Security
Healthcare Security & Privacy

Expertise you can trust

Patient Access to Medical Records

Access to Medical Records *is a patient RIGHT!*

The number one complaint the Office for Civil Rights (OCR), the HIPAA enforcement agency, receives from patients is about providers and payers **not giving them access to their medical record**.

"**Information is key** to making good healthcare decisions. Understand your health history to ask better questions and make healthier choices. Track your lab results and medications, get X-rays and other medical images, or share your information with a caregiver or a research program," said Roger Severino, Director of the Office for Civil Rights (OCR) from his HIMSS presentation on February 12, 2019.

Elaborating further on the subject at the OCR/NIST 12th Annual HIPAA Conference in Washington D.C. in October, Director Severino confirmed that one of the OCR's top policy initiatives is to **enforce the rights of patients under the HIPAA Privacy Rule** and ensure that patients are given timely access to their health information.

That access must be at a reasonable cost: fees applied to an individual's request for access to their own records must be reasonable, and **those fee limits are strictly enforced**.

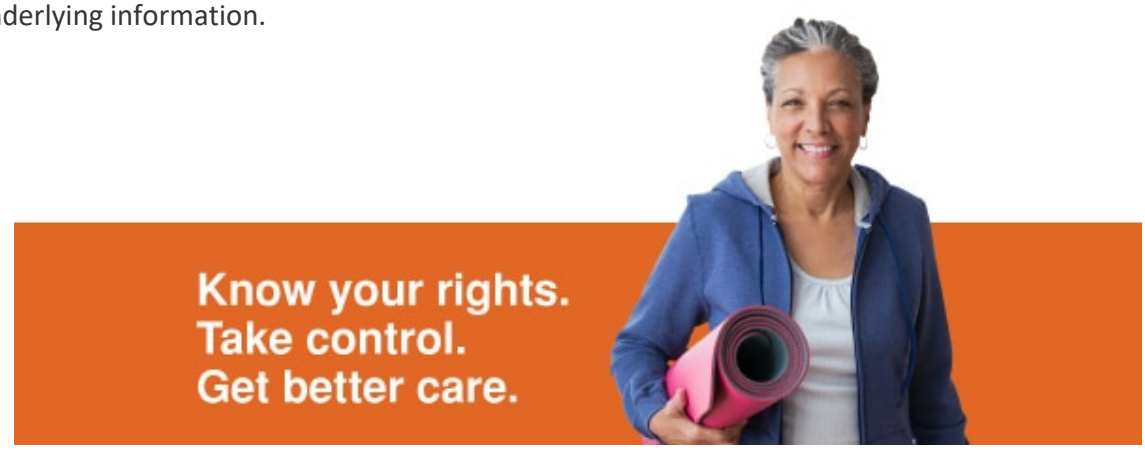
Failure to comply with the rules governing patient right of access have resulted in **fines and corrective action plans** for both large and small organizations:

Recent Actions

Incident Date	Organization	Reason Cited	Fine
Dec. 12, 2019	Korunda Medical, LLC Naples, FL	Not providing patients with access to their health data within 30 days of the request; allegedly did not provide the records in the format requested (electronic) to the patient's third-party designee; charged unreasonable fees.	**$85,000**
Sept. 9, 2019	Bayfront Health, St. Petersburg, FL	Not providing patients with access to their health data within 30 days of the request being received.	**$85,000**

The OCR's goal is for patients to actively be involved in their health care decisions. Therefore, one's health information should be obtained quickly, with no delays, accessible through the patient portal, with the capability to store on a smart phone so that records can freely be shared with care providers. The request should only be denied if the app poses a security risk to the covered entity.

It doesn't matter how old the PHI is, where it is kept, or where it originated. This includes clinical lab test reports and the underlying information.



What providers can do NOW!

Assess the current state

- Conduct a complete review of your Release of Information (ROI) workflow and policies related to requests for access to/copies of patient information.
- Identify pitfalls and complications such as mental health records, substance abuse records, HIV, family planning, and state regulations regarding minors.

Answer these questions

- How easy is it for patients to request their records?
- What is the typical turnaround time?
- What is the communication process?
- How are requests prioritized and documented?
- What is the EMR portal capability? Does it provide the information that patients typically request?

Take these steps FIRST

- If the ROI form requires patients to provide a reason or purpose to obtain their information, **revise the form.**
- Identify the organizational and operational risks, and document the remediation decisions.

Create a plan

- Develop a 'patient as consumer' privacy and security strategy that drives patient empowerment and which is aligned with the organization's business goals, and create a roadmap for achieving it.
- Recommend metrics—both strategic and tactical—for consumption by leadership and the board.

Conduct an independent validation

- Consider using "fresh eyes" to evaluate your processes, policies, and strategic and remediation plans.

Form and Format and Manner of Access

Not just any form and format…

"The Privacy Rule requires a covered entity to provide the individual with access to the PHI **in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed** to by the covered entity and individual ... If the individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format, or if not, in an agreed upon alternative, readable electronic format."

See "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/ *(February, 2016)*

…and not just any access!

"**Form and format** is an aspect of the law that is **very important to patients**, who often can't accept a fax or CD or for whom encrypting data could create a barrier (encryption can "stick" to the data and the password typically will expire within 30 days or less). OCR's guidance emphasizes that **patients can choose convenience over security in getting their records**, and providers (or their vendors) who ignore this aspect of a patient's request **are placing obstacles** in the path of patients exercising their HIPAA Right of Access."

See "New Release of The Patient Record Scorecard: Reasons for Optimism – But Still Too Much Noncompliance with HIPAA." www.ciitizen.com/new-release-of-the-patient-record-scorecard/ *(November 12, 2019)*

Need Help Getting Started?

Meet tw-Security.

Our experts have helped many organizations increase their programs' maturity, capability, and **compliance levels.**

We take an integrated approach that is tightly focused on efficiency, cost effectiveness, and achievement of **practical, measurable results** that drive value.

Since 2003, tw-Security, LLC has been a recognized leader and trusted advisor providing information security, privacy, and compliance services to the healthcare industry, covered entities, and business associates.

In fact, in a report on cybersecurity service advisory vendors conducted by an impartial healthcare research organization, **tw-Security ranked highest** among fully rated firms in *healthcare knowledge, ability to cater to their customers' needs, and strategic expertise.*

Relax. We've got this.

We are ready to partner with you to help you address your data privacy and patient access needs.

Office for Civil Rights (OCR) audit preparation services have been a tw-Security offering since the first HIPAA Audit Program Protocol was released in June 2012. We are experts in both **strategic planning and practical remediation** in the areas of data privacy, information security, and patient data access, among many others.

We can provide comprehensive information risk management and help you maintain and mature your compliance programs. We offer solutions ranging from a simple compliance remediation project, to support for your privacy policy team, up to providing a full Virtual Privacy Officer (VPO) engagement where tw-Security will act as the organization's trusted strategic and tactical advisor.

Meet the Experts

Joe D. Gillespie, MHS, RHIA, CHPS

Joe Gillespie has over 40 years of patient privacy experience and 20 years' experience with HIPAA Security.

Joe recently retired from the University of Kansas where he served as the HIPAA Privacy Official for the Lawrence campus. Also, Joe has served as the Director of Health Information Management at several hospitals across the country.

The Kansas Hospital Association published his master's thesis which served as the definitive resource on patient privacy and HIM practices in Kansas for over ten years.

Joe has been an active member in the American Health Information Management Association (AHIMA) since 1974, including membership on the Privacy and Security Practice Council. He is also a member of the International Association of Privacy Professionals (IAPP).

Susan M. Lucci, RHIA, CHPS, CHDS, AHDI-F

Susan Lucci has over 35 years of health information management (HIM) and HIPAA compliance leadership experience.

Susan currently serves on the AHIMA's Privacy and Security Practice Council and has spoken at national and state conventions on privacy and security.

Susan authored the Association for Healthcare Documentation Integrity's *HIPAA Compliance Guide & Quick Reference* (AHDI, 2017).

Susan also contributed to the AHIMA's 2014 Breach Management Toolkit, and to the book *Implementing Information Security in Healthcare: Building a Security Program* (Hertzig, et al., HIMSS, 2013).

Both Susan and Joe provide their expertise in patient privacy, incident response, breach management, and HIPAA compliance advisory and data security.

Let's Go!

Don't let inaction or indecision expose your organization to significant penalties. Act now to achieve compliance.

For more information:

To speak with one of our expert consultants, or to request a proposal, **Contact us today.**

Phone: 1-913-396-8321

Email: CustomerCare@tw-Security.com

Postal address: tw-Security, LLC | 6108 W. 121st Street | Overland Park, KS 66209

