sharecare

Fraudulent ROI and Cybersecurity; What you need to know today

2025

About Me

01. Launched IT career as a head network administrator for MWC Public Schools, creating a foundational IT infrastructure.

02. Developed a migration SOP for the U.S. Army at Ft. Jackson, transitioning from Windows 3.1 to Windows 95.

03. Created AOL 9.0's first secure browser with an integrated security addition.

04. Partnered with Google Earth at TruGreen, automating lawn measurements to drive efficiency and save significant operational costs.

05. Achieved ISO 27001, SOC 2 Type 2, and HITRUST certifications at Sharecare, securing HIH credentials with CMS and launching the company's esMD service

sharecare
Achieved ISO 27001, SOC 2 Type 2, and HITRUST certifications at Sharecare, securing HIH credentials with CMS and launching the company's esMD service

All Together Better.

Overview: Sharecare Health Data Solutions

Sharecare is a **health & well-being interoperable ecosystem** that **unifies all the elements** of individual and community health so everyone can live better, longer across the **dynamic continuum of their healthcare needs. All Together Better.**

Strategic partners & clients

HCA Healthcare · Wellstar · Ascension · Mass General Brigham · HONORHEALTH
Cedars Sinai · Atrius Health · Providence St. Joseph Health · SHARP · Beth Israel Lahey Health
Intermountain Healthcare · Memorial Healthcare System · BAPTIST HEALTH · R1 · CHS Community Health Systems
CareFirst · Anthem BlueCross BlueShield · BlueCross BlueShield of Arizona · United Healthcare · DELTA · KOCH
AARP · BeWell SHBP · health net · LENNAR · KOHLER · Aflac

Strategic partners & clients

6M+ medical records processed annually	**33** years of experience with providers/health systems	**90K+** total active providers
$1B+ investment in technology	**3M+** audit requests completed annually	**19K+** client sites supported
3.5K+ unique healthcare systems served	**2.87M** social followers	

Supporting

- Large/midsize employers
- Health systems
- Health plans
- Government/public sector

What you will learn today

- What Cybersecurity action items your organization could take today to protect against fraudulent requesters.
- Understand what constitutes a fraudulent medical record request
- What steps can your organization take to protect your patients' data.

Cybersecurity

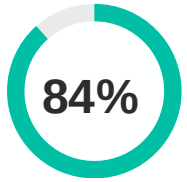
Rural and Midsize Healthcare are not immune to cybersecurity threats

- Limited IT infrastructure and cybersecurity expertise.
- Greater financial vulnerability, with many rural hospitals already in precarious financial states.
- Greater impact on patient outcomes due to geographic isolation and limited alternative healthcare options.

Cybersecurity in Rural and Midsize Hospitals

Growing Threat

# of Ransomware attacks on rural hospitals



of ransomware attacks on rural hospitals caused operational disruptions, comparable to urban hospitals.

Experienced EMR Downtime

Faced delays or cancellations of care

Had ambulance diversions

Government Response

Update to HIPAA in 2013

1. **Conduct Risk Assessments:** Identify and mitigate vulnerabilities in ePHI systems.
2. **Control Access**: Use unique IDs, multi-factor authentication, and role-based access.
3. **Secure Data:** Encrypt ePHI in transit and at rest; securely wipe devices.
4. **Respond to Incidents:** Detect, respond to, and report breaches effectively.
5. **Train Staff:** Regularly educate employees on recognizing and preventing cyber threats.
6. **Ensure Vendor Compliance:** Sign BAAs and verify third-party adherence to HIPAA standards.

$9.23 Million

Avg. Cost of a Cybersecurity Incident 2023

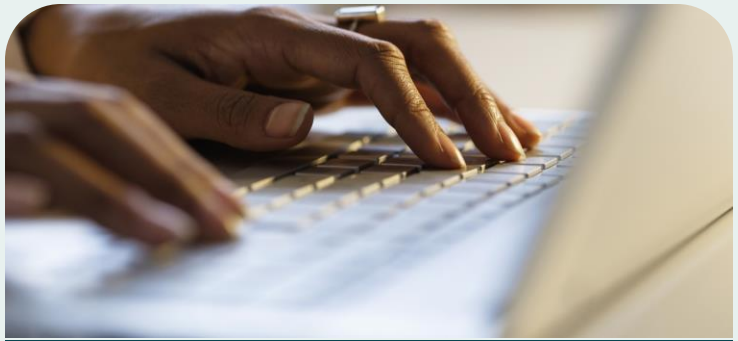
Neprash, H.T., McGlave, C.C., Rydberg, K., & Henning-Smith, C. (2024). *Understanding the Rise of Ransomware Attacks on Rural Hospitals*. University of Minnesota Rural Health Research Center Policy Brief, June 2024. Retrieved from https://rhrc.umn.edu/publication/understanding-the-rise-of-ransomware-attacks-on-rural-hospitals.

IBM. "IBM Report: Cost of a Data Breach Hits Record High During Pandemic." *IBM Newsroom*. July 28, 2021. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.

Cybersecurity best practices

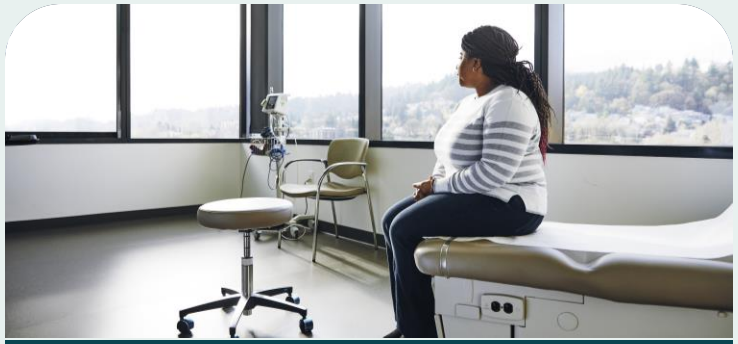
Conduct Risk Assessments

- Perform regular evaluations of systems and processes to identify cybersecurity vulnerabilities.
- Implement appropriate security measures to mitigate risks to ePHI.



Control Access

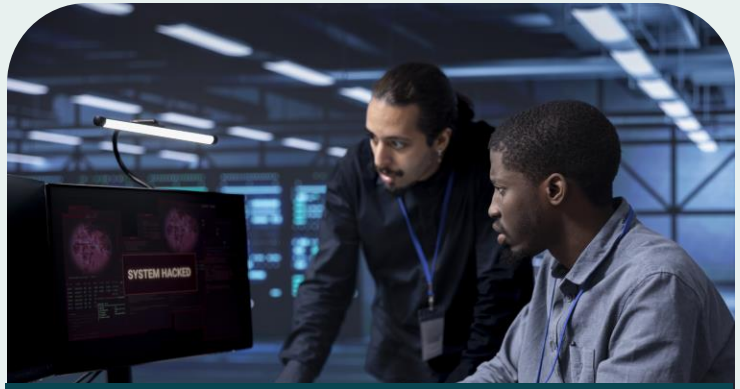
- Enforce unique user IDs and multi-factor authentication for all system users.
- Limit access to PHI based on specific job roles and responsibilities..



Secure Data

- Encrypt ePHI during transmission (e.g., email, file sharing) and storage to prevent unauthorized access.
- Securely dispose of or wipe devices containing ePHI before reuse or disposal.

Cybersecurity best practices

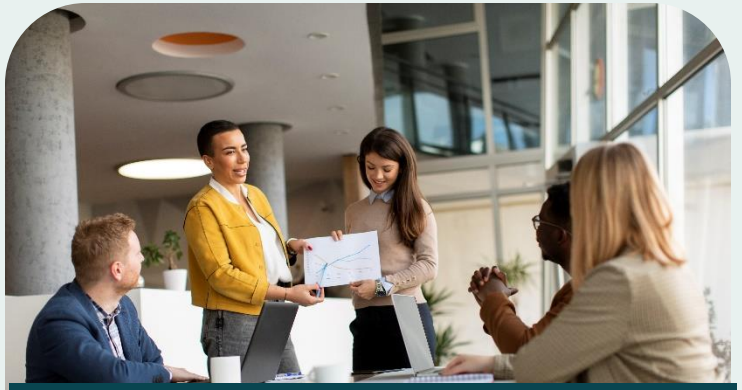


Respond to Incidents

- Develop an incident response plan to address breaches and cyberattacks promptly.
- Notify affected individuals and regulatory authorities as required by HIPAA.

Train Staff

- Conduct regular cybersecurity training to educate staff on identifying and responding to threats like phishing, malware, or fraudulent ROI.
- Update training programs to reflect the latest threats and compliance requirements.



Ensure Vendor Compliance

- Establish Business Associate Agreements (BAAs) with all third parties accessing ePHI.
- Ensure vendors are certified.

Cybersecurity- Quick Take-Aways

Conduct Risk Audits

- These should be a team effort
- Recognize this is to keep your job safe too. It protects the entire organization

Have MFA

- Multifactor Authentication drastically lowers risk
- Not having MFA would look very bad during a breach incident. Like your organization doesn't take cybersecurity seriously enough

Electronics Discharge Process

- Computers should have a "Discharge process.
- Don't just give away computers or other electronics without IT wiping data.

Operations Plan

- Disaster recovery should not just be an IT exercise. Operations should also have a plan.
- You know your operations better than IT does.

Send Questions to Cyber Security

- Ask cybersecurity questions about what you don't know.
- Inform cybersecurity about items you are unclear on and foster communication

Beware of BCNCs

Big Companies No Certifications

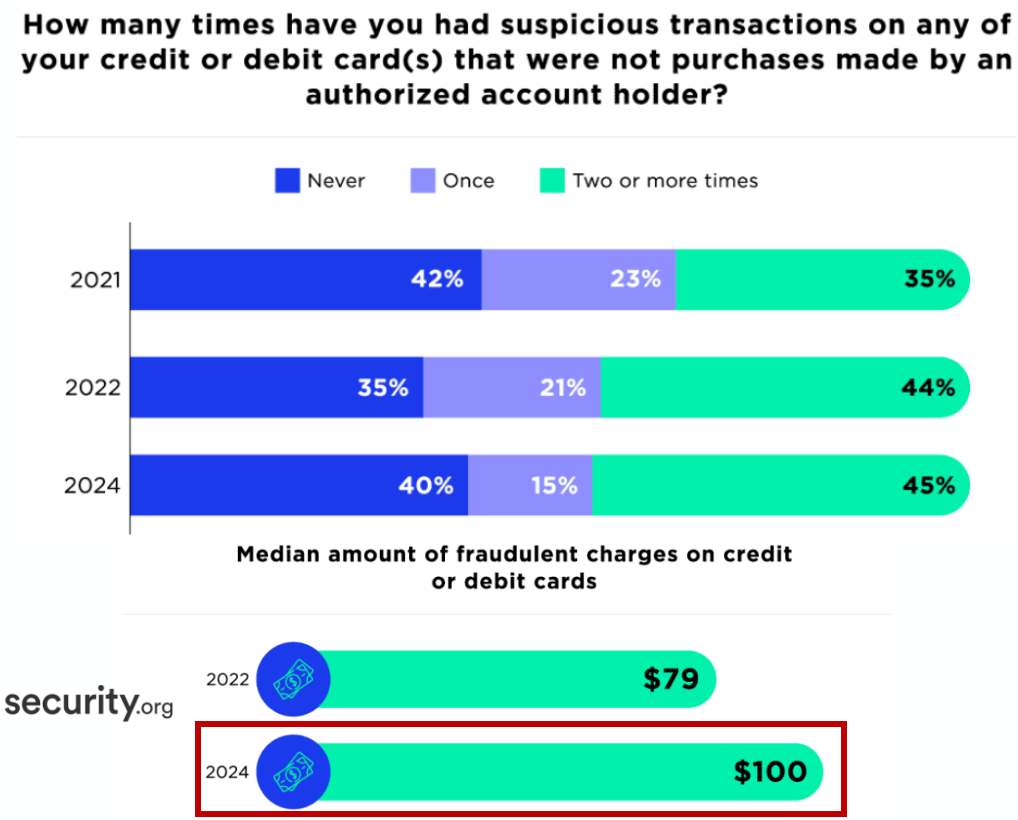
- If a large company doesn't have a certification, there's a reason, and it's not a good one for you.

sharecare

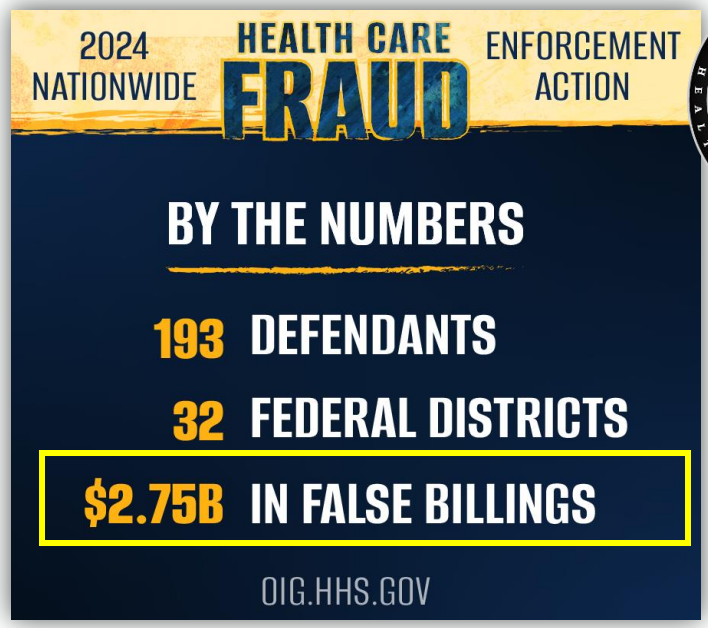
Fraudulent ROI...
The Problem

Same problem, different industry

Financial Crimes



Healthcare Fraud



Median Loss/Offense of Healthcare Fraud: **$1,416,231**

In contrast to credit card numbers and other financial information, healthcare data ***has an incredibly long lifespan*** *and can often be misused for long periods undetected.*

How Much Americans Have In Their Checking Account

Types of Healthcare Fraud

The FBI has broken down the relevant types of healthcare fraud

Contributed to by Fraudulent ROI

Fraud Committed by Medical Providers

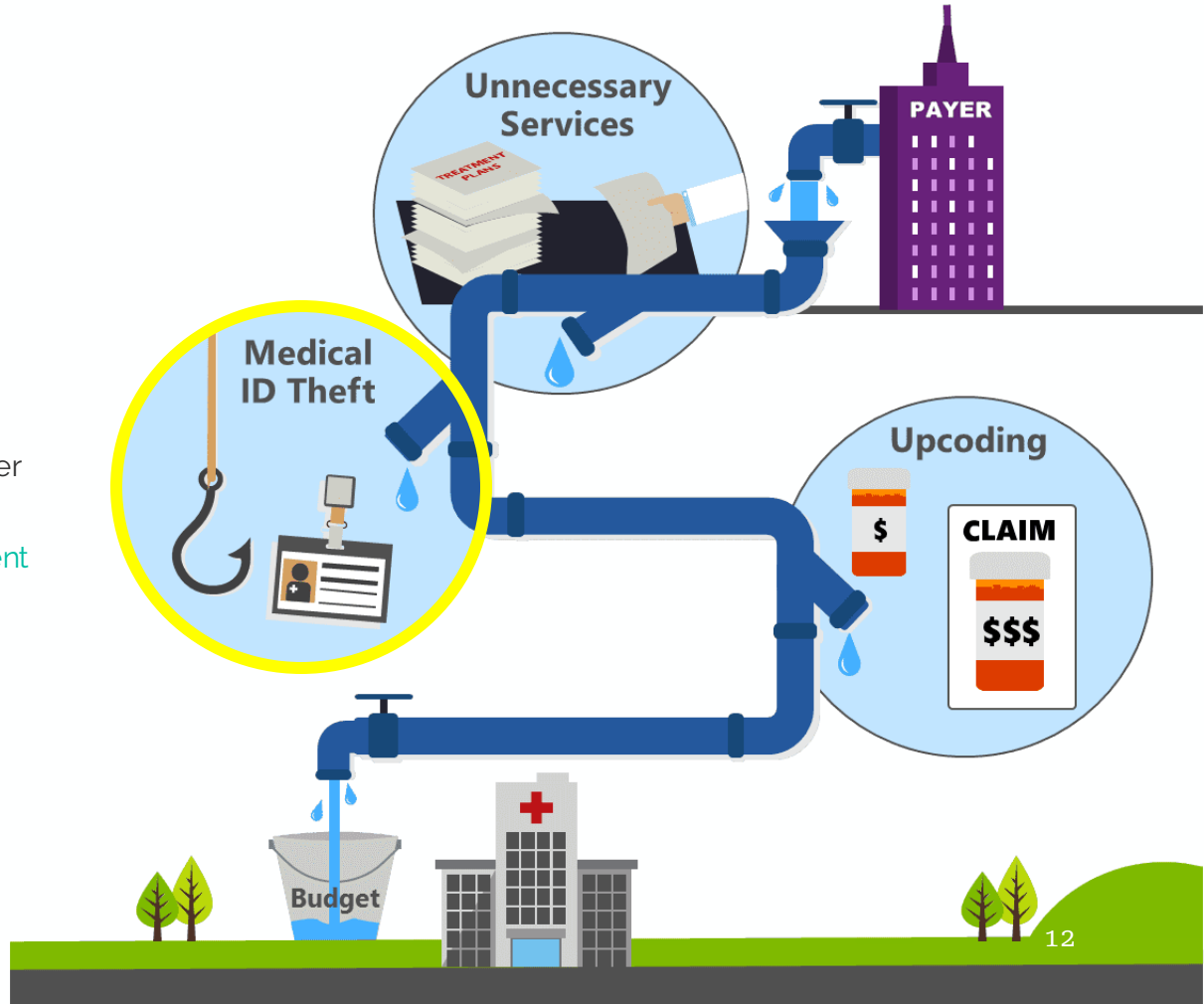
- **Double billing:** Submitting multiple claims for the same service
- **Phantom billing:** Billing for a service visit or supplies the patient never received
- **Unbundling:** Submitting multiple bills for the same service
- **Upcoding:** Billing for a more expensive service than the patient actually received

Fraud Committed by Patients and Other Individuals

- **Bogus marketing:** Convincing people to provide their health insurance identification number and other personal information to bill for non-rendered services, steal their identity, or enroll them in a fake benefit plan
- **Identity theft/identity swapping:** Using another person's health insurance or allowing another person to use your insurance
- **Impersonating a health care professional:** Providing or billing for health services or equipment without a license

Fraud Involving Prescriptions

- **Forgery:** Creating or using forged prescriptions
- **Diversion:** Diverting legal prescriptions for illegal uses, such as selling your prescription medication
- **Doctor shopping:** Visiting multiple providers to get prescriptions for controlled substances or getting prescriptions from medical offices that engage in unethical practices



Defining Fraudulent ROI

Susan

67 years old
Female

Susan recently underwent a routine surgery to repair an MCL tear on her knee. She is healthy patient but does have Type-2 Diabetes.

Fraudulent requester purchases demographic info from “dark web” service

Susan receives surgery. All relevant notes are recorded in EMR

Fraudulent request is provided to all medical facilities in a geographic radius of Susan’s home

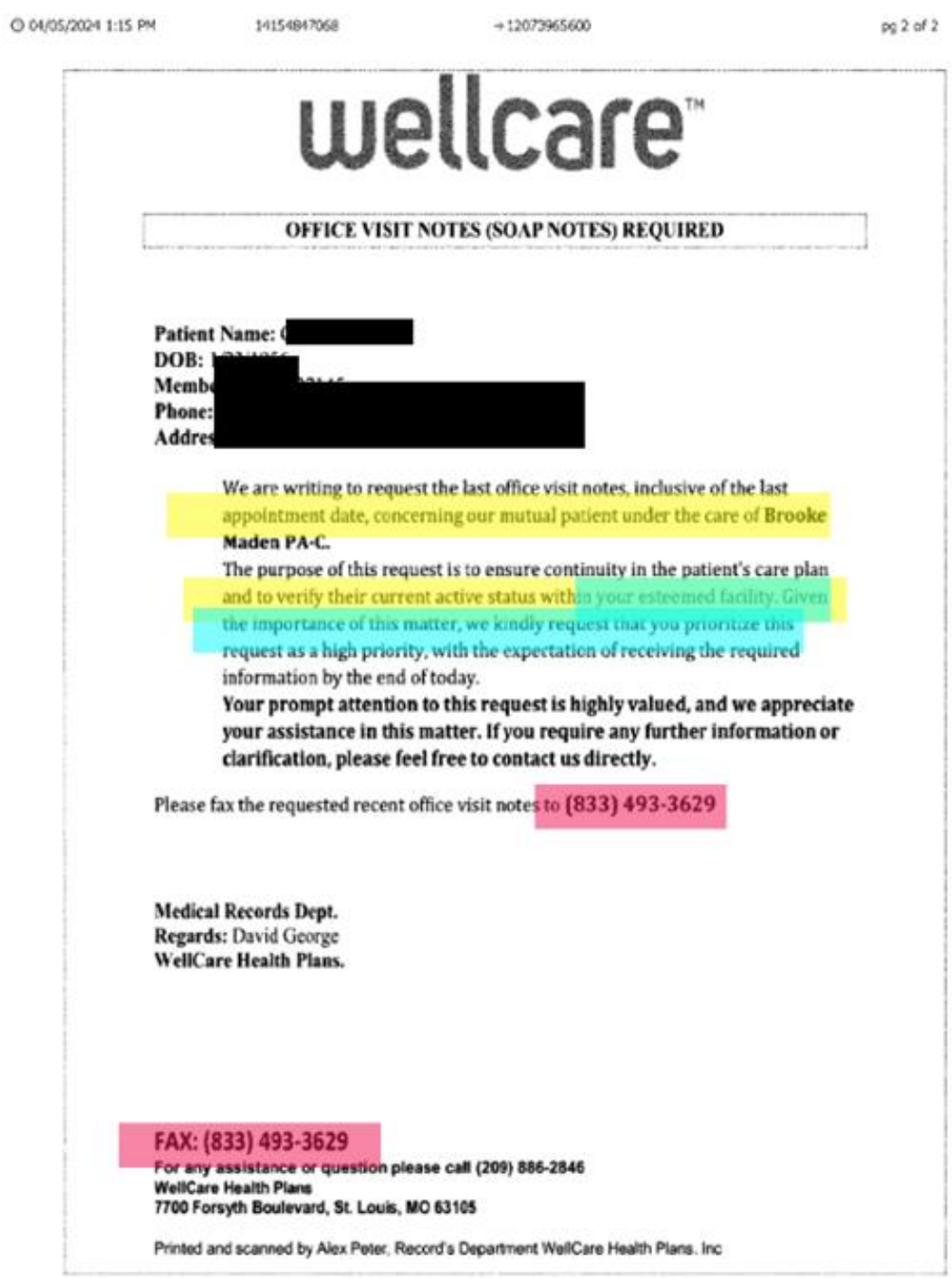
These requests are mostly delivered via fax

Requests are received in the medical records department and records are provided

These requests look like normal requests but have key differences to look for

Fraudulent requester reviews the charts with AI and finds conditions to bill insurance carrier

In the chart, it indicates Susan has Type-2 Diabetes, the fraudulent requester starts billing insurance carrier for diabetic test strips, glucose monitors, etc.



04/05/2024 1:15 PM 14154847068 →12073965600 pg 2 of 2

wellcare™

OFFICE VISIT NOTES (SOAP NOTES) REQUIRED

Patient Name: [redacted]
DOB:
Membe
Phone:
Addres

We are writing to request the last office visit notes, inclusive of the last appointment date, concerning our mutual patient under the care of **Brooke Maden PA-C.**

The purpose of this request is to ensure continuity in the patient's care plan and to verify their current active status within your esteemed facility. Given the importance of this matter, we kindly request that you prioritize this request as a high priority, with the expectation of receiving the required information by the end of today.

Your prompt attention to this request is highly valued, and we appreciate your assistance in this matter. If you require any further information or clarification, please feel free to contact us directly.

Please fax the requested recent office visit notes to **(833) 493-3629**

Medical Records Dept.
Regards: David George
WellCare Health Plans.

FAX: (833) 493-3629
For any assistance or question please call (209) 886-2846
WellCare Health Plans
7700 Forsyth Boulevard, St. Louis, MO 63105

Printed and scanned by Alex Peter, Record's Department WellCare Health Plans, Inc

Commonly Used Letterhead for Fraudulent Requests

wellcare™

Nationwide Pharmacy
Caring for Everyone

CVS Caremark®
HIPAA COMPLIANT

northern health
the northern way of caring

Anthem. BlueCross

NABP
National Association of Boards of Pharmacy

GLOBAL PHARMACY

ORTHOPEDIC SPECIALISTS

Walgreens
There's a way.

WellCare
Beyond Healthcare. A Better You.

Care View Diagnostics
Phone: (888) 454-1379
Fax: (561) 331-6143
results@careviewdiagnostics.org

Scan the QR code for a complete list of identified Fraudulent Requesters

How does this happen?

“There's no way to police the system. It's too large. So basically, it works on faith.” Malcom Gladwell

Referring to Medicare

Fraudulent ROI...
Combating the problem

The industry is combating this through both technological and human centered innovations

Blocking Known Fraudulent Fax Numbers

- Over 95% of these requests are coming through Fax
- The easiest way to prevent these requests from being fulfilled is to block the requests from coming in from identified fraudulent fax numbers
- The ROI industry has built technology to prevent records going to designated locations without human intervention

Train the Team

- It is imperative that the team handling medical records is trained on identifying and reporting fraudulent requests
- Fraudulent tactics are cyclical. Fraudsters will try one method and move on to another once it proves successful. Consistent retraining is necessary.
- Review Prescriptions/Orders/DME requests to make sure they make sense.

Communicate with Relevant Agencies

- Government Agencies, FBI, CMS etc. need our assistance as much as we need theirs.
- We (ones managing ROI) are on the front lines of this battle. Sharing resources with our agencies will then promote reciprocative communications, better arming your teams

Over a three-year period, multiple breaches and a higher number of breached records lead to a significant decline in outpatient visits and admissions, particularly in competitive markets.

Kwon, J., & Johnson, M. E. (2015). *The market effect of healthcare security: Do patients care about data breaches?* Workshop on the Economics of Information Security (WEIS). Retrieved from https://econinfosec.org/archive/weis2015/papers/WEIS_2015_kwon.pdf

What do we do with them, once discovered?

It's one thing to recognize a request could be fraudulent, it's an entirely different thing to figure out what to do about that problem, once realized.

Justin Vogt *CTO Dell Computers while reviewing this very presentation, with 8 other CISOs*

Have Fraud Mitigation Policies

- Document all new policies created in partnership with CEO and/or CFO with HIM Director
- Examples; Send DME requests to the HIM first. Must review before approving Rx requests etc.
- Reach out to the purported requestor if a known brand name.

Document and Report

- When you deny a request, have the reason documented.
- Add a newly discovered fraudulent requestor to your list.
- IF it becomes an OCR complaint and you followed your policies, it becomes a mitigating factor instead of an aggravating factor.

Continued Education

- Send periodic reminders to keep fraudulent requests in front of mind.
- Inform staff of new fraudulent methods identified.
- Do a retro-audit when you identify a new fraudulent actor and see what you can learn.

sharecare

Questions?

Let’s Get in Touch

Email
C.Shatswell@sharecare.com

Phone
+1 (405)-245-0075