usage due to COVID-19 and more work-from-home. 2) Used to access H: Drive (personal and shared files) and to connect to Allscripts & DentalEHR.	**1) Clarify which staff are using which remote access services and for what purposes. 2) Strengthen Active Directory credential requirements to follow best practice recommendations in Appendix 4 control 1430. 3) Require 2 Factor Authentication for VPN connections.**
22	Remote Desktop Gateway	Remote desktop access from off-site (without using VPN)	N/A	N/A	1) RD Gateway provides access to internal RDP Terminal Servers over HTTPS/443. It avoids exposing RDP/3389 to the internet. This mitigates many of the security concerns of using RDP for remote access. 2) Some employees use RD Gateway instead of VPN due to connection performance issues.	**1) Clarify which staff are using which remote access services and for what purposes. 2) Strengthen Active Directory credential requirements to follow best practice recommendations in Appendix 4 control 1430. 3) Require 2 Factor Authentication for RD Gateway Connections**

#	Name	Application or Service Description	Number of Unique Identities	Host Device / Service	# of Authorized System Users	SSO Manager or Password Policies (Length, Complexity, Restrict reuse, Failures before lockout)	Multifactor Authentication?	Are access rights disabled upon employee termination? Approximate timeframe termination to account disabled.	Approximate Date of most recent review of user access credentials:	Are audit logs monitored regularly? Monitored for troubleshooting or incident response reasons only? Approximately when were audit logs last reviewed?
30	**Electronic Records Systems**									
31	Allscripts	EHR for medical, behavioral health, clinical pharmacy	7,445	On-Prem, multiple servers	37	Length and complexity not determined. Password change enforced every 90 days.	No	Yes, within a week	3/1/2020	Quarterly manual internal audits by C. Browne
32	DentalEHR	Dental EHR	3,107	On-Prem, multiple servers	12	Up to 12 characters. Complexity not determined. Password change enforced every 90 days.	No	Yes, within a week		No
33	DentaScan	Dental Imaging System	(Linked to DentalEHR)	On-Prem, multiple servers	10	Up to 12 characters. Complexity not determined. Password change enforced every 90 days.	No	Yes, within a week		No
34	PatientIntake	Patient check-in & registration system for medical, behavioral health, and clinical pharmacy.	(Linked to Allscripts)	Cloud SaaS	23	Unknown	No	Yes, within a week	3/1/2020	Only monitored when issues arise
40	**Telehealth**									
41	Zoom	Videoconferencing system for telepsychiatry and telehealth	N/A	Zoom through Irwin Telehealth	Unknown		No	Not managed by ICHC		No
42	Doxy.Me	Telehealth platform		Doxy.Me	Not managed by ICHC		No	Not managed by ICHC		No
43	Doximity (doximity.com)	Clinician's networking platform/smartphone app with patient video/call/text features		Doximity	Not managed by ICHC		No	Not managed by ICHC		No

#	Name	Application or Service Description	Is data at rest encrypted? What are key management procedures?	Description of backup: - Frequency - Number of generations - Type: Full, Incremental, or Differential - Date of most recent backup recovery test	Additional Notes	Recommendations
30	**Electronic Records Systems**					
31	Allscripts	EHR for medical, behavioral health, clinical pharmacy	No	Daily -- See Appendix 4 control 1720.		
32	DentalEHR	Dental EHR	No	Daily -- See Appendix 4 control 1720.	1) DentalEHR is accessed within the ICHC network via a Remote Desktop session. 2) Remote Desktop availability within a network is frequently used by attackers to move between machines and/or spread malware across the network.	**1) Implement host-based and network firewall restrictions for RDP within the network, including disabling port 3389 on any computers not requiring DentalEHR access, blocking inbound 3389 traffic on hosts, etc.**
33	DentaScan	Dental Imaging System	No	Daily -- See Appendix 4 control 1720.	1) Software has no access controls -- any user can see all images.	
34	PatientIntake	Patient check-in & registration system for medical, behavioral health, and clinical pharmacy.	PatientIntake responsible	PatientIntake responsible	1) PatientIntake interfaces with Allscripts. 2) Application has added features during COVID-19 including patient texting & telehealth integrations. 3) ICHC uses text message feature -- in-person patients wait in their cars (not waiting room) and receive a text when provider is ready for them.	**1) Explore integrations with telehealth solutions.** **2) Review password strength, access controls, and Allscripts integration.**
40	**Telehealth**					
41	Zoom	Videoconferencing system for telepsychiatry and telehealth	N/A	N/A	1) Prior to COVID-19, was used by Psychiatrist for telepsychiatry through the corporate Zoom account of ICHC's telepsychiatry vendor Irwin. 2) Due to COVID-19, other providers have been using Zoom. Unclear if through Irwin account or other/personal. 3) ICHC is exploring establishing a company Zoom account for ongoing managed use.	**1) Consolidate all providers into a single telehealth solution for better management.** **2) If Zoom will be primary plaform, establish a managed company account, provide appropriate access to providers/staff, and ensure BAA is in place.** **3) Implement best practice security configurations, including meeting passwords, waiting rooms, etc.**
42	Doxy.Me	Telehealth platform	N/A	N/A	1) Some providers started using this platform during COVID-19. 2) Not managed by ICHC.	**1) Consolidate all providers into a single telehealth solution for better management.** **2) If Doxy.Me will be primary plaform, establish a managed company account, provide appropriate access to providers/staff, and ensure BAA is in place.** **3) Implement best practice security configurations, including meeting passwords, waiting rooms, etc.**
43	Doximity (doximity.com)	Clinician's networking platform/smartphone app with patient video/call/text features	N/A	N/A	1) Used independently by one provider. Not managed by ICHC. 2) Eagle previously reviewed platform for ICHC and expressed concerns with security, management, and features.	**1) Discontinue use of the platform and provide a centrally-managed solution instead.**

#	Name	Application or Service Description	Number of Unique Identities	Host Device / Service	# of Authorized System Users	SSO Manager or Password Policies (Length, Complexity, Restrict reuse, Failures before lockout)	Multifactor Authentication?	Are access rights disabled upon employee termination? Approximate timeframe termination to account disabled.	Approximate Date of most recent review of user access credentials:	Are audit logs monitored regularly? Monitored for troubleshooting or incident response reasons only? Approximately when were audit logs last reviewed?
50	**Other**									
51	Accountable	Accounting System	Unknown. Some patient names possible.	On prem	4	No password policies	No	Yes, within a week	3/1/2020	No
52	Interpreting Service	On-demand video access to language interpreters	N/A					N/A	N/A	N/A

#	Name	Application or Service Description	Is data at rest encrypted? What are key management procedures?	Description of backup: - Frequency - Number of generations - Type: Full, Incremental, or Differential - Date of most recent backup recovery test	Additional Notes	Recommendations
50	**Other**					
51	Accountable	Accounting System	No	Daily -- See Appendix 4 control 1720.		
52	Interpreting Service	On-demand video access to language interpreters	N/A	N/A	1) Accessed via iPad on dedicated rolling cart.	

Servers Inventory

Name	Description	Physical or Virtual?	Location	Operating System	Status	Encrypted Storage?	Notes / Comments
ICHCESXI01	VMWare Host Server	Physical Server	Server Rack	VMWare ESXi 6.7	Active	No	Server (hardware) has 24/7 4-hour response contract from vendor.
ICHCESXI02	VMWare Host Server	Physical Server	Server Rack	VMWare ESXi 6.7	Active	No	Server (hardware) has 24/7 4-hour response contract from vendor.
ICHCAPP2	Application Server	Virtual Server	Server Rack	Windows Server 2016	Active	No	
ICHCAPP3	Application Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	
ICHCDC1	Domain Controller	Virtual Server	Server Rack	Windows Server 2012	Active	No	
ICHCRDS2	Remote Desktop Server	Virtual Server	Server Rack	Windows Server 2016	Active	No	
ICHCWTG01	Web Reporting Server	Virtual Server	Server Rack	Linux Based	Active	No	Watchguard reporting service that goes along with firewall.
ICHCAPP1	Application Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	
ICHCBACKUP	Backup Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	Backs up to QNAP.
ICHCDC2	Domain Controller	Virtual Server	Server Rack	Windows Server 2016	Active	No	
ICHCFS1	File Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	
ICHCRDGW1	Remote Desktop Services Gateway	Virtual Server	Server Rack	Windows Server 2016	Active	No	
ICHCRDS1	Remote Desktop Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	
ICHCSQL1	SQL Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	SQL Server 2014
ICHCUTILITY	Utility Server	Virtual Server	Server Rack	Windows Server 2012	Active	No	Mainly used by Techwin for IT management.
vCenter6.7	VMWare vCenter Virtual Appliance	Virtual Server	Server Rack	Linux Based	Active	No	

Appendix 8 - Other IT Inventory

Name / Machine ID	Description or S/N	Quantity	Asset Class	Location	Operating System	Status	Processes Protected Data?	Encrypted Storage?	Notes / Comments
MANGED BY ICHC									
ICHC1001	HP Tower	1	Workstation	Susie	Windows 10 Pro	Active	Yes	Yes	
ICHC1003	Dell Latitude	1	Laptop	Bobby	Windows 10 Pro	Active	Yes	Yes	
ICHC1004	Dell Latitude	1	Laptop	Jimmy	Windows 10 Pro	Active	Yes	Yes	
ICHC1005	Dell Latitude	1	Laptop	Frank	Windows 10 Pro	Active	Yes	Yes	
ICHC1006	Dell Latitude	1	Laptop	Dr. Rob	Windows 10 Pro	Active	Yes	Yes	
ICHC1007	Dell Latitude	1	Laptop	Harper	Windows 10 Pro	Active	Yes	Yes	
ICHC1008	Dell Latitude	1	Laptop	Melanie	Windows 10 Pro	Active	Yes	Yes	
ICHC1009	Dell Latitude	1	Laptop	Stephanie	Windows 8 Pro	Active	Yes	Yes	
ICHC1011	Dell Latitude	1	Laptop	Nurse Ashley	Windows 10 Pro	Active	Yes	Yes	
ICHC1012	Dell Latitude	1	Laptop	Student	Windows 10 Pro	Active	Yes	Yes	
ICHC1013	Dell Latitude	1	Laptop	Laura	Windows 10 Pro	Active	Yes	Yes	
ICHC1015	Dell Latitude	1	Laptop	Jackson	Windows 10 Pro	Active	Yes	Yes	
ICHC1016	Dell Latitude	1	Laptop	EXTRA	Windows 7 Pro	Inactive	Yes	No	No BitLocker - Windows 7
ICHC1017	Dell Latitude	1	Laptop	Katie	Windows 10 Pro	Active	Yes	Yes	
ICHC1019	Dell Latitude	1	Laptop	Renae	Windows 10 Pro	Active	Yes	Yes	
ICHC1020	Dell Latitude	1	Laptop	Shelly	Windows 10 Pro	Active	Yes	Yes	
ICHC1021	Dell Latitude	1	Laptop	Natalie	Windows 10 Pro	Active	Yes	Yes	
ICHC1022	Dell Latitude	1	Laptop	Sherry	Windows 10 Pro	Active	Yes	Yes	
ICHC1023	Dell Latitude	1	Laptop	Dr. Rogers	Windows 10 Pro	Active	Yes	Yes	
ICHC3002	HP Tower	1	Workstation	Logan	Windows 10 Pro	Active	Yes	Yes	
ICHC3003	HP Tower	1	Workstation	Jessie	Windows 10 Pro	Active	Yes	Yes	
ICHC3006	HP Tower	1	Workstation	Dr. Rogers	Windows 10 Pro	Active	Yes	Yes	
ICHC3007	HP Tower	1	Workstation	ADMIN. ASST.	Windows 7 Pro	Inactive	Yes	No	No BitLocker - Windows 7
ICHC3009	HP Tower	1	Workstation	Lucy	Windows 10 Pro	Active	Yes	Yes	BitLocker is disabled due to EHR reporting software
ICHC3011	HP Tower	1	Workstation	X-RAY - DENTAL	Windows 10 Pro	Active	Yes	Yes	
ICHC3012	HP Tower	1	Workstation	Laura	Windows 10 Pro	Active	Yes	No	BitLocker is disabled due to EHR reporting software
ICHC3014	HP Tower	1	Workstation	Dr. Kevin	Windows 10 Pro	Active	Yes	Yes	
ICHC3015	HP Tower	1	Workstation	TREATMENT 5	Windows 10 Pro	Active	Yes	Yes	
ICHC3016	HP Tower	1	Workstation	TREATMENT 4	Windows 10 Pro	Active	Yes	No	Disabled BitLocker due to numerous issues with it
ICHC3017	HP Tower	1	Workstation	TREATMENT 3	Windows 10 Pro	Active	Yes	No	Disabled BitLocker due to numerous issues with it
ICHC3018	HP Tower	1	Workstation	TREATMENT 2	Windows 10 Pro	Active	Yes	Yes	
ICHC3019	HP Tower	1	Workstation	TREATMENT 1	Windows 10 Pro	Active	Yes	Yes	
ICHC3024	HP Tower	1	Workstation	DENTAL CHECKOUT	Windows 10 Pro	Active	Yes	Yes	
ICHC3025	HP Tower	1	Workstation	Dental	Windows 10 Pro	Active	Yes	Yes	
ICHC3026	HP Tower	1	Workstation	Admin Office	Windows 10 Pro	Active	Yes	Yes	
ICHC3027	HP Tower	1	Workstation	Front Desk	Windows 10 Pro	Active	Yes	Yes	
ICHC3028	HP Tower	1	Workstation	Front Desk	Windows 10 Pro	Active	Yes	Yes	
ICHC3029	HP Tower	1	Workstation	Dr. Mitchell	Windows 10 Pro	Active	Yes	Yes	
ICHC3030	HP Tower	1	Workstation	TREATMENT 7	Windows 10 Pro	Active	Yes	Yes	
ICHC3031	HP Tower	1	Workstation	Front Desk	Windows 10 Pro	Active	Yes	Yes	
ICHC3032	HP Tower	1	Workstation	Michael	Windows 10 Pro	Active	Yes	Yes	

Appendix 8 - Other IT Inventory

Name / Machine ID	Description or S/N	Quantity	Asset Class	Location	Operating System	Status	Processes Protected Data?	Encrypted Storage?	Notes / Comments
ICHC3033	HP Tower	1	Workstation	TELEPSYCH	Windows 10 Pro	Active	Yes	Yes	
ICHC3034	HP Tower	1	Workstation	CONFERENCE	Windows 10 Pro	Active	Yes	Yes	
ICHC3035	HP Tower	1	Workstation	Chris	Windows 10 Pro	Active	Yes	Yes	
iPad	Translation Service System	1	Mobile Device	Rolling Cart	iOS -- version?	Active	Yes	Unknown	
MANAGED BY Techwin									
ICHC_XTM	WatchGuard M200	1	Network Component	Server Rack	WatchGuard XTM 12.5.2	Active	Yes	N/A	
HP-2920-Switch-1	HP 2920-48G POE (J9729A)	1	Network Component	Server Rack	WB.16.07.0003	Active	Yes	N/A	
HP-2920-Switch-2	HP 2920-48G POE (J9729A)	1	Network Component	Server Rack	WB.16.07.0003	Active	Yes	N/A	
HP-2920-Switch-3	HP 2920-48G POE (J9729A)	1	Network Component	Server Rack	WB.16.07.0003	Active	Yes	N/A	
HP-2920-Switch-4	HP 2920-48G POE (J9729A)	1	Network Component	Server Rack	WB.16.07.0003	Active	Yes	N/A	
HP-2920-Switch-5	HP 2920-48G POE (J9729A)	1	Network Component	Server Rack	WB.16.06.006	Active	Yes	N/A	
Office 2 (New Building)	WG AP325 -Access Point	1	Network Component	New Building Office 2	8.8.1-101	Active	Yes	N/A	
Dentist Lobby	WG AP320 - Access Point	1	Network Component	Dentist Lobby	8.8.1-101	Active	Yes	N/A	
Dentist Hall	WG AP320 - Access Point	1	Network Component	Dentist Hall	8.8.1-101	Active	Yes	N/A	
Medical Lobby	WG AP320 - Access Point	1	Network Component	Medical Lobby	8.8.1-101	Active	Yes	N/A	
Medical Hall	WG AP320 - Access Point	1	Network Component	Medical Hall	8.8.1-101	Active	Yes	N/A	
Medical Office	WG AP320 - Access Point	1	Network Component	Medical Office	8.8.1-101	Active	Yes	N/A	
Medical Hall2	WG AP320 - Access Point	1	Network Component	Medical Hall 2	8.8.1-101	Active	Yes	N/A	
Administration Hallway Rear	WG AP320 - Access Point	1	Network Component	Admin Hallway Rear	8.8.1-101	Active	Yes	N/A	
Administration Hallway Middle	WG AP320 - Access Point	1	Network Component	Admin Hallway Middle	8.8.1-101	Active	Yes	N/A	
Administration Hallway Front	WG AP320 - Access Point	1	Network Component	Admin Hallway Front	8.8.1-101	Active	Yes	N/A	
Office 1 (New Building)	WG AP325 -Access Point	1	Network Component	New Building Office 1	8.8.1-101	Active	Yes	N/A	
QNAP	QNAP Backup Appliance	1	Network Component	Server Rack	4.4.2.1270	Active	Yes	Yes	