Enabling GDPR Compliant Digital Workflows for Healthcare Providers

How to Improve Care and Boost Patient Engagement with a Data-Centric, User-First Approach to Security

virtru

Table of Contents

Digital Healthcare Opportunities vs. GDPR Compliance and Patient Confidentiality Challenges

Advances in modern medical technology and information systems have transformed the healthcare industry. As providers meet meaningful use requirements and evolve to value-based care systems, the introduction of new digital healthcare delivery models, cloud-based applications, and connected health devices has presented unique challenges and opportunities.

Mirroring remote workforce trends in other industries, digital health workflows allow distributed healthcare provider teams to more easily coordinate care and interact with their patients, leading to better outcomes. But these trends also bring significant risks to patient confidentiality. Multi-cloud environments that support digital care delivery leave protected health information (PHI) at risk of exposure, raising concerns regarding patient confidentiality and compliance.

The healthcare industry is no stranger to privacy regulations. In the US, healthcare privacy regulations are neatly packaged up in the Health Insurance Portability and Accessibility Act (HIPAA). Throughout the rest of the world, healthcare providers often had to patch together regulations, until the General Data Protection Regulation (GDPR) was introduced.

GDPR aims to not only consolidate privacy regulations, but also broaden the scope of data protection. Any data that is related to a person's physical or mental health, genetic makeup, or physical or behavioral characteristics is considered personal and protected under GDPR.

Inherent Risks in the Cloud

While the cloud transforms operations, it introduces substantial risks.

Across industries, organizations use an average of 78 different cloud-based applications every week. Yet security professionals are only aware of 38% of the applications known to IT administrators.

SOURCE: Data Security & Privacy in The Digital Workplace

Health workers need to share PHI rapidly, sometimes in life or death scenarios. This helps explain why over 60% of reported data breaches in the first half of 2019 were due to human error, and healthcare was affected more than any other sector.

SOURCE: Healthcare IT News

Widespread adoption of electronic medical record (EMR) systems has served a key role in making PHI accessible and secure. However, many care scenarios require immediate access to PHI, so health workers often take the path of least resistance and use email and file systems to share it—making email and file protection a centerpiece of any GDPR compliance and patient confidentiality program.

The demands of modern healthcare organizations reveal the inadequacies of traditional approaches to protecting data throughout the course of care. This guide offers a close look at a fictional scenario based on real healthcare use cases. It identifies key pain points associated with traditional data protection methods and uncovers how data-centric, user-first protections support rapid care delivery to optimize outcomes and keep patient data confidential and compliant.

GDPR Compliance Requirements

In order to comply with the GDPR Security Principle, 'appropriate technical safeguards' should be put in place to ensure the security of sensitive health data:

- **Encryption:** GDPR includes an explicit duty to consider encrypting personal data as part of an overall obligation to use "state of the art" security measures. As a result, encryption is effectively mandatory for sharing sensitive data, such as PHI.

- **Key Management:** GDPR's risk-based approach to cybersecurity implicitly requires organizations to consider the issue of key management—specifically preventing access by the cloud provider—as part of their overall policies for the protection of personal data.

- **Access Controls:** GDPR requires that organizations take control of the personal data they manage. Organizations must show they have adopted policies and procedures to ensure control of personal data. This includes privileges and restrictions for the information healthcare workers can and cannot access.

- **Audit:** GDPR emphasizes data accountability and audit. This includes developing processes that support the analysis of activity in the information systems that contain or use PHI, especially for assessing whether PHI has been breached.Organizations must keep records to show they are complying with GDPR requirements, and make those records available to regulators.

The Scenario: Digital Care Delivery and Coordination

Acme Health

Acme is a medium-sized healthcare organization focused on behavioral health and individualized care, with a mission to help their patients achieve their long-term health goals and live better lives. Acme recently implemented a range of new digital health technology tools to help streamline care delivery across distributed provider teams and ultimately improve patient engagement. This is in addition to G Suite to facilitate productivity and collaboration for Acme's distributed workforce.

Acme's commitment to its patients extends beyond physical health to digital health—specifically, patient confidentiality, privacy, and security. Trust is critical to the patient-provider relationship, especially throughout a long-term behavioral health program, and Acme sees keeping PHI secure as a key factor in patient trust. In addition, patient confidentiality isn't just the right thing to do, it's the law. The Acme leadership team takes GDPR compliance seriously, because violations do more than impact their bottom line; they erode patients' trust and negatively impact their mission.

GDPR Compliance Risks

Organizations in violation of GDPR can be subject to fines up to 20 million Euro or 4% of its annual revenue – whichever amount is greater.

Breach damages are more than financial: a study found that in the three years following a data breach, care delivery lagged, and patients had increased mortality rates.

SOURCE: Data breach remediation efforts and their implications for hospital quality

The Use Case: External and Internal PHI Sharing

The Stakeholders

Penelope is Acme's Health Administrator, helping physicians and specialist providers coordinate care with patients while facilitating patient engagement. When Acme's IT team began scoping requirements for a new electronic health records system (EHR) and patient portal, Penelope was a key stakeholder that helped assess how new digital workflows could support patient programs. She frequently shares PHI internally between different departments, and externally, both with patients and with Acme's extended network of specialist providers.

Brittany is a middle aged patient who partnered with Acme to take charge of her health after her primary care physician advised that she was at risk of developing diabetes and hypertension. Her Acme Health program prescribes weekly digital checkpoints via telehealth services and patient portal communications, plus monthly in-person visits with her care specialist.

Melissa is a Care Specialist with extensive prior experience across a variety of nursing disciplines. Melissa also serves as a liaison between priority patients and Acme's care providers, both internal and external, helping scale care delivery and optimize Acme's behavioral health model. Like Penelope, Melissa is a tech-savvy health professional committed to excellence in patient care. Melissa manages Brittany's health regimen and taps external care providers when necessary.

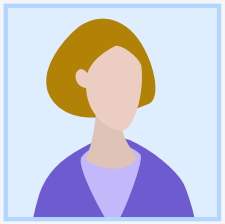
Evan is a Physician and Endocrinologist and serves as one of Acme's most trusted external care providers. Evan works with Acme as an out-of-network provider, as a way to extend the reach of his expertise and services beyond his small, stable private practice.

User Profiles

Penelope - Acme Health Administrator

- 34 year old healthcare professional.
- 10 years experience in healthcare administration, six years with Acme.
- Familiar with a broad range of health IT systems and digital health tools.

Brittany - Patient



- 55 year old patient at risk of diabetes and hypertension.
- Partnered with Acme to take a more proactive role in managing her health.
- Familiar with digital workflows but gets frustrated managing multiple accounts, often forgetting usernames and passwords.

During her weekly telehealth check-in, **Brittany** reported feeling lethargic throughout the previous week, so the Acme team had her visit the office for a quick check-up and blood tests.

Penelope now needs to share PHI even more frequently to give Brittany clear visibility into the test results and any changes to her existing care regimen, and facilitate PHI sharing with Melissa internally.

Melissa needs to share Brittany's test results and patient record with **Evan**, so he can review the results against her medical history and conditions. From there, Evan will recommend modifications to her care regimen and work with Melissa to implement them.

Pain Points with Traditional Approaches

As Penelope begins sharing the test results with Brittany, she recalls previous attempts to send important information via the patient portal that were unsuccessful. Brittany is often locked out of her account due to forgetting her username and password, or unable to access the account due to scheduled maintenance periods.

Brittany prefers email for communications in general—it's the digital tool she's most familiar with. When she gets frustrated with the patient portal, she often uses email as the path of least resistance to get in touch with Penelope.

Upon remembering that Acme has planned for scheduled IT maintenance in the coming days, Penelope decides to just send the test results to Brittany via Gmail and hopes her IT team has built protections into their email workflows. Ultimately she doesn't want to prevent Penelope from having easy access to the test results or contribute to unnecessary delays in Brittany's care delivery.

Melissa and Penelope also need to determine how to share Brittany's test results and patient history with Evan. Melissa doesn't feel comfortable sharing PHI with external providers without protections.

User Profiles

Melissa - Acme Care Specialist and Provider

- 38 year old healthcare provider.
- 15 years experience spanning a variety of nursing roles, three years with Acme.
- Familiar with a broad range of health IT systems and digital health tools, but has had to work with tech support on interoperability issues between the EHR and patient portal.

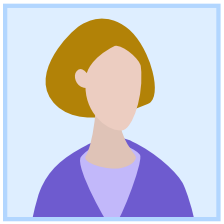
Evan - Out-of-Network Provider

- 55 year old physician and endocrinologist.
- Partnered with Acme to provide specialized medical expertise.
- Also owns and operates a small medical practice.
- Very little familiarity with digital health tools. Still relies on fax and paper records for most workflows and prefers email for digital care coordination.

How the Users Feel

Penelope is anxious

- She knows there are GDPR compliance risks with sharing PHI via email, but does so anyway to go with her patient-first philosophy.
- This scenario makes her feel like Acme's mission of serving patients is at odds with risks of breached PHI. By putting the patient first and making her data accessible, she compromises Acme's security posture.



Brittany feels frustrated and powerless:

- She wants to stay engaged with the Acme team, but it seems like the patient portal hardly ever works for her.
- The patient portal also feels like an unnecessary extra step—she gets a notification in her email when she has messages in the patient portal, so why can't Acme just send the message directly via email?

How the Users Feel

Melissa feels uneasy:

- Previous GDPR violations have taught Melissa to take PHI protection seriously, so she decides the best immediate approach is to provision Evan a new account within Acme's EHR system.
- After some push back, Acme's IT team makes an exception to their policies and creates Evan's account. Despite doing the right thing from a security & compliance perspective, she still has to plead with the IT team to provision a new EHR account for Evan.
- She recalls Evan has little experience with EHRs, so she is worried this step will extend his timeline and lead to costly care delays.

Evan is frustrated:

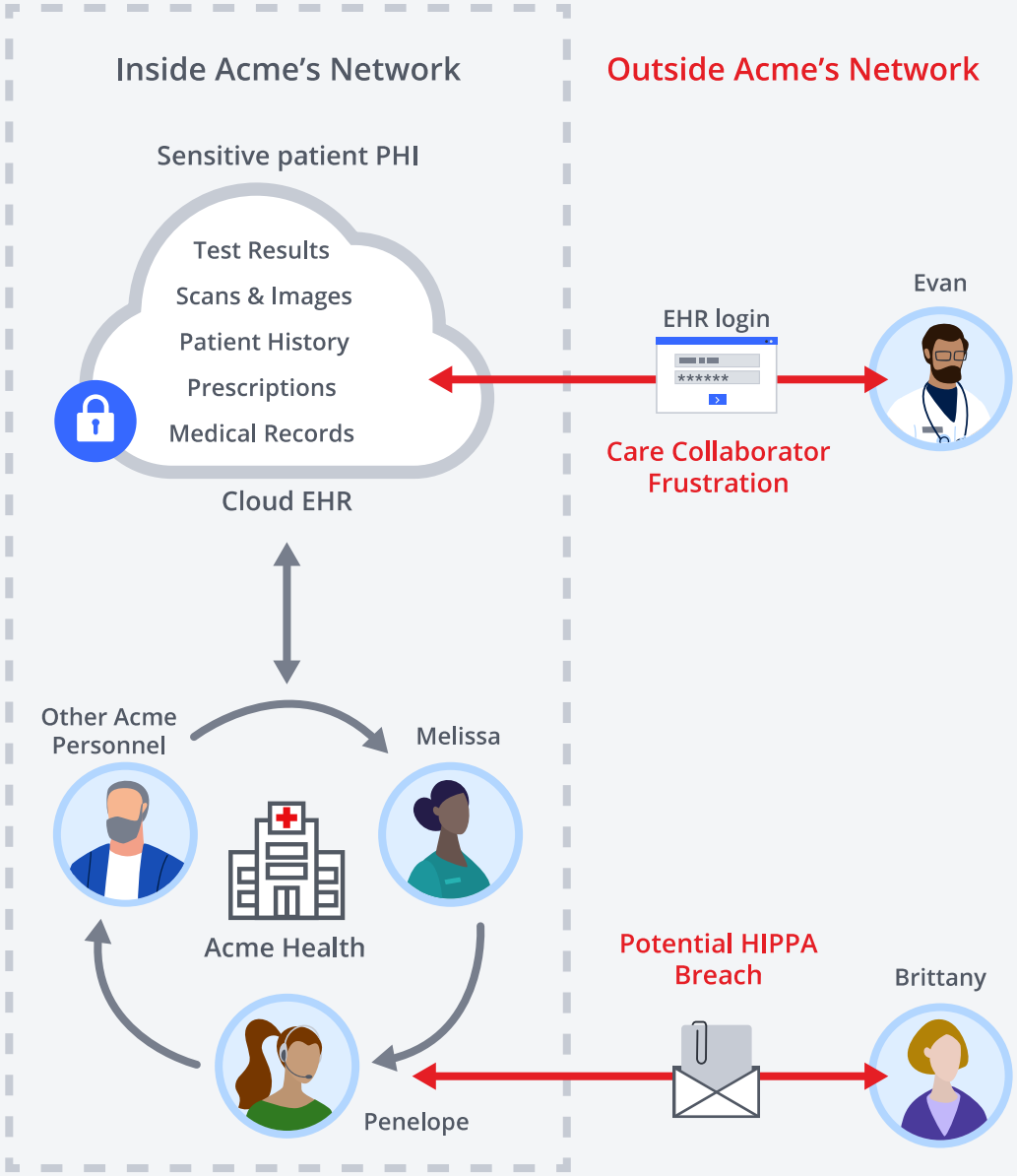
- Evan has never had a positive experience with EHR systems—"they get in the way of actually providing care." He'd rather coordinate care like he always has: faxes, emails, and phone calls.
- Evan begrudgingly registers his EHR account, but the application times out several times in the process, so he has to spend nearly an hour working with tech support.
- While he works through these technical issues, Evan's workload piles up. He has to prioritize the patients in his practice first, so he doesn't get to reviewing Brittany's test results and medical history until a day after Melissa shares it.

The Result

Acme will not have control or visibility of what Brittany does with the patient records. Penelope can only hope Brittany doesn't unwittingly expose her PHI to unauthorized access (and expose Acme to GDPR compliance risks in the process). Brittany's frustrations make her less engaged with Acme over time, which may inadvertently impact her health outcomes.

As Melissa and Evan work through the IT provisioning and enablement issues to get him access to Brittany's test results and medical history, precious time is wasted. If the blood tests end up revealing an acute health issue, the extra day it takes to review and prescribe care presents a missed care opportunity.

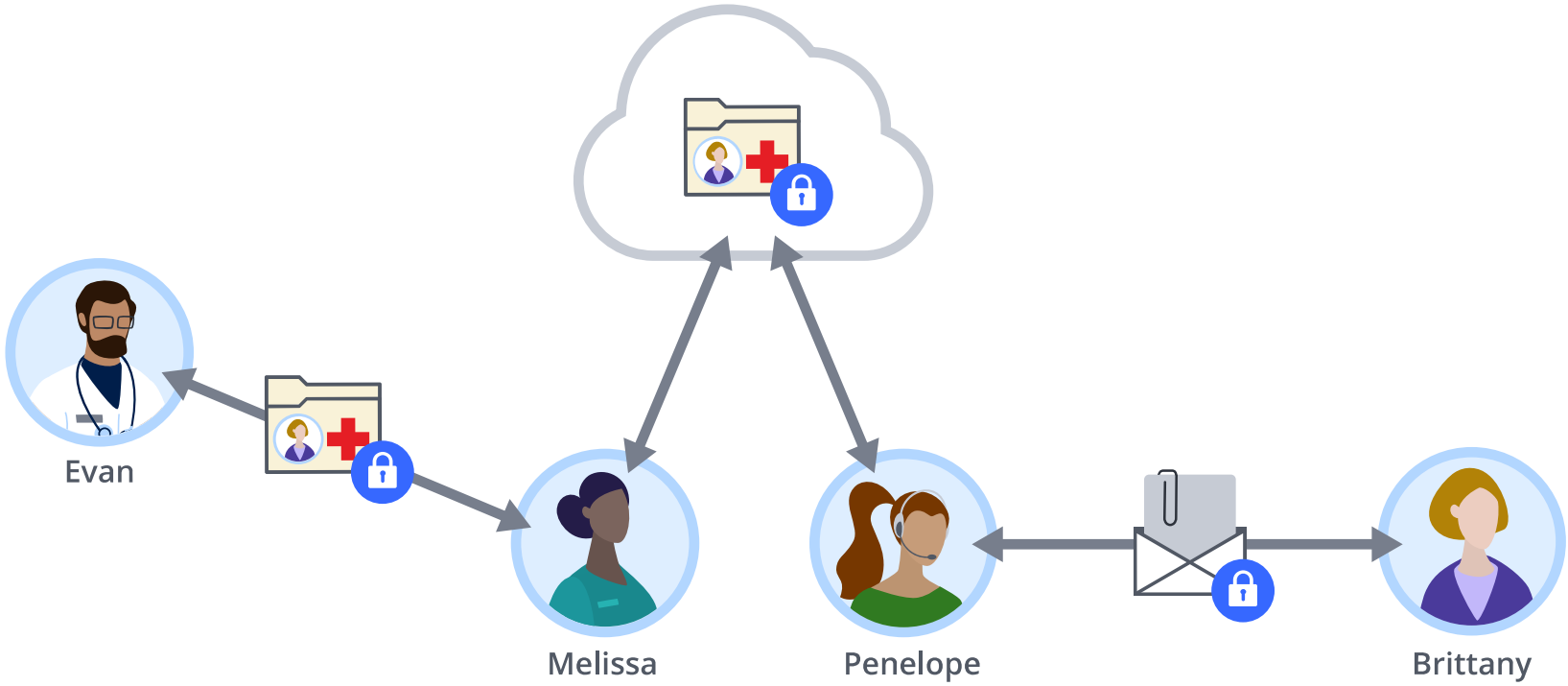
GDPR noncompliance risks and potential penalties will persist throughout the course of care, while the lack of easy, secure PHI access weakens patient engagement and leads to suboptimal care outcomes.



A Better Way: The Data-Centric, User-First Approach

Virtru's email and file protections offer data-centric security via end-to-end encryption that prevents unauthorized access and enables persistent control and visibility as PHI is shared. With data-centric security in place, protection, control, and visibility persist throughout the full care lifecycle, enabling better patient engagement and more rapid care collaboration, without sacrificing patient confidentiality and compliance. Virtru's user-centric approach also ensures protections are embedded directly into Acme's email and file workflows yet still protect files beyond G Suite, everywhere PHI is shared.

Now, Penelope can easily and securely share the test results with Brittany and coordinate her follow-up appointments via email, then upload Brittany's test results and medical history to Google Drive in a secure folder shared with Melissa. Similarly, Melissa can simply share the test results and medical history externally via email, Evan's preferred digital tool, to expedite care.

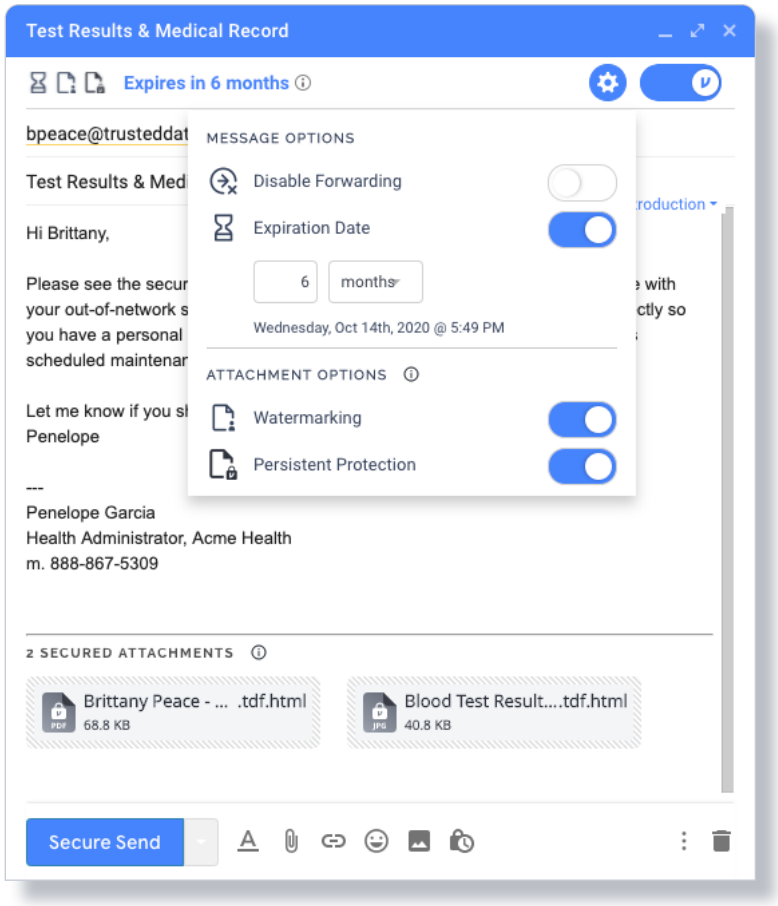


How the Users Feel Now

Penelope feels **EMPOWERED**.

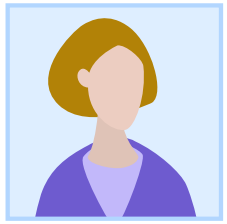
- Penelope simply attaches the test results to a Gmail message and enables Virtru's end-to-end encryption to prevent access by unauthorized parties to ensure confidentiality and GDPR compliance.

- Using Virtru's granular access controls, Penelope also:
  - Sets an expiration date for six months from now, after Brittany's initial Acme program concludes.
  - Adds watermarking, which puts any recipients' name across the background of the file to deter them from leaking it.
  - Applies persistent protection, which keeps the test result confidential and compliant even beyond the initial email, in case Brittany downloads it from email to her desktop.
- Throughout the course of care, Acme maintains visibility and control, and can always adjust the access controls as necessary.



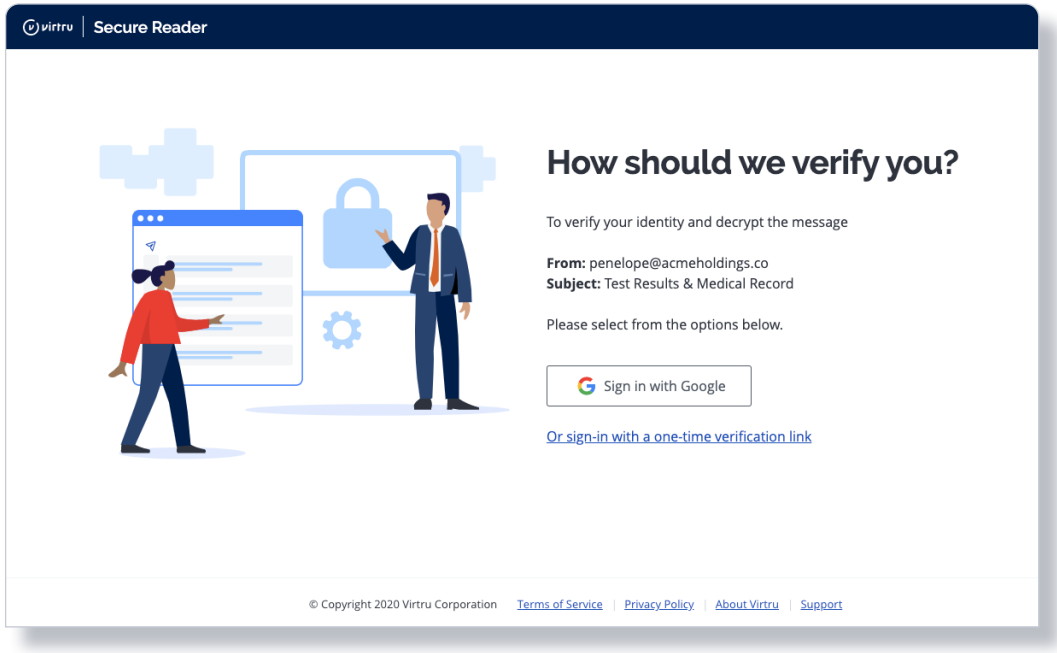
Virtru's easy end-to-end encryption protects PHI shared via email and files for patient confidentiality and GDPR compliance.

How the Users Feel Now



Brittany feels much more **CONFIDENT** in her care program.

- She gets her test results almost immediately via email, along with a message from Penelope with clear instructions on the follow-up steps she needs to take.
- She doesn't have to worry about dealing with another application, managing a new account, or remembering another password, she simply accesses the protected test result with the Virtru Secure Reader.

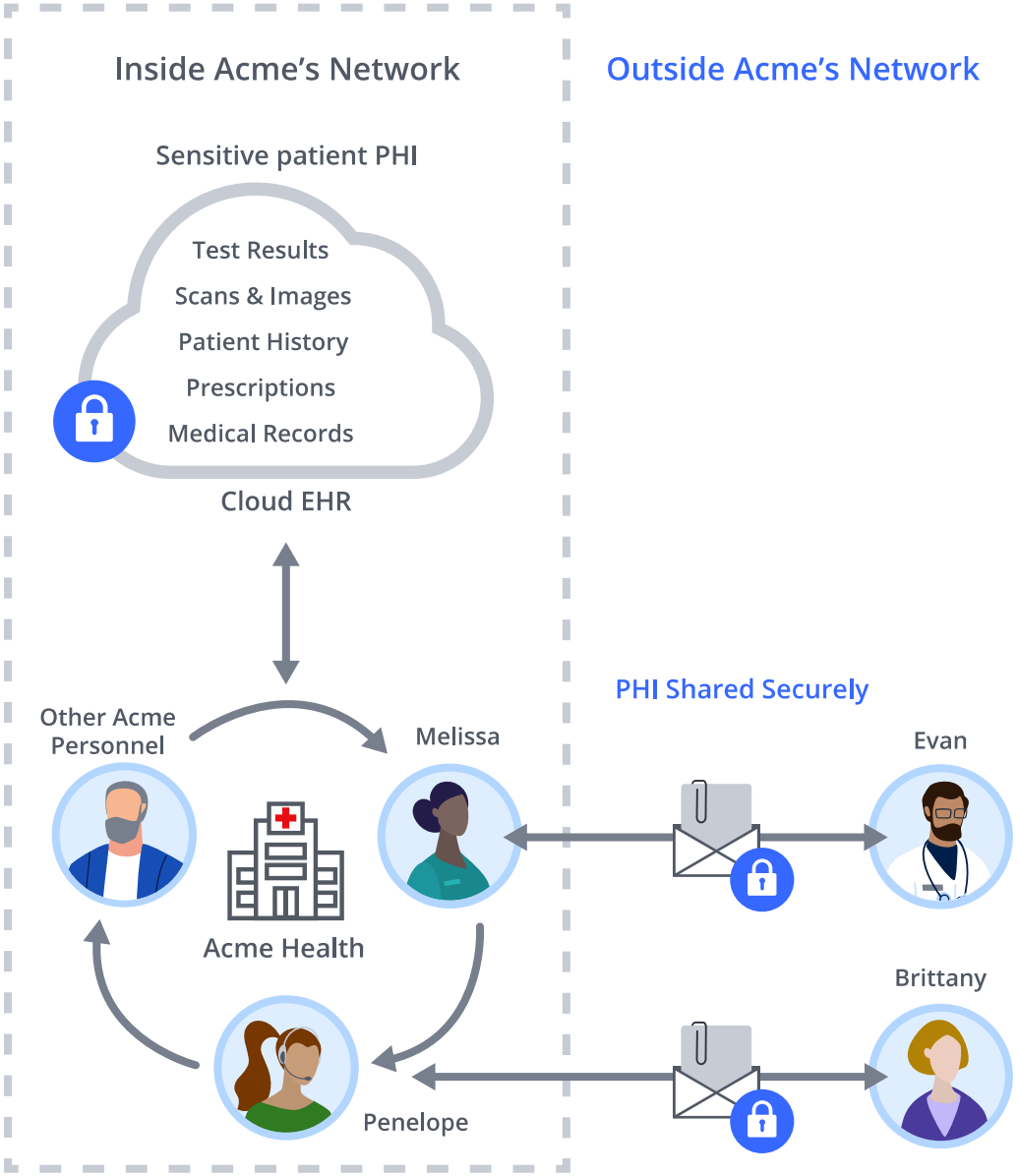


Virtru's user-first approach enables easy access using existing accounts and credentials, so patients stay engaged.

How the Users Feel Now

Melissa and **Evan** also feel **EMPOWERED.**

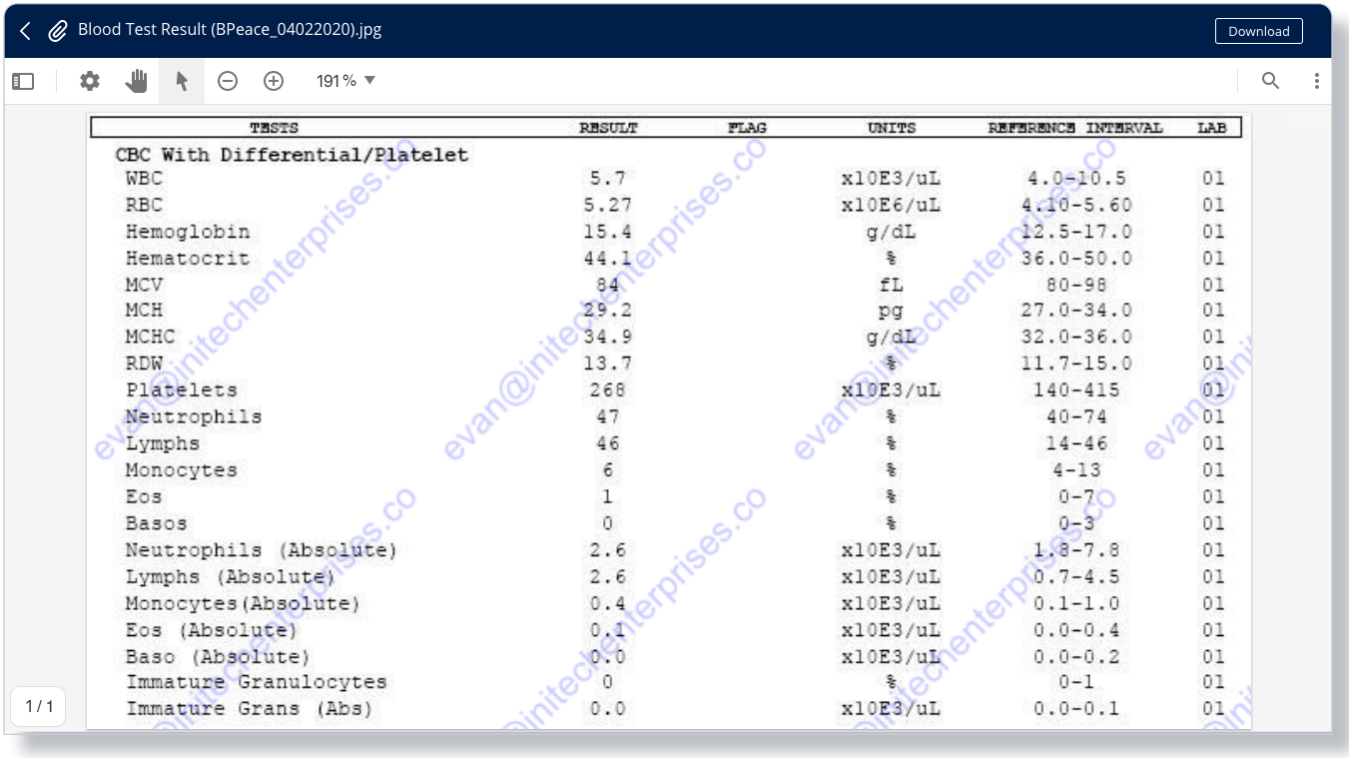
- Melissa simply shares the medical history and patient results with Evan via a protected email. She no longer has to make the case with the IT team to create a new EHR account for an external user.
- Melissa uses a similar workflow to Penelope to ensure greater control and visibility for GDPR compliance. As she encrypts the message, she adds a watermark and disables forwarding of the PHI.
- Evan is relieved that this workflow aligns with how he already works. He can quickly access and evaluate the test results, then work with Melissa and the Acme team on a new care regimen that will limit Brittany's diabetes and hypertension risks.



The Result

Instead of feeling uneasy, frustrated, and powerless, all parties involved are empowered and can move forward by providing efficient, timely care for Brittany. Penelope gives Brittany the confidence and trust that she needs to maximize the impact of Acme's behavioral health program. Any delays between Acme's team and Evan are resolved by aligning with their existing workflows. Virtru's user-first approach ensures they're all on the same page to quickly prescribe new steps in Brittany's care regimen.

Data-centric security enables GDPR compliant digital care collaboration, giving Acme and Brittany confidence that they'll achieve her health goals and help her live a heathier life.



TESTS	RESULT	FLAG	UNITS	REFERENCE INTERVAL	LAB
CBC With Differential/Platelet					
WBC	5.7		x10E3/uL	4.0-10.5	01
RBC	5.27		x10E6/uL	4.10-5.60	01
Hemoglobin	15.4		g/dL	12.5-17.0	01
Hematocrit	44.1		%	36.0-50.0	01
MCV	84		fL	80-98	01
MCH	29.2		pg	27.0-34.0	01
MCHC	34.9		g/dL	32.0-36.0	01
RDW	13.7		%	11.7-15.0	01
Platelets	268		x10E3/uL	140-415	01
Neutrophils	47		%	40-74	01
Lymphs	46		%	14-46	01
Monocytes	6		%	4-13	01
Eos	1		%	0-7	01
Basos	0		%	0-3	01
Neutrophils (Absolute)	2.6		x10E3/uL	1.8-7.8	01
Lymphs (Absolute)	2.6		x10E3/uL	0.7-4.5	01
Monocytes(Absolute)	0.4		x10E3/uL	0.1-1.0	01
Eos (Absolute)	0.1		x10E3/uL	0.0-0.4	01
Baso (Absolute)	0.0		x10E3/uL	0.0-0.2	01
Immature Granulocytes	0		%	0-1	01
Immature Grans (Abs)	0.0		x10E3/uL	0.0-0.1	01

The Virtru Secure Reader gives Evan seamless access, while Acme maintains control with persistent protection and watermarks that help prevent GDPR compliance violations.

Data-Centric, User-First PHI Protection for Patient Engagement & Care Optimization

Digital workflows and cloud-based systems bring plentiful opportunities to healthcare organizations, but they can also carry significant risks for patient confidentiality and GDPR compliance. As Acme's experience illustrates, traditional methods of protection don't support the dynamic, rapid care collaboration needed for modern health systems, leaving users frustrated and putting care outcomes at risk.

Combining data-centric protections with a user-first approach to PHI protection gives healthcare organizations a head start in providing optimal care. IT and security teams can empower users with secure care collaboration workflows that enable quick care delivery and increased patient engagement, while protecting PHI to prevent the risk of noncompliance fines.

If your organization is interested in learning how Virtru can help modernize your care delivery, contact us to see how easy it is to maintain patient confidentiality and compliance. virtru.com/contact-us

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection.

Visit virtru.com or follow us on Twitter at @virtruprivacy.