Data Breach Risks & Best Practices for Small and Mid-Size Healthcare Providers (2023 Update)[1]

By: Siddharth "Sid" Bose and Dakota M. Coates[2]

[1] This publication is intended to serve as a preliminary research tool for attorneys for educational purposes only. It should not be used as the sole basis for making critical business or legal decisions. This publication does not constitute, and should not be relied upon as, legal advice.

[2] Sid Bose is a Partner at Ice Miller LLP and the chair of Ice Miller's Technology, Privacy and Cyber Risk Practice. As an attorney with an information systems and security background, Sid counsels clients on various cybersecurity, privacy, and compliance issues.

Dakota Coates is an Associate in Ice Miller LLP's White Collar & Internal Investigations and Data Security and Privacy Groups. Dakota counsel's national and international clients on various data security, privacy, and regulatory/ethical compliance matters.

TABLE OF CONTENTS

I. INTRODUCTION

Since the initial draft of *Data Breach Risks & Best Practices for Small and Mid-Size Healthcare Providers* in 2016, the likelihood of suffering from a data breach has only continued to rise for American companies. Similarly, the associated cost with data breaches has continued to grow year-after-year as data breaches become more frequent, more sophisticated, and more commercialized. Unfortunately, healthcare providers continue to be a prime target for data breaches. Due to the wide array of financial exposure through fines, legal fees, notification costs, loss of business, and diminished reputation and goodwill, the industry continues to be both the most frequent victim of data breaches as well as the most financially impacted.[1]

Thus, as the risk and financial impact from data breaches has only continued to grow for healthcare providers since 2016, it is critical to revisit the importance of companies ensuring that they continue to take the necessary steps and allocate sufficient resources to ensure compliance with the privacy regulations set forth under the Health Insurance Portability and Accountability Act of 1996 (hereinafter "HIPAA") and the Health Information Technology for Economic and Clinical Health Act (hereinafter "HITECH Act"), as well as other state and federal privacy regulations. Across the growing horizon of data security and privacy regulations, healthcare providers continue to see compounding obligations to implement, maintain, and enforce a wide array of policies and procedures aimed at protecting the confidentiality, integrity, and availability of protect health information ("PHI"). PHI includes any individually identifiable health information that (1) is held or transmitted by an entity in any form or media, whether electronic, paper, or oral; (2) relates to (a) an individual's past, present, or future physical or mental health or condition; (b) the provision of health care to an individual; and (c) the past, present, or future payment for the provision of health care to an individual; and (3) identifies an individual or for which there is a reasonable basis to believe it can be used to identify an individual.[2] Common examples of what constitute identifiers for health information include:

- Name;
- Address;
- Dates of birth, admission, discharge, and/or death;
- Phone or fax numbers;
- Social Security Numbers;
- Medical record or health plan beneficiary numbers;
- Emails;
- State or federal license numbers;
- Internet Protocol (IP) numbers; and
- Biometric identifiers.[3]

Furthermore, as the pervasiveness and sophistication of data breaches continue to increase, healthcare providers must also ensure that they are taking appropriate steps to minimize their potential exposure to data breaches (for example, implementing and maintaining strong, segregated backups) while also enhancing their internal efforts to bolster employee awareness and resilience.

II. RECENT DATA BREACH TRENDS FOR HEALTHCARE PROVIDERS

The Cost of a Data Breach

The Department of Health and Human Services ("HHS") has found that health care data breaches have continued on an upward trend since 2012, with the most significant jump in large health care data breaches (those involving 500 or more records) starting in 2019 and nearly doubling from the 369 breaches in 2018 to a peak of 717 breaches in 2021.[4] Subdivided across the industry, approximately 72% of breaches came from healthcare providers, 15% from health plans, and 13% from business associates.[5] Furthermore, in 2022 alone we saw nearly 50 million patients affected by health care data breaches. At the same time, we have seen the individual cost of a data breach per patient record increase from approximately $363/record in 2015 to over $500/record today.[6] As a result, for the 12th year in a row the health care industry continues to have the highest total cost for breaches out any industry—sitting at an average cost of $10.1 million per breach.[7] By comparison, the next highest cost by industry is the financial sector, which is only at $5.97 million per breach.[8]

The Source of the Data Breach

More than 93% of health care organizations have experienced a data breach over the past three years, and a concerning 57% have experienced more than five data breaches during that same period.[9] And despite the upward trends in costs and frequency, we continue to see a majority of health care organizations only allocating 7% (or less) of their IT budgets to cybersecurity—significantly less than other equally vulnerable industries.[10] As a result of insufficient financial resources and inadequate security practices, health care organizations continue to be 2-3 times more likely to suffer a cyberattack than other industries, and ransomware attacks have quintupled since 2016.[11] Examining the most common sources of these attacks further, studies have found that the most common cause of health care data breaches is hacking or IT infrastructure incidents which are now involved in more than 75% of all data breaches.[12] Relatedly, the next highest cause of health care data breaches results from unauthorized access or disclosure, which is involved in 15-20% of breaches.[13] Across these breaches, approximately 56% involved network server breaches, 23% involved email-targeting, 20% involve compromised credentials, 17% involved phishing attacks, and 15% involved internal cloud misconfiguration.[14]

III. RECENT ENFORCEMENT TRENDS AGAINST HEALTHCARE PROVIDERS

A. Potential Monetary Penalties for Healthcare providers that Suffer a Data Breach

The HHS Office of Inspector General ("OIG") has the authority to pursue a wide array of different civil monetary penalties ("CMPs") against individuals or health care entities for a wide array of prohibited activities. For example, under the Medicaid Drug Rebate Program, the OIG can pursue CMPs against those who fail to properly report the required price information. In the context of HIPAA, there are four tiers of violations that the OIG can pursue CMPs for based on the level of awareness/knowledge of the violation—with the most common violations including not completing the required risk assessments, improper disclosure or protection of PHI, untimely notification of a data breach, and failure to establish compliant business associate agreements.[15] These four tiers and their respective penalty ranges will include both the CMP annual caps as

established in the Federal Registrar as well as the CMP annual caps established under HHS's April 2019 *Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties*.[16] This enforcement discretion notification sought to correct a potential misinterpretation/misapplication of the HITECH Act to Tiers 1-3, and instead established a separate discretionary penalty table that differentiates the annual cap based more on the specific tier. [17] This is reflected below by showing the Federal Registrar cap, demarcated by a "FR" and the Notice of Enforcement Discretion cap, demarcated by a "NED."

- Tier 1: Lack of Knowledge. Under this tier, the covered entity was unaware of the fact that a HIPAA rule was being violated and it could not have known about the violation even if it had done its reasonable diligence. A covered entity has completed its reasonable due diligence when it acts with the proper business care and prudence expected from a person under similar circumstances seeking to satisfy the specific legal obligation. The penalties currently range from $127-63,973 per violation, with an annual NED cap of $31,987 (effectively reducing the maximum penalty down to this amount) and a FR cap of $1,919,173.

- Tier 2: Reasonable Cause and No Willful Neglect. Under this tier, the covered entity knew or should have known through reasonable diligence that its action or omission violated its legal obligations but there is no willful neglect (defined in Tier 3). The penalties currently range from $1,280-63,973 per violation, with an annual NED cap of $127,974 and a FR cap of $1,919,173.

- Tier 3: Willful Neglect but Corrected Within 30 Days. Under this tier, the covered entity engaged in willful neglect but took appropriate corrective action within 30 days of the violation. An entity's actions constitute willful neglect when there is a conscious, intentional failure or reckless indifferent to the obligation to comply. The currently range from $12,794-63,973 per violation, with an annual cap NED cap of $317,865 and a FR cap of $1,919,173.

- Tier 4: Willful Neglect not Corrected Within 30 Days. This tier covers the same conduct as identified in Tier 3; however, it institutes increased penalties for covered entities that did not attempt to take corrective action within 30 days of the violation. An example of this would be unreasonably exceeding the notification window for discovery of a data breach. As a result, the penalties are significantly increased for this violation with penalties currently ranging from $63,973-1,919,173, with an annual cap of $1,919,173.

Each of these values will be increased to include an inflationary update. The 2023 multiplier is currently set to 1.07745, which has not yet officially been applied to the discretionary penalty table.[18]

Additionally, under the HITECH Act, the Michigan State Attorney General also has the ability to pursue civil actions against healthcare providers for unauthorized use or disclosure of the PHI of Michigan residents. Currently, the fines that can be sought by the AG is a range of $100-25,000 per violation.[19]

B. Examples of Recent Data Breach Settlements with OCR

Over the past decade, the HHS Office of Civil Rights ("OCR") has steadily increased its annual number of HIPAA-related settlements, landing at 20 settlements in 2022 alone—nearly double the number of settlements in 2016—and serving as the highest number in any given year.[20] Much of this aggressive push by the OCR has been related to its crackdown against HIPAA Right of Access violations which has been a major initiative for the OCR since 2019, and was the reason for over 80% of all settlement allegations in 2022 and 2021 alone. The Right of Access under HIPAA provides that individuals have the right to see and request copies of their health information and, absent an extension/exception, a healthcare provider must provide that information within 30 days.[21] In each of these cases, the enforcement actions are generally brought because a covered entity failed to provide a patient with their medical information within a reasonable timeframe. Based on this growing enforcement trend, we suspect that the OCR will continue this push throughout 2023 and for years to come. And while these may sound like minor infractions, it is critical that healthcare providers understand that the settlement amounts can still be quite weighty—ranging from $3,500 to upwards of $240,000 in 2022 alone.[22] Other common areas of enforcement actions over the past few years have been lack of encryption, failure to perform risk analysis, inadequate breach notification, lack of appropriate access controls, and failure to use sufficient business associate agreements.[23]

Banner Health - $1,250,000 (2023)

In February of 2023, Banner Health ("Banner"), a non-profit health system that was the subject of the largest data breach in 2016 in which a threat actor gained access to the electronic PHI ("ePHI") of 2.81 million individuals (although it sent letters to over 3.7 million individuals) finally entered into a settlement with HHS.[24] This breach primarily involved a threat actor gaining unauthorized access to Banner through the cover entity's payment system, which in turn impacted their servers and allowed them to potentially access and exfiltrate names, birth dates, addresses, physician names, health insurance information, clinical information, lab results, social security numbers, and much more.[25] Following its breach notification to HHS, HHS opened up a compliance review of Banner and discovered a wide array of HIPAA violations, including failing to: conduct an accurate and through risk analysis, implement sufficient tracking and review tools to analyze system activity, utilize verification for persons/entities seeking access to ePHI, and leverage appropriate technical safeguards against unauthorized access.[26]

As part of the settlement, Banner had to pay a hefty $1.2 million fine and agreed to implement a lengthy corrective action plan ("CAP") under a two-year monitoring period. The CAP requires Banner to (1) conduct a risk assessment to gauge the risks and vulnerabilities of its systems across the organization; (2) develop and implement a risk management plan; (3) develop, implement, and distribute policies and procedures for an array of data security and privacy issues, including (a) risk analyses; (b) risk management plans; (c) information system activity reviews; (d) authentication processes for data access; and (e) other security measures for preventing unauthorized access and strengthening electronic data transfers; and (4) requiring certification and ongoing monitoring of personnel compliance with these policies and procedures, including an obligation to investigate and report and failures to comply within thirty (30) days.[27]

Oklahoma State University – Center for Health Sciences - $875,000 (2022)

Oklahoma State University–Center for Health Sciences ("OSU-CHS") is another case stemming from a breach notification. In this case, OSU-CHS filed a report in 2018 identifying that a third party had gained access to a web server that hosted ePHI and the third-party had deployed malware compromising the ePHI of 279,865 individuals in late 2017.[28] However, it was later discovered that the threat actor had also accessed this same server in 2016—when OSU-CHS was not even aware of the fact that it stored ePHI on the server. This breach resulted in a wide array of ePHI being breached, including names, Medicaid numbers, treatment information, and more.[29] OSU-CHS was required to pay a fine of $875,000 and had to enter into a two-year CAP. Similar to Banner, OSU-CHS was required to conduct a comprehensive, enterprise-wide risk analysis to ensure that it had full insight into all of its systems and what information was stored on what servers. Furthermore, the entity was requested to implement a risk management plan as well as policies and procedures around how to better protect the privacy and security of PHI on its systems. Notably, OSU-CHS had to identify a monitoring entity that would review and monitor its compliance with the CAP. This monitor had to be approved by HHS and had to facilitate review requests from HHS throughout the duration of the CAP.

Memorial Hermann Health System - $240,000 (2022)

Memorial Herman Health System ("MHHS"), a not-for-profit health system in Texas, was just one of the numerous Right of Access cases brought in 2022. In this particular case, a patient of MHHS had filed five requests between June 2019 and January 2020 to MHHS's billing department requesting a full copy of their medical and billing request.[30] However, despite HIPAA's requirement that such data be provided within thirty (30) days (absent an extension) it took MHHS 564 days to after the initial request to actually provide the information. Due to the egregiousness of this delay, MHHS was required to pay $240,000—the highest Right to Access penalty thus far.[31] Additionally, MHHS was required to enter into a two-year CAP and monitoring period. As part of this CAP, MHHS was required to: revises its internal control policies and procedures relating to patient access to PHI, to develop and implement training materials for the billing department regarding a patient's right to access PHI, and to provide annual compliance reports.[32] Furthermore, every 90-days MHHS was required to submit a list of all requests for medical information and records to HHS, identifying the data received/completed, format requested/provided, number of pages, cost, and any documentation related to denials.[33] An owner or officer of MHHS was also required to sign and submit an attestation to HHS summarizing and affirming the implementation of these changes.

Anthem Inc. - $16,000,000 (2018)

In 2018, Anthem Inc. ("Anthem") became subject to the largest HIPAA fine (thus far) in connection to a cyberattack that compromised the PHI over 78.8 million individuals—the largest US health data breach. [34] Anthem's cyberattack involved threat actors gaining access to their IT system through a phishing email sent to an Anthem subsidiary which opened the door to granting the hackers access to Anthem's system writ-large from December 2014 through January 2015.[35] As a result, these hackers were able to steal extensive amounts of ePHI, including Social Security numbers, medical identification numbers, and employment information. Unfortunately, it was Anthem's failure to implement appropriate detection measures, coupled with weak password

policies and access controls, that had enabled this threat actor's effectiveness.[36] Accordingly, the CAP required Anthem to conduct a full risk analysis of its systems and required Anthem to in turn create a Statement of Work as to how it was going to address its deficiencies, including implementation of specific policies and procedures aimed at protecting the security of PHI.[37]

Other Examples

In addition to the Anthem settlement, HHS had two more settlements with particularly hefty fines in the past few years. This includes the Excellus Health Plan ("EHP") settlement in 2021 for $5.1 million and the Touchstone Medical Imaging ("TMI") settlement in 2019 for $3 million. EHP, another breach case, involved a data breach than spanned nearly two years in which a threat actor had installed malware that ultimately gathered information more than 9.3 million individuals—including their names, Social Security numbers, bank account information, and health/clinical information.[38] A cornerstone of the EHP CAP was that EHP had to implement specific policies and procedures related to information system activity monitoring (e.g., audit logs, access reports, review parameters) and access controls (e.g., network segmentation, role-based access rights).[39] Meanwhile, the TMI incident involved an insecure file transfer on a web server that resulted in some 300,000 patients having their PHI made visible through a basic internet search.[40] And despite being notified in May of 2019 by the Federal Bureau of Investigation ("FBI") that some of its servers were allowing unauthorized access, TMI initially asserted that its investigation revealed that there was no exposed PHI.[41] However, after OCR's initial investigation in the months following this initial notification, TMI admitted that PHI had been exposed. Accordingly, OCR found that TMI had not fully investigated the security incident until several months after it had been notified by both the FBI and OCR—and as a result its data breach notification to individuals was inappropriately delayed.[42] Compounding this, OCR also found that TMI failed to: conduct appropriate risk assessments, utilize appropriate business associate agreements, sufficiently manage access rights, and manage its data breach response.[43] In light of these numerous failures, the CAP required TMI to develop and implement a cast of compliance policies, including, but not limited to: access controls, termination of user accounts, password management, security incident responses, designation of personnel and templates for business associate agreements (including specific, required terms for these agreements), and training and technical safeguards.[44]

C. Examples of Recent Data Breach Settlements with State Attorneys General

DNA Diagnostic Center - $400,000 (2023 – Pennsylvania/Ohio)

In an investigation spearheaded by the Attorneys General of Pennsylvania and Ohio, DNA Diagnostics Center, Inc. ("DDC") was faced with the potential downfalls of acquisition liabilities. Specifically, this incident involved a breach of a database used by Orchid Cellmark, an entity acquired by DDC, that had not been used for business purposes and that had inadvertently been transferred into DDC's systems.[45] Unaware that these databases were in its system—for more than nine years—sensitive personal information in plain text sat vulnerable on its system. To make the situation more concerning, DDC started receiving automated alerts in May of 2021 from its service provider of suspicious activity on its network, but it failed to activate its incident response plan until August of 2021 when the Cobalt Strike malware was identified on the system.[46] Already in the system at this point, the threat actor then accessed five servers and twenty-eight databases allowing it to exfiltrate data for over 2 million patients, including over 30,000 Ohioans and over

12,000 Pennsylvanians.[47] The Attorneys General concluded that DDC had repeatedly failed to adequately protect (or even maintain record of) the data under its care. This failure to update, manage, and remove asset inventory, coupled with its clear lack of safeguards and lax incident response, led the Attorneys General to conclude that DDC engaged in improper cybersecurity practices and had unreasonably and unnecessarily exposed personal data to unauthorized access and theft.[48] As part of its assurance of voluntary compliance, DDC was required to pay a $400,000 fine to these two states and had to design, implement, test, and maintain a comprehensive security program.[49] The assurance set forth a comprehensive collection of required components, such as methods and criteria for managing information security risks, allocations of sufficient resources to protect PHI, designating personnel to oversee and operate the program, requiring annual audits of the program, incorporate stronger information security safeguards, maintaining a full and current data/asset inventory, restricting transmission of data, disabling/removing unnecessary assets, enhance and hasten its incident response timelines, manage event logs, and much more.[50]

McLean Hospital - $75,000 (2018 – Massachusetts)

McClean Hospital ("McClean") was subject to a fine with respect to a 2015 data breach, in which it potentially exposed the data of 1,500 employees, patients, and donors when it lost four, unencrypted backup tapes.[51] Specifically, the tapes were lost when an employee, who would regularly take eight unencrypted tapes home with her that contained PHI such as Social Security numbers, diagnostic information, and family medical histories.[52] However, once McClean terminated the employee she only returned four of the eight tapes, and McClean was never able to recover the remaining records. Accordingly, the Massachusetts Attorney General alleged that McClean failed to properly identify, assess, and plan for such a security risk and that it had failed to properly train employees on security practices.[53] Furthermore, the Massachusetts Attorney General also underscored that McClean did not properly encrypt devices nor did it even report the loss of the tapes in a timely manner.[54] Alongside a $75,000 fine, McClean also had to agree to implement and maintain a written security program, provide mandatory training to all employees, create and maintain an inventory of all of its portable devices, and encrypt each of these devices with PHI within 60 days.

IV. NEW DATA BREACH NOTIFICATION OBLIGATIONS UNDER HIPAA/HITECH ACT

A. HIPAA Updates

Perhaps one of the most notable HIPAA-impacted changes in the past few years was the adoption of the so-called "Interoperability and Patient Access" Rule.[55] This rule was designed to ensure that health information was made more easily available to patients by requiring covered entities to implement and maintain an application programming interface ("API") that allows patients greater access to apps that access PHI. Specifically, these APIs should allow patients to access claims data, clinical data, prover information, prescription and pharmacy information, and other directory information.[56]

Furthermore, as the COVID-19 Public Health Emergency came to an end in May 2023, a wide array of temporary HIPAA policies sunsetted. A couple examples of these policies include:

- Notification of Enforcement Discretion for Telehealth issued in January of 2021, which provided for lenient enforcement for good faith provision of telehealth services and technologies that did not fully comply with the HIPAA rules.[57]

- Notification of Enforcement Discretion Regarding Online Appointments, which similarly provided for no penalties or sanctions for entities that use online or web-based scheduling applications in good faith for scheduling COVID-19 vaccination appointments.[58]

- Notification of Enforcement Discretion for Good Faith Uses and Disclosures of PHI by Business Associates for Public Health and Health Oversight Activities in which sanctions were not imposed on business associates for disclosures of PHI for public health oversight so long as the business associates notified the covered entity within 10 days of the use or disclosure occurring.[59]

Currently, each of these enforcement discretion issuances are slated to expire 90-days after May 11, 2023. After that point, any healthcare provider operating in the space or offering the services will have to come within full HIPAA compliance.

HHS also issued new guidance for how HIPAA-covered entities should operate in the context of online tracking technologies (including advertisement tracking).[60] For context, tracking technologies are "used to collect and analyze information about how users interact with . . . websites or mobile applications." [61] In healthcare, covered entities (and even business associates) may often leverage such technologies to help analyze the use of their websites, improve the visitor experience to a website, and even determine effectiveness and success of marketing campaigns.

To that end, HHS does not have a blanket prohibition on the use of online tracking technologies in the healthcare context. The mere existence of tracking technologies alone is *not* an issue or a violation of HIPAA. Notably, the HHS guidance recognized that many healthcare providers rely on tracking technologies and acknowledge an acceptable use of such technologies even in the healthcare context. However, healthcare providers must ensure that they understand how these technologies operate and use them accordingly.

B. HITECH Act Updates

In 2021, the HITECH Act was amended to incorporate HIPAA Safe Harbor provisions that were meant to encourage health care entities to adopt "recognized security practices" in exchange for HHS refraining from encoring penalties and/or otherwise mitigation penalties.[62] Additionally, the amendment also provides for flexibility around shortening audit periods and reducing investigation burdens.[63] Healthcare providers are able to seek the benefits of this safe harbor if they can show that for the 12 months before the violation the covered entity adhered to section 2(c)(15) of the NIST standards—incorporating its best practices, guidelines, procedures, processes, and methodologies.[64] And for organizations that are unclear if they are in alignment with these standards, they should consider conducting a risk assessment to (1) identify current risks and vulnerabilities and (2) allow for targeted and more efficient operational adjustments.

C. Other Notable Rules and Changes

In 2017, the Confidentiality of Substance Use Disorder Patients Records (formerly Confidentiality of Alcohol and Drug Abuse Patients Records) extended the restrictions on confidentiality to include substance abuse disorder records controlled by "other lawful holders of patient identifying information."[65] Additionally, the new rule expanded a patient's right not to agree to disclosures of their personal information and to specifically outline what individuals or entities they want their information shared with.[66]

D. New HHS Unit

On February 27, 2023, HHS announced the formation of a new unit—the Health Information Privacy, Data, and Cybersecurity Division (HIPDC)—"to be more reflective of their work and role in cybersecurity."[67] The newly established division is expected to take a stronger role in cybersecurity and privacy related concerns. For instance, with unsecured PHI, there was an increase from 663 large breaches (500 or more individuals impacted) in 2020 to 714 large breaches in 2021.[68] At least 80 percent of large breaches are due to hacking.[69]

The HIPDC is expected to address the demand gaps arising from privacy and cybersecurity. Healthcare providers should take note as they can expect increasing regulatory focus on cybersecurity and privacy from the HHS. This may lead to anything from increasing compliance needs to additional enforcement activities by the HHS after a breach.

V. DATA BREACH NOTIFICATION OBLIGATIONS OF HEALTHCARE PROVIDERS UNDER MICHIGAN STATE LAW

In each state and territory in the United States there are individual statutes governing a healthcare providers notification obligations involving personal information. In Michigan, data breaches are governed by the Identity Theft Protection Act (Mich. Comp. Laws § 445.63, 72 et seq.). This regulation applies to any entity that maintains personal information of a Michigan resident, regardless of whether the entity was organized under Michigan law.

Much like other states, "personal information" means "the first name or first initial and last name linked to 1 or more of the following data elements of a resident of [Michigan]: (i) [s]ocial security number[;] (ii) [d]river license number or state personal identification card number[;or] (iii) [d]emand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts."[70] Alternatively, personal identifying information ("PII") is a broad term that includes:

> [a] name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other

> account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

A security breach under Michigan law means "the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals."[71] Notably this does not include a good-faith but unauthorized access by an employee or individual where the access was related to the activities of the entity so long as the individual did not misuse or disclose the personal information to any unauthorized person(s).[72] Accordingly, a healthcare provider is required to notify Michigan residents of a security breach when (i) the resident's PII was accessed by an unauthorized person and (ii) the breach is likely to cause identity theft or other losses to at least one affected resident.[73] This does not apply to a breach of encrypted data so long as the encryption key was not also extracted during the incident. This notification must be made to consumers "without unreasonable delay" and is required once a single Michigan resident has been involved in a security incident. Therefore, once a single unredacted record of personal information of a Michigan resident has been accessed by an unauthorized person then these obligations are triggered. As part of that process, a healthcare provider would be required to provide each Michigan resident with written notice in "clear and conspicuous" language that describes: (i) the security incident; (ii) the of types of personal information impacted; (iii) what steps the healthcare provider has taken to remediate and protect against future breaches; (iv) a phone number that the residences can call for additional information; and (v) a reminder for the resident to remain vigilant for fraud and/or identity theft.[74] Additionally, if a breach requires that more than 1,000 residents must be notified then the healthcare provider must also notify each consumer reporting agency of the security incident and must include the exact number of residents who received notices and when the notices were sent.

However, Michigan law does include a special provision for covered entities that are subject to HIPAA. Specifically, these a healthcare provider that is subject to and complies with HIPAA with respect to preventing unauthorized access to PHI and its requirements for notification shall be deemed in compliance with the state law.[75] Yet, it is important to know that not every state has such an exception, and thus, healthcare providers in Michigan must ensure that they examine each impacted state's data breach notification statute to make sure that they meet all of its notification obligations.

VI. BEST PRACTICES FOR HEALTHCARE PROVIDERS IN RESPONDING TO DATA BREACHES

Thankfully, since the 2016 iteration of *Data Breach Risks & Best Practices for Small and Mid-Size Healthcare Providers* the general best practices for healthcare providers in responding to data breaches have remained relatively consistent. Nonetheless, HHS has continued to issue guidance on what it generally recommends as its best practices—which we have summarized below.

HHS continues to call for healthcare providers to embrace clear and accessible data security and privacy policies and procedures, including, but not limited to data loss prevention, password, incident response, backup, and access control policies.[76] Similarly, during the implementation of

these policies and procedures, HHS encourages healthcare providers to identify critical components of their networks; develop and maintain business continuity, data security and privacy training, and communication plans; and to detail specific roles and responsibilities for data security and privacy personnel, particularly with respect to security incident response.

And after resolving a data breach, it is critical that healthcare providers do not cease their commitment to data security and privacy or their HIPAA/HITECH Act obligations. Instead, after a covered entity experiences a data breach, they should leverage a healthy mix of the following remedial actions to both mitigate the lingering challenges of the data breach and to reduce the likelihood of another breach:

- Implementing multi-factor authentication for remote access;
- Changing passwords and any other login-credentials;
- Removing access for dormant or terminated user accounts;
- Practicing data minimization and de-identification to the greatest extent possible;
- Revising data security and privacy policies and procedures;
- Retraining all employees on how to handle PHI and how to prevent/detect data breaches;
- Maintaining an asset inventory;
- Penalizing employees who violate(d) PHI policies and procedures, including, if necessary potential termination;
- Enhancing encryption, particularly on any portable devices such as flash drives or cellphones;
- Implementing, testing, and appropriately segregating data backups and recovery options;
- Performing a risk assessment;
- Conducting regular audits of IT infrastructure;
- Monitoring federal guidance for common vulnerabilities and exploits, and maintaining regular updates and patching schedules for all firewalls, anti-virus, and other programs;
- Assembling an internal team who are designated for (i) incident response, (ii) emergency communications, and (iii) technology troubleshooting;
- Reviewing and updating cyber insurance, with previously considered panel counsel; and
- Reviewing and revising any contracts involving PHI to include more detailed guidance for data breaches, addressing potential liability, specifying expected data protections, and outlining responsibilities for confidentiality and incident response.[77]

VII. CONCLUSION

The health care industry continues to be one of the most lucrative targets for threat actors, and will continue to be increasingly high value victims of data breaches. To that end, it remains more important than ever that healthcare providers take the necessary steps to minimize those risks and protect themselves and their customers from the harms and penalties associated with insufficient data security and privacy practices. Furthermore, as state and federal regulators continue to crackdown on data security and privacy regulations it remains crucial that small and mid-size

healthcare providers remain vigilant of their operational practices and ensure that their compliance infrastructure is well supported and high functioning.

---

[1] *See e.g.*, Monica McCormack, *Health Care Remains Top Target in 2022 ITRC Breach Report*, COMPLIANCY GROUP (January 25, 2023) <https://compliancy-group.com/itrc-breach-report-2022/> (accessed June 9, 2023).
[2] U.S. Department of Health & Human Services, *Annual, Summary of the HIPAA Privacy Rule* (Oct. 19, 2022) <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (accessed June 9, 2023).
[3] *HIPAA PHI: Definition of PHI and List of 18 Identifiers*, UC BERKELEY < https://cphs.berkeley.edu/hipaa/hipaa18.html> (accessed August 7, 2023).
[4] U.S. Department of Health & Human Services, *2022 Health care Cybersecurity Year in Review, and a 2023 Look-Ahead*, HHS (Feb. 9, 2023) p 6 <https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf> (accessed May 31, 2023).
[5] U.S. Department of Health & Human Services, *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2021* (2021) p 8 <https://www.hhs.gov/sites/default/files/breach-report-to-congress-2021.pdf> (accessed May 31, 2023).
[6] See *U.S. Department of Health & Human* Services, *A Cost Analysis of Health Care Sector Data Breaches Health Sector Cybersecurity Coordination Center (HC3)* (April 12, 2019), pp 4-5, <https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf> (accessed May 31, 2023); see also Luke Irwin, *What Is the Cost of a Health care Data Breach in the US?*, IT GOVERNANCE (July 7, 2021) < https://www.itgovernanceusa.com/blog/what-is-the-cost-of-a-health-care-data-breach-in-the-us#:~:text=According%20to%20the%20US%20Department,in%20losses%20of%20%2413%20billion> (accessed May 31, 2023).
[7] *Cost of a Data Breach Report 2022*, IMB (July 2022), p 11 <https://www.ibm.com/downloads/cas/3R8N1DZJ> (accessed May 31, 2023).
[8] ABA Banking Journal, *Data Breaches Grow Costlier for Financial Institutions*, <https://bankingjournal.aba.com/2022/07/data-breaches-grow-costlier-for-financial-institutions/> (accessed July 5, 2023).
[9] *The 2020 Health Care Cybersecurity Report*, HERJAVEC GROUP (2020), p 3, < https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf> (accessed May 31, 2023).
[10] Susan Morse, *Health Care's Number One Financial Issue Is Cybersecurity* (July 30, 2019) https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity#:~:text=four%20to%20seven%20percent%20of,information%20being%20in%20electronic%20form. (accessed August 7, 2023); see also *Share of cyber security budget out of current IT budget in U.S. health care organizations as of 2021*, STATISTA (February 2023) < https://www.statista.com/statistics/856300/cyber-security-budget-share-in-health-organization-in-us/> (accessed May 31, 2023).
[11] *Supra* note 7.
[12] HHS, *supra* note 4; *Most Common Types of Health Care Data Breaches*, DEFINITIVE HEALTH CARE (January 31, 2023) < https://www.definitivehc.com/resources/healthcare-insights/most-common-healthcare-data-breaches#:~:text=Hacking%20and%20IT%20incidents%20have,over%20the%20last%20few%20years> (accessed May 31, 2023).
[13] *Id.*
[14] *Id.*; McCormack, *supra* note 2.
[15] Andrew Magnusson, *What Are the Penalties for Violating HIPAA? (Civil & Criminal)*, <https://www.strongdm.com/blog/hipaa-violation-penalties> (accessed May 31, 2023).
[16] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties*, 84 Fed Reg 18151 (April 30, 2019).
[17] *Id.*
[18] Steve Alder, *What Are the Penalties for HIPAA Violations*, HIPAA J. (Mar. 1, 2023) <https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/> (accessed May 31, 2023).
[19] *Id.*
[20] *HIPAA Violation Fines*, HIPAA J. <https://www.hipaajournal.com/hipaa-violation-fines/> (accessed May 1, 2023).

[21] U.S. Department of Health & Human Services, *Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA*, (July 15, 2022) <https://www.hhs.gov/about/news/2022/07/15/eleven-enforcement-actions-uphold-patients-rights-under-hipaa.html> (accessed May 31, 2023).
[22] *Supra* note 20.
[23] *Id.*
[24] U.S. Department of Health & Human Services, *Banner Health Resolution Agreement and Corrective Action Plan*, (Dec. 21, 2022), < https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health-ra-cap/index.html> (accessed May 31, 2023); see also Stephanie Innes, *Banner Health paid $1.25 million to resolve federal data breach probe*, AZ CENTRAL (Feb. 3, 2023) <https://www.azcentral.com/story/money/business/health/2023/02/04/banner-health-paid-1-25-million-to-resolve-federal-data-breach-probe/69871530007/> (accessed May 31, 2023).
[25] *Id.*
[26] U.S. Department of Health & Human Services, *Banner Health Resolution Agreement and Corrective Action Plan*, (Dec. 21, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health-ra-cap/index.html> (accessed August 7, 2023).
[27] *Id.*
[28] U.S. Department of Health & Human Services, *Oklahoma State University—Center for Health Sciences (OSU-CHS) Resolution Agreement and Corrective Action Plan* (May 5, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/osu-ra-cap/index.html> (accessed August 7, 2023).
[29] *Id.*
[30] U.S. Department of Health & Human Services, *Resolution Agreement In the Matter of The United States Department of Health and Human Services, Office for Civil Rights, Transaction No. 20-396202* (July 15, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial-hermann-roa-ra-cap/index.html> (accessed August 7, 2023).
[31] *Supra* note 20.
[32] *Supra* note 28.
[33] *Id.*
[34]U.S. Department of Health & Human Services, *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History*, (October 15, 2018), available at <https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach#:~:text=Anthem%2C%20Inc.%20has%20agreed%20to,after%20a%20series%20of%20cyberattacks> (accessed August 7, 2023).
[35] *Id.*
[36] *Id.*
[37] U.S. Department of Health & Human Services, *Anthem Resolution Agreement*, (Oct. 15, 2018).
[38] U.S. Department of Health & Human Services, *Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People* (January 15, 2021).
[39] *Supra* note 37.
[40] U.S. Department of Health & Human Services, *Touchstone Medical Imaging Resolution Agreement and Corrective Action Plan* (April 5, 2019), available at <https://www.hhs.gov/sites/default/files/tennessee-diagnostic-medical-imaging-services-ra-cap.pdf> (accessed August 7, 2023).
[41] U.S. Department of Health & Human Services, *Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients' protected health information* (May 6, 2019).
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Pennsylvania v DNA Diagnostics Center, Inc*, No 230201521, (Pa Cmwlth February 2023).
[46] *Id.* at 3.
[47] *Id.* at 2.
[48] *Id.* at 4.
[49] *Id.* at 7–13.
[50] *Id.*
[51] Massachusetts Office of Attorney General, *McLean Hospital to Implement New Security and Training Programs After Data Breach Exposed Sensitive Health Information* (Dec. 19, 2018) <https://www.mass.gov/news/mclean-

hospital-to-implement-new-security-and-training-programs-after-data-breach-exposed-sensitive-health-information> (accessed June 6, 2023).
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *See* U.S. Department of Health & Human Services, *Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers*, 85 Fed Reg 25510 (May 1, 2020).
[56] *Id.*
[57] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (January 20, 2021).
[58] U.S. Department of Health & Human Services, *Enforcement Discretion Regarding Online or Web-Based Scheduling Applications for the Scheduling of Individual Appointments for COVID-19 Vaccination During the COVID-19 Nationwide Public Health Emergency*, 86 Fed Reg 11139 (February 24, 2021).
[59] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19* (April 2, 2020), available at <https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf> (accessed August 7, 2023).
[60] HHS has described these "tracking technologies" as technology, such as a script or code, that is "used to collect and analyze information about how users interact with regulated entities' websites or mobile applications." U.S. Department of Health & Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (December 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (accessed August 7, 2023). Common examples of these tracking technologies that healthcare providers should be cognizant of are cookies, web beacons, session replay scripts, and embedded mobile-app trackers. *Id.*
[61] *Id.*
[62] Steve Adler, *What is the New HIPAA Safe Harbor Law?*, THE HIPAA JOURNAL (November 10, 2022) <https://www.hipaajournal.com/hipaa-safe-harbor-law/#:~:text=The%20new%20HIPAA%20Safe%20Harbor%20Law%20(HR%207898)%20was%20signed,and%20extent%20of%20HIPAA%20audits.> (accessed June 6, 2023).
[63] *Id.*
[64] *Id.*
[65] Steve Adler, *HHS Issues Final Rule on Confidentiality of Alcohol and Drug Abuse Patient Records Regulations*, THE HIPAA JOURNAL (Jan. 19, 2017) <https://www.hipaajournal.com/hhs-issues-final-rule-on-confidentiality-of-alcohol-and-drug-abuse-patient-records-regulations-8653/> (accessed June 6, 2023).
[66] *Id.*
[67] U.S. Department of Health & Human Services, *HHS Announces New Divisions Within the Office for Civil Rights to Better Address Growing Need of Enforcement in Recent Years* (February 27, 2023) <https://www.hhs.gov/about/news/2023/02/27/hhs-announces-new-divisions-within-office-civil-rights-better-address-growing-need-enforcement-recent-years.html> (accessed June 19, 2023).
[68] *Id.*
[69] *Id.*
[70] MCL 445.63(3)(r).
[71] MCL 445.63(3)(b).
[72] *Id.*
[73] MCL 445.72.
[74] *Id.*
[75] *Id.* 445.72(10).
[76] U.S. Department of Health & Human Services, *supra* note 6, p. 7–8.
[77] *Supra* note 6, p. 14.