Access at the Expense of Privacy in the Emerging App Economy

December 7, 2021

AHIOS Authors:

Elizabeth McElhiney, MHA, CHPS, CPHIMS, CRIS
Secretary of AHIOS
Privacy and Security Officer at ScanSTAT Technologies

Carlos Rodriguez, MBA
Marketing Coordinator of AHIOS
Vice President of Health Information Management Services at VitalChart

Glossary of Terms

API – Application Programming Interfaces are messengers or translators that work behind the scenes to help software programs communicate with one another. APIs have become an integral part of both our personal and business worlds. The Office of the National Coordinator for Health Information Technology (ONC) has adopted API certification criteria for electronic health records (EHRs) to help enable access to health information for clinical and patient-facing uses.

EHI – Electronic Health Information, refers to patient data stored in electronic form that are collected and shared for healthcare delivery and public health purposes.

EHR – Electronic Health Record

ePHI – ePHI is any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media.

HIPAA – Health Insurance Portability and Accountability Act of 1996

HIT – Health Information Technology

Information Blocking – Information Blocking is defined as the intentional withholding (a practice that is likely to interfere with, prevent or materially discourage access, exchange, or use) of patient health information by an act either from provider to provider, or from provider to patient. Info blocking rules apply to portals and apps but not to information received from Health Information Management (HIM) or a Release of Information (ROI) vendor.

mHealth – mHealth is an abbreviation for mobile health, a term used for the practice of medicine and public health supported by mobile devices. The term is most commonly used in reference to using mobile communication devices such as mobile phones, tablets, and wearable devices such as smart watches, for health services, information, and data collection.

Protected Health Information (PHI) – as defined by the Privacy Rule, is any information within a person's medical record that can identify them and is held by a covered entity. Under HIPAA and the Privacy Rule, there are 18 specific identifiers that must be handled with certain safeguards.

TABLE OF CONTENTS

Introduction

There is little debate that health care provider and patient access to protected health information (PHI) has significantly improved since HIPAA was signed into law in 1996. As with many periods of substantial progress, consequences resulted from the guaranteed access to PHI enumerated in HIPAA and subsequent regulatory and legislative efforts. These consequences have often – unintentionally – resulted in greater risks to the privacy and security of a patient's health data. Significant privacy challenges lie ahead with the skyrocketing growth of mobile health apps as the industry works towards delivering an "app economy" that provides patients, providers and payers with enhanced innovation and choice.

This white paper, "Access at the Expense of Privacy in the Emerging App Economy", is intended to provide education, insights, and best practices for health care providers and organizations regarding how to safeguard patient privacy during this period of unprecedented growth in mHealth apps and access-driving regulations and initiatives.

This paper will provide a brief history of HIPAA to provide the context for today's environment, describe what it means to be "standing in the shoes of the patient" when fulfilling medical record requests, provide real world examples of where increased access from mHealth apps have threatened patients' privacy, and provide AHIOS' recommended best practices for protecting patients' privacy in light of recent access enhancing regulations.

The History, Purpose and Intent of HIPAA

It is helpful to understand the initial intent or purpose of regulations or laws before examining how it is implemented in the current environment. This section will review the initial purpose of HIPAA as well as the impetus for revisions to, and expansion of,

HIPAA. These efforts formed the foundation for modern health care privacy. Here's a brief look at the history of HIPAA from the initial legislation to the present day.

The Beginnings of HIPAA

HIPAA was signed into law by President Clinton in 1996. The original purpose of the legislation was to assist more Americans in obtaining health insurance coverage and ensuring that employees would not lose their health insurance if they changed jobs. Within the larger document, lawmakers charged the Department of Health and Human Services (HHS) with devising privacy and security standards for the safeguarding of individually identifiable health information if Congress failed to do so within a specified time period. Consequently, HHS drafted and enacted the Privacy Rule and Security Rule to enumerate a patient's rights with regard to their PHI as well as the standards that were required to maintain the confidentiality, integrity, and availability of ePHI. Additional modifications were made to HIPAA through further regulatory actions and legislation including the Enforcement Rule, HITECH Act, Breach Notification Rule, the 2013 Final Omnibus Rule, and the 21st Century Cures Act. A brief overview of the additional legislation and regulations follows.

The HIPAA Privacy Rule: Effective in April 2003, the main goal of the Privacy Rule is to ensure that an individual's health information is well protected but within a framework that still enables the information flow between the parties that must access PHI in order to provide the highest quality of care available. The Privacy Rule additionally enumerated the rights that patients had over their PHI – to request an amendment of their record, to request an accounting of disclosures, to request a restriction of their record, to access a copy of their record, and request an alternate form of communication.

The HIPAA Security Rule: The Security Rule became effective in 2005. The purpose of this amendment was to secure the confidentiality, integrity, and availability of an individual's electronic personal health Information (ePHI). The HIPAA Security Rule contains three types of required and addressable (adjustable) standards of safeguard that all business associates and covered entities must utilize. There are Administrative, Physical, and Technical safeguards.

The HIPAA Enforcement Rule: In March of 2006, the HIPAA Enforcement Rule was drafted and enacted after it was determined that many covered entities were not fully complying with the Privacy and Security Rules. This rule allows HHS' Office for Civil Rights to investigate complaints that have been made about covered entities' non-compliance with HIPAA. This Rule also empowered HHS to fine these entities for breaches of Electronic Protected Health Information (ePHI) that were avoidable if the covered entity had implemented the appropriate Security Rule safeguards.

The HITECH Act: A significant update to HIPAA was the passage of the Health Information Technology for Economic and Clinical Health, or HITECH Act. It was signed into law in February 2009 as part of the American Recovery and Reinvestment Act (ARRA) and its purpose was to encourage healthcare providers to adopt Electronic Health Records (EHRs) and supporting technology. The HITECH Act provided financial incentives to motivate hospitals and other healthcare providers to adopt EHRs. The adoption of EHRs was intended to simplify the transfer of PHI between health care providers or organizations, improve administrative efficiency, and increase patient involvement in their health care.

In addition to the creation of the Meaningful Use program, the HITECH Act further defined patients' rights with regard to their PHR. Under the HITECH Act, patients' right to obtain their own health data in an electronic format and at a reasonable, cost-based fee was established. These rights were related to the process of transferring PHI between health care providers or organizations as well as to promote patient involvement in their health care. The HITECH Act provided for direct regulation of business associates by requiring them to comply with the Privacy and Security Rule as well as made business associates liable to their covered entity partner for violations of the business associate agreement.

The Breach Notification Rule: In September of 2009, the Breach Notification Rule was passed. It mandates that any breach of ePHI by a covered entity and their business associates that affects 500 or more individuals be reported to the Office of Civil Rights (OCR) and notice must be sent to any individuals that could be affected by the breach. The Breach Notification Rule lays out what a breach is, who needs to be notified that one happened and what penalties there are for violations. This came after many years where HIPAA was in place but was not being carefully followed by covered entities and their associates.

The HIPAA Final Omnibus Rule: The HIPAA Omnibus Rule became effective in 2013. It contained edits, updates, and modifications to the prior rules that were intended to enhance confidentiality and security in data sharing. One of the most significant changes was that business associates were now directly liable for any HIPAA violation.

The 21st Century Cures Act: A Separate But Related Act to HIPAA

The 21st Century Cures Act (Cures Act), effective on April 5, 2021, was a separate piece of legislation that was still related to HIPAA. Intended to promote consumer-focused health care and encourage competition between Health Information Technology (HIT) vendors, the Cures Act promoted interoperability between health care providers, across platforms, as well as between health care providers and patients. Under the Interim Final Rule, patients are entitled to access all their electronic health information (EHI), structured and/or unstructured, in a form that is convenient for them.

The Interim Final Rule enables the health care system to deliver an "app economy" that provides patients, physicians, hospitals, payers, and employers with innovation and choice. Through smartphones and software apps, patients will have more convenient and easier options to gain on-demand access to their electronic health information (EHI) whenever and wherever they need it. In addition, there will be the increasing ability for patients to choose apps that will assemble and read their records.

While the Final Rule of the Cures Act provides for some of the most sweeping enhancements to patient access via new technology tools (APIs, apps, etc.), these innovations need to be carefully vetted to ensure the requisite safeguards are in place to secure patient privacy.

Key Dates in HIPAA History

August 21, 1996:	HIPAA is signed into law by President Clinton
April 2003:	HIPAA Privacy Rule becomes effective
April 2005:	HIPAA Security Rule goes into effect
March 2006:	HIPAA Enforcement Rule effective
February 2009:	HITECH Act Signed into law by President Obama
September 2009:	Breach Notification Rule becomes effective
March 2013:	Final Omnibus Rule effective
April 2021:	21st Century Cures Act effective

Standing in the Shoes of the Patient

HHS Office for Civil Rights (OCR) has clearly established that a patient may direct their information to a representative that is making medical decisions on behalf of the patient as that personal representative is "standing in the shoes of the patient." In the "patient directive" scenario, the patient's personal representative would be charged under the patient cost-based fee or an established safe harbor of a $6.50 flat fee. The Privacy Rule delineated who was empowered to serve as a patient's personal representative at §164.502(g)(2) and a third- or fourth-party must provide evidence of their standing under the Privacy Rule to requests records. The intent was to ensure those individuals representing patients may be able the access the PHI necessary to make appropriate care decisions on behalf of the patient.

An unintended consequence was that third- or fourth-party requestors have tried to take advantage of the patient directive to obtain the patient's medical records at the patient safe harbor rate. For any directive received from a third- or fourth-party without the appropriate documentation stated above, the recipient would be obligated to view the directive as a third party designee whereby the patient safe harbor rate would not be applicable and any applicable state rates would govern fees (45 C.F.R. 164.524(c)(3)(ii). In an effort to further their case, third- and fourth-party requestors would often file complaints with hospital and practice administrators as well as the OCR.

A 2016 guidance issued by HHS serves as the origin of the debate surrounding patient directives and the impetus for third- and fourth- parties to utilize these directives. At the time of writing, HHS included the third-party directive in their recent Notice of Proposed Rulemaking (NPRM) regarding modifications to the Privacy Rule despite the US District Court for the District Court vacating the guidance in 2020. HHS' reintroduction of the third-party directive provisions is counterproductive to the department's stated goal of increasing access to medical records with little or no cost to the patient or designated personal representative. While there is great detail in the decision invalidating the expansion of the third-party directive, the memorandum opinion noted that Congress had opted for a more limited scope for third-party directives than the interpretation envisioned and enacted by HHS. The narrower scope should be construed as deliberate as Congress built the HITECH Act upon language and concepts delineated a decade earlier and had the

requisite institutional knowledge to incorporate a wider scope if it deemed it appropriate.[1]

The paternalistic imposition of HHS' interpretation of the 2013 Omnibus Rule and 2016 Guidance resulted in a period of substantial uncertainty and concern within the health care industry. The resulting chaos resulted in many health care organizations opting to take a conservative approach in order to avoid spurious and intimidatory complaints made to OCR by third-parties seeking to avail themselves to rates and demand PHI formats they were never meant to receive. The acceptance of third- and fourth-party directives removes the privacy protections provided by the HIPAA Privacy Rule. The timing of HHS' approach is curious in that the continued COVID-19 public health emergency, compounded with various natural disasters and the implementation of Information Blocking provisions, make this an inopportune time to engage in a notice and comment period for health care stakeholders. Present circumstances would provide a substantial barrier to the participation of health care providers, organizations, and their business associates.

Health care stakeholder input is essential for this particular rulemaking endeavor as the current state of privacy laws within the United States are inconsistent and wide-ranging in their scope. Recent articles have raised ethical concerns, particularly regarding vulnerable populations and the safety of personal data during a rapid increase in data sharing between covered entities, business associates, and other third-parties[2].

While EHRs are invaluable at keeping patients involved in their health care, the risk of inappropriate disclosure is increased with the change from paper records to electronic format due to mismanagement and external factors such as ransomware[3]. Additional risk factors to maintaining privacy include rapidly changing laws and technologies, immature information governance models, and weak policies for sharing aggregate health data[4]. The input of stakeholders will be necessary to avoid clear risks observed both in the United States and internationally.

Patient Access: When Things Go Wrong

As previously established, improved patient access to their health care data is essential to increased patient involvement in their care and improved clinical outcomes. The most recent significant gains in increasing patient access to EHI include the Interoperability Rule and the Information Blocking provisions. The increased access gained by promoting interoperability is intended to reduce the number of duplicative diagnostic tests and ensure high-quality decision-making by health care providers. As previously discussed, the increased access to EHI may come with an unintentional increase in risk to a patient's privacy.

Recent scholarly literature as well as the larger, popular media have generated a robust and growing body of research regarding the rapid adoption of mHealth technology and expansion of affordable, available technologies has contributed to a gap between the current environment and existing legislation. This discrepancy was only exacerbated by the COVID-19 pandemic and the promulgation of electronic solutions to assist with remote work, patient monitoring, and other pressing needs. AHIOS supports state, federal, and international initiatives to strengthen patient access to their medical records; however, AHIOS is concerned about the degree to which unintended consequences of regulations and legislation can result in increased risk to a patient's privacy.

Adding to the gap between outdated laws and modern technology, the common perception of HIPAA to an individual is not aligned with the reality of the scope of HIPAA and subsequent legislation. This discrepancy leads people to believe that their PHI is protected when it is not covered. One common fallacy is that HIPAA compliance applies to any entity that obtains or handles protected health information (PHI), which is not correct.

[1] Ciox v. Azar, 435 F. Supp. 3d 30 (DDC 2020). Retrieved from https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51

[2] Chiruvella, V., & Guddati, A. K. (2021). Ethical issues in patient data ownership. *Interactive Journal of Medical Research, 10*(2), e22269. doi:10.2196/22269 https://www.i-jmr.org/2021/2/e22269

[3] Duckett, S. (2019). Australia's new digital health record created ethical dilemmas. *Healthcare Management Forum, 32*(3), 167-168. doi:10.1177/0840470419827719

[4] Kloss, L. L., Brodnik, M. S., & Rinehart-Thompson, L. A. (2018). Access and disclosure of personal health information: A challenging privacy landscape in 2016-2018. *Yearbook of Medical Informatics, 27*(1), 60. doi:10.1055/s-0038-1667071

Other organizations who are not subject to HIPAA laws include:

- Life insurance companies that request medical records for the purpose of underwriting
- Attorneys that request medical records for personal injury or workers' compensation litigation
- mHealth trackers such as physical devices worn on the body or apps on mobile devices
- Data brokers who purchase medical records for other purposes than continuity of care.

Covered entities often have large amounts of extremely valuable data making them targets for criminals. In addition, many health care organizations lag behind other industries in adopting and updating their hardware, software, or infrastructures despite the protections of the Privacy and Security Rules. Consequently, the health care industry is a natural target for criminals as cybersecurity for health care providers is dependent on some required elements and a multitude of scalable, addressable options. This results in vulnerable targets who have access to a trove of information that is available to the average Health Information Management (HIM) employee including patient name, date of birth, social security numbers, address, employer, phone number, email, next of kin, and credit card information.

The combination of safeguards in HIPAA covered entities and a wide array of unregulated entities has resulted an environment where unregulated third-parties are monetizing patient health data without any patient protections. There have been multiple instances of negative privacy consequences resulting from expediting development of software without implementing controls. The following examples demonstrate real-world examples of these negative implications:

- The COVID-19 global health emergency provides the context for the first example of where the need to access patient health data was not appropriately weighed against the need to protect patient privacy. A large metropolitan area in the Northeastern United States had entered into an arrangement with a third-party contractor to provide vaccinations to citizens. The city had not realized that the third-party was not covered by HIPAA and the contractor was subsequently found to be reselling patients' PHI. In order to protect citizen's privacy, the city elected to terminate the contract for vaccination services.

- Highmark, a major health plan in the United States, developed their internal innovation program – VITAL – into a commercial product where startups can test their products in a "real" clinical environment. One critical selling point for VITAL is that startups may access claims data from 4.5 million customers from 3 states[5]. As other organizations look to monetize their health data, patients must be aware that their PHI may be shared or sold to insurance companies, pharmacies, and researchers without the patient's knowledge or permission.

- A *New England Journal of Medicine* article, published in June 2021, argued that the most valuable thing within a hospital may not be excellent care or cutting edge technology but rather the substantial amount of patient health data stored in the hospital's EHR[6]. The authors then noted that hospitals, health plans, and other covered entities may monetize PHI after it was de-identified. PHI can be considered de-identified when 17 elements are removed from a patient's chart. An article published in *Becker's Health IT* one month later maintained that: "(E)ven with de-identification, patients can be re-identified fairly readily from datasets, for marketing and other purposes, using computational methods"[7] This begs the question - Should we treat de-identified data the same as HIPAA protected information?

- GoodRx, a mHealth app with over 10 million downloads on the Google Play Store, provides a current example of a large scale effort to monetize health data. The GoodRx app is used to provide price comparisons and coupons for patients. The health data, which includes the medication names being searched and other sensitive information, was sent to more than 30 other companies. A brief review of the recipient list showed that Google, Facebook, and a marketing company named Braze received health data from GoodRx as well as potentially

[5] Padmanabhan, P. (2019). The new innovation model: Monetizing healthcare data. *CIO,* Retrieved from https://www.cio.com/article/3433158/the-new-innovation-model-monetizing-healthcare-data.html

[6] Mandl, K. D., & Perakslis, E. D. (2021). HIPAA and the leak of "Deidentified" EHR data. *The New England Journal of Medicine, 384*(23), 2171-2173. doi:10.1056/NEJMp2102616

[7] Mitchell, H. (2021, June 23,). Monetizing EHRs with open data puts patients at risk. *Becker's Health IT* Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/physician-viewpoint-monetizing-ehrs-with-open-data-puts-patients-at-risk.html

identifiers which would let them link data to one user according to an article in Consumer Reports[8]. After this article was published, GoodRx issued a statement that they would not share information in Facebook and would appoint a new Vice President of Data Privacy, as well as implement a method to enable users to delete their data.

These four examples demonstrate the significant challenges of safeguarding patient privacy in the current healthcare environment where mHealth app development and use is skyrocketing. A *British Medical Journal* study reported that most of 20,000 mHealth apps sold on the Google Play Store collected and tracked user data; 28% of the mHealth apps were also in violation of the Google Play Store terms of service by not providing a privacy statement or notice[9]. The *British Medical Journal* is consistent with an analysis of 83 mHealth apps for older European adults published in *JMIR Aging*. The authors found that 49% of the surveyed apps contained no data or security safeguards; if safeguards were in place, they were not clear to users[10]. These analyses are especially concerning in light of research that shows that smartphones, and the mHealth apps utilized on them, increase an individual's likelihood to disclosing personal information[11].

AHIOS Recommended Best Practices

Staying aware of the current technology available and the growing number of laws and regulations to govern that information can be a daunting task for even seasoned privacy professionals. It is clear that patient privacy and access rights exist in a tenuous balance in both established areas, such as hospitals or EHRs, as well as the emerging mHealth app market. It is necessary to find a way forward that will allow health care providers and organizations to ensure patient access while protecting their patients.

Best Practices for Health Care Providers and Organizations

1. **Understand Who Can Access Your Data –** It is tempting to automate the sharing of data between different EHR platforms, billing and denial management software, and third/fourth party applications. The simplification of information sharing will – in a perfect world – reduce staff errors and time spent in data entry and reduce turnaround time, and improve patient engagement. However, it is necessary to vet downstream relationships in addition to business associates in order to determine that information is not being shared with a contractor that would sell patient data. It's an additional step to the security risk assessment but it's a necessary step in an increasingly interconnected and outsourced health care industry.

   It is also necessary to establish how the health care organization will be made aware of any potential data privacy and security issues. It should not be assumed that prompt notification is made when multiple parties are involved.

2. **Promote Patient Digital Literacy** – It is easy to discount this step and deem it "someone else's job." With the new information blocking provisions, health care organizations must accommodate reasonable requests for patient health record (PHR) software to connect with an organization's EHR. Promoting patient digital literacy is just good practice because engaged patients have better clinical outcomes. The extended benefits of digital literacy include patients utilizing mHealth apps from trusted vendors, lower IT expenditure as staff have fewer connections to maintain, and reduced risk for the health care organization through lowering the number of API connections.

   There are many resources available to health care providers and organizations that can be used to promote digital literacy, privacy awareness, and security best practices – even if the practice is small or no budget has been allocated for patient outreach. Organizations such as AHIOS (AHIOS.org) and the National Cyber Security Alliance (staysafeonline.org) as well as private companies have patient-facing materials that can be utilized.

3. **Choose an Opt-In Approach Rather Than an Opt-Out Approach** – It may be easier upfront for an organization to create an Opt-In Approach to patient portals; patients

[8] Germain, T. (2020, March 6). GoodRx saves money on meds--it also shares data with Google, Facebook, and Others. *Consumer Reports. shorturl.at/hxyN2*

[9] Tangari, G., Ikram, M., Ijaz, K., Kaafar, M. A., & Berkovsky, S. (2021). Mobile health and privacy: Cross sectional study. *BMJ (Online), 373*, n1248. doi:10.1136/bmj.n1248

[10] Portenhauser, A. A., Terhorst, Y., Schultchen, D., Sander, L. B., Denkinger, M. D., Stach, M., . . . Messner, E. (2021). Mobile apps for older adults: Systematic search and evaluation within online stores. *JMIR Aging, 4*(1), e23313. doi:10.2196/23313

[11] Melumad, S., & Meyer, R. (2020). Full disclosure: How smartphones enhance consumer self-disclosure. *Journal of Marketing, 84*(3), 28-45. doi:10.1177/0022242920912732

would not need to contact the organization to obtain an invitation or undertake multiple steps to participate after initially opting out. In the attempt to improve patient access, key privacy and ethical decision-making processes may be overlooked or avoided entirely[12]. For example, a health care surrogate may be assigned to make medical decisions on behalf of a temporarily incapacitated relative and would be granted access to the patient's portal account as their surrogate. When the patient has sufficiently recovered, the patient may not be aware that they have a patient portal account and who has been granted privileges to utilize it. Consequently, the patient may not know that they need to revoke access privileges for other individuals and applications that they were enrolled in without their knowledge.

4. **Require Patients to Confirm Their Third-Party Connections Periodically** – Patients may initially want to connect their third-party apps to an EHR for a multitude of reasons, including providing real-time data from mHealth wearables (e.g. glucometers or heart rate monitors). Eventually, the patient may switch devices or applications – and leaves an open, unused API connection between the EHR and the mHealth app. By asking patients to confirm they wish to retain the connection, health care providers and organizations may only maintain open connections with actively used mHealth applications and reduce their overall potential exposure.

5. **Have a Set Policy and Procedure for Handling "Risky" Apps** – If a health care provider is presented with a mHealth app that is a privacy and security risk to their network, the provider is not obligated to immediately permit API connectivity if it could compromise their network's security. It will be necessary to work with compliance and information security professionals to determine the minimum standards required to connect to an organization's programs. As information blocking provisions become more detailed, providers should take care to have a detailed policy and procedure for working with the mHealth app developer to reach an acceptable standard as well as a procedure for working with the patient to provide PHI in a mutually agreeable format in the interim.

[12] Duckett, S. (2019). Australia's new digital health record created ethical dilemmas. *Healthcare Management Forum, 32*(3), 167-168. doi:10.1177/0840470419827719

Summary & Conclusion

The health care industry has worked to ensure the privacy and security of patient's PHI while acknowledging the need for timely access for the appropriate, authorized individuals. The 25 years since the original passage of HIPAA has seen a rapid growth in the number and variety of health information technology solutions and their implementation. This growth has significantly exceeded the scope of HIPAA, its implementing regulations, and subsequent regulations and legislation, such as the HITECH Act and the Office of the National Coordinator for Health Information Technology (ONC) Interoperability Rule.

Concurrently, patients and health care providers have often not kept pace with the increased capabilities of mHealth devices, apps, and interoperability. As patients have sought out methods to both access and understand their health data, there has been a proliferation of mHealth and PHR options that were not created with HIPAA privacy and security standards in mind. Essentially, the patient's choice to use mHealth or PHR apps may not only provide the patient with their PHI but may also allow others to access and monetize the PHI of unaware patients.

As health care professionals and government regulators seek to improve patient access to their ePHI, it is critical that future efforts consider that individuals and health care providers do not often fully understand the capabilities of their EHR and the possible unintentional downstream effects of utilizing unregulated third-party applications. Until further regulations are enacted, it is necessary for health care providers to educate themselves and their patients in order to carefully balance the need for access with the need to ensure the privacy rights of patient.

About the Association of Health Information Outsourcing Services

Established in 1996, AHIOS is a trade association of leading health information outsourcing companies whose mission is to establish standards of excellence for the Release of Information (ROI) industry. AHIOS strives to achieve the highest levels of patient privacy throughout the ROI process by educating healthcare providers as well as federal and state agencies on the impact of legislative and regulatory initiatives and on the value that specialized ROI software and processes provide in safeguarding patient privacy and lowering healthcare costs. The association has developed a code of ethics, standards and professional values for HIM professionals; established the AHIOS Institute's Certified Release of Information Specialist (CRIS) competency program which tests ROI staff knowledge in protecting the confidentiality of patients' PHI; and continually works to educate the industry on how to remain in compliance with healthcare's complex and ever-increasing regulatory environment. For more information, visit us at www.AHIOS.org and follow us on LinkedIn and Twitter.

Disclaimer: This white paper is for informational purposes only and does not constitute legal advice. You should contact your attorney to obtain advice with respect to your specific issue or problem.