Navigating the ChiroTouch / TriZetto HIPAA Breach

What Chiropractors Need to Know—and What to Do Now

Audience: Doctors, Chiropractic practice owners, Office managers, Billing leaders

Purpose: Practical, chiropractic-focused guidance to help you respond to the ChiroTouch / TriZetto incident, protect your patients, and document HIPAA compliance.

Educational Notice (Not Legal Advice): This white paper is provided for general educational purposes only and does **not** constitute legal advice. HIPAA requirements and timelines can vary based on the specific facts of your situation, your vendor contracts, and applicable state law. For legal interpretation or advice about your particular circumstances, consult qualified legal counsel.

Key Takeaways for Chiropractors (Read This First)

- **If you use ChiroTouch and submit claims or eligibility transactions through TriZetto, your patients' PHI may have been involved** in this breach—even though your office was not directly attacked.
- **Even when a vendor is involved, your practice should ensure its response is** timely, appropriate to the facts, and well-documented.
- **TriZetto and Kroll are offering to help** with notifications, reporting, and credit monitoring, but this is **delegated work, not a transfer of liability**. Your practice should oversee, confirm, and document what is done on your behalf.
- **Time matters.** HIPAA generally requires breach notifications **without unreasonable delay** and **no later than 60 days after discovery**. **Treat the date your practice receives notice as Day 0 for internal tracking, and move promptly**—HIPAA's outside deadline is generally 60 days from discovery of the breach, and delays can create compliance risk.
- **Your documentation is your defense.** If regulators, payers, or patients ever ask questions, your strongest protection is a clean file showing **what you knew, when you knew it, and what you did next**.
- **Use this incident as a compliance stress-test.** Vendors get breached; audits happen. The practices that fare best already have **current policies, training records, risk analyses, and business associate oversight** organized and available.

Background: What Happened in the TriZetto Breach?

TriZetto Provider Solutions, a Cognizant-owned provider of revenue management and clearinghouse services for healthcare organizations, reported a cybersecurity incident involving unauthorized access to a web portal used by some of its healthcare provider customers.

1. Key Facts Reported

- **October 2, 2025:** TriZetto detected suspicious activity within a web portal used by certain healthcare providers. Immediate action was taken to secure the portal and mitigate the incident.
- TriZetto engaged the cybersecurity firm **Mandiant**, as well as **law enforcement**, to investigate the activity, review the security of the web portal, and remediate the incident.

- The forensic investigation determined that an unauthorized third-party had been accessing **historical eligibility transaction reports** in TriZetto's system since **November 24, 2024**—an exposure period of nearly **11 months** before discovery.
- These reports contained **protected health information (PHI)** of patients of certain healthcare provider clients, including many **chiropractic offices that use ChiroTouch and route claims or eligibility transactions through TriZetto**.

2. Types of Information Potentially Involved

According to TriZetto, information potentially involved includes patients' and primary insureds':

- Names
- Addresses
- Dates of birth
- Social Security numbers
- Health insurance member numbers (in some cases, Medicare beneficiary numbers)
- Health insurer names
- Information about the primary insured or beneficiary
- Other demographic, health, and health insurance information

TriZetto has stated that **no financial account information** (such as bank account or credit card numbers) was involved. TriZetto also reports that no further unauthorized web portal activity has been detected since October 2, 2025, and that the threat actor has been eradicated from its system.

3. Why Chiropractors Should Care

If your practice uses **ChiroTouch** and submits claims or eligibility transactions through **TriZetto** (directly or indirectly), your patients' PHI may have been stored in the compromised environment—even though the breach occurred at a **third-party vendor**, not inside your office.

4. Why This Is an Emergency for Chiropractors

Under the **HIPAA Breach Notification Rule**, once a covered entity (you or your practice) becomes aware of a breach affecting unsecured PHI, notifications are generally required **without unreasonable delay** and **no later than 60 days after discovery**.

When a **business associate (such as TriZetto)** notifies you of a breach involving your patients' unsecured PHI, you should act immediately. Additional reporting obligations (including reporting to HHS/OCR and, in certain situations, state regulators or the media) depend on the facts—especially the number of individuals affected—and applicable state law.

Practical takeaway:

- **Act immediately.** Track deadlines and retain proof of completion—even if a vendor is coordinating logistics.
- **Individual notice:** generally, without unreasonable delay and no later than 60 days after discovery.
- **Other reporting:** may include HHS/OCR and, depending on the facts, state regulators or the media (as applicable).

Failure to act within these timeframes can expose you to:

- Substantial **fines and penalties**
- **Investigations** by OCR and/or state agencies
- Allegations of **willful neglect**, even though the breach occurred at a third-party

Bottom line: You may not have caused this breach—but you can still be held accountable for **how you respond.**

What TriZetto and Kroll Are Offering to Do for You

TriZetto has begun notifying affected healthcare provider clients and has offered a significant level of assistance, often through **Kroll**, a cybersecurity and identity protection firm.

Services They May Offer

Depending on the communication you receive, offered services may include:

- Preparing and mailing **patient breach notification letters** on your behalf
- Notifying **HHS/OCR**, **state regulators**, and **media outlets** where required
- Providing a **list of affected individuals** and a copy or description of the affected data
- Covering the cost of **complimentary credit monitoring**, **fraud consultation**, and **identity theft restoration services** for affected individuals

For many chiropractors, TriZetto has engaged Kroll to carry out these functions. This assistance is typically offered at **no cost to your practice**, provided you register by the stated deadline (for example, **January 19, 2026**, if that date appears in your specific notice).

Important: These services are valuable—but they do **not** remove your underlying legal responsibilities as a HIPAA-covered entity. Treat them as **delegated tasks, not transferred liability**.

You remain responsible for:

- Understanding what is being done in your name
- Confirming that the required steps have been completed
- Keeping **proof** that those steps were completed **on time**

Your HIPAA Compliance Responsibilities (Practical Reality for Practices)

Chiropractic practices are required by federal law to implement and maintain a **HIPAA compliance program**. This is **not optional**.

A properly structured program typically includes:

- A **HIPAA policies and procedures manual** (often 2–500+ pages) as your foundational "starting manual"
- **Documented risk analyses** and **risk management plans**
- Regular, **documented reviews, evaluations, and internal audits**—generally at least annually
- **Ongoing staff training** on HIPAA requirements and updates
- **Business Associate Agreements (BAAs)** with any third-party entities that access or handle your patients' PHI

Two Common Misunderstandings

1) **"I have a Business Associate Agreement, so I'm covered."** BAAs are essential and can provide some liability protection when a business associate has a breach. However, a BAA is **not** a "get out of jail free" card.

   Regulators will still commonly focus on the covered entity's response and documentation to confirm that:
   - Appropriate breach response steps occurred
   - Patients' rights were protected
   - Documentation exists to prove a timely, reasonable response

2) **"I bought a HIPAA manual years ago, so I'm compliant."** HIPAA compliance is **not** a binder—it is an **operating system** for how your practice handles PHI every day.

   HIPAA requires that you not only **have** policies and procedures but also **implement** and **regularly update** them. Failing to conduct required reviews, updates, and trainings—even if you own a HIPAA manual—is often used as evidence of **willful neglect** (you knew what was required but did not do it).

Civil monetary penalties can be significant and are adjusted for inflation; in the highest tiers, **per-violation minimums can exceed $71,000**, and may rise over time. Outcomes vary based on the specific facts and—critically—whether you can produce documentation showing a reasonable compliance program and an organized, timely response. Penalties are often most severe when regulators conclude a practice failed to implement basic safeguards or maintain required documentation.

Key point: Having paperwork is not enough. **Implementation plus documentation** is what protects you.

What You Should Do Right Now: Step-by-Step Plan

This section is designed to be practical. You can work through it as a checklist.

Step 1 — Confirm Whether You Were Notified
Check immediately for any notice related to the TriZetto incident:
- Email inboxes (including spam/junk) for:
  - Doctor / Practice owner
  - Office manager
  - Billing lead or billing vendor contact
- Physical mail at your office address
- Any online portals used by your:
  - Billing vendor
  - Clearinghouse
  - EHR (e.g., ChiroTouch)
- Communications from:
  - TriZetto
  - Cognizant
  - Kroll
  - ChiroTouch
  - Your billing or IT partners

Search for terms like: **"TriZetto," "Cognizant," "Kroll," "cybersecurity incident," "data breach," "eligibility transaction reports."**

If you have not received any communication:

- It may mean TriZetto has **not** identified your practice as affected—yet.
- Continue monitoring.
- Consider proactively contacting ChiroTouch, TriZetto, or your clearinghouse/billing partner to ask whether your data was involved.

If you have been contacted:

- Proceed to the next steps.

Step 2 — Verify Authenticity Before Clicking Anything

Breach events often create opportunities for **phishing** and scam emails.

Before you click any links or open attachments:

- **Confirm** the sender's email domain and contact information.
- **Cross-check** phone numbers and URLs with official vendor websites or documentation.
- When in doubt, **call a known support number** from your existing agreements or the official website—not from the email itself.

Step 3 — Record Your "Day 0" Date

As a best practice, immediately write down:

- The date you or your practice first became aware of the incident communication
- Who received it (name and role)

This is your internal **Day 0** and helps you track follow-up and demonstrate timeliness.

Example: Day 0 date: January 5, 2026 Received by: Jane Smith, Office Manager

Step 4 — Decide Whether to Enroll in TriZetto/Kroll Services

If your notice includes an offer for services such as notifications, credit monitoring, and regulatory reporting support, carefully review the details.

In most cases, it will be **strongly advisable** to take advantage of TriZetto/Kroll's offer to:

- Handle patient notifications
- Provide credit monitoring and identity theft services
- Submit required notices to HHS/OCR, state regulators, and media (as applicable)

These tasks are complex, time-consuming, and potentially very costly if you attempt to handle them entirely on your own.

If you enroll, treat it like a professional engagement:

- Save the **enrollment confirmation**.
- Save the **scope of services** (what they are promising to do).
- Note any **deadlines** mentioned in the communication.
- Identify **one person in your practice** responsible for tracking follow-up and communication with TriZetto/Kroll.

Remember: enrolling does **not** mean you can "set it and forget it." You are still responsible for oversight.

Step 5 — Create a Simple "Breach Response File" (Your Compliance Shield)
Create a folder (digital, paper, or both) titled: **"TriZetto Breach Response – [Practice Name] – 2025/2026"**

Place the following items in it as they become available:
1) **Copy of the notice** letter/email you received (save as PDF).
2) **Day 0 record:** date you became aware of the incident and who received the notice.
3) Any **affected-individual list** or data summary provided by TriZetto/Kroll.
4) **Written confirmation** of what TriZetto/Kroll will do on your behalf.
5) **Final versions of patient notification letters** (if they prepare them).
6) **Proof of mailing or completion confirmation** for patient notifications.
7) **Confirmation of OCR submission** and any state/media notifications (or proof they were done on your behalf).
8) **Internal notes:**
    - Calls made
    - Emails sent
    - Internal meetings
    - Decisions taken
    - Dates and times of each
    - **Patient inquiry log** (optional but very helpful).
    - The **staff script** to use when responding to patient calls.

If OCR or a state regulator ever asks questions, this file is what makes you appear **organized, responsible, and compliant**.

Step 6 — Conduct an Internal HIPAA Review
Even with external help, you remain responsible under the law. Use this incident as a prompt to review your HIPAA program:
- **HIPAA manual:** Is it current? Have you made and documented annual updates?
- **Risk Analysis:** Do you have a current Security Rule risk analysis on file, and can you show follow-through on identified risks?
- **Business Associate Agreements (BAAs):** Do you have signed BAAs with:
    - ChiroTouch
    - TriZetto (or their parent companies/intermediaries)
    - Billing companies
    - IT providers
    - EHR vendors
    - Cloud storage and backup services
    - Shredding vendors
    - Remote access/IT support providers
- **Incident documentation:** Are you clearly documenting your response to this event in your Breach Response File?
- **Breach Notification Policy:** Does your current written policy reflect current OCR guidance and match what you are actually doing?

If you are unsure how to do this, or if you discover gaps, consult with a **HIPAA compliance professional promptly**.

Step 7 — Communicate Internally With Your Staff
Your staff will be on the front lines if patients call with questions.
- Brief your team—especially front-desk, billing, and administrative staff—on the situation in **clear, simple terms**.

- Identify **one point person** (doctor, office manager, or compliance lead) for escalated questions.
- Emphasize that staff should **not speculate**, **not minimize**, and **not provide details** they are unsure about.

Suggested Staff Script (Front Desk / Phone)

> "We're aware of a cybersecurity incident involving a third-party vendor used for certain billing and insurance transactions. We are working with the vendor and appropriate experts to ensure all required steps are completed in accordance with HIPAA. If your information is confirmed to be affected, you will receive a formal notification with details and available support resources, which may include credit monitoring and identity protection services."

Staff Guardrails:
- Do **not** speculate about who is affected.
- Do **not** confirm that a specific patient is affected unless you have verified information.
- Route escalated or upset callers to your **designated point person**.

Step 8 — Prepare for Possible Patient Questions
Patients may ask:
- "Was my information exposed?"
- "What is being done to protect me?"
- "Do I need to do anything right now?"

Be ready to explain, in simple terms:
- That a **third-party clearinghouse (TriZetto)** experienced a security incident.
- That your office is **working closely with the vendor and experts** to ensure all required steps are completed.
- **Affected patients should receive individual notification**, and the notice may include credit monitoring and identity theft protection at no cost. *Do not confirm that a particular patient was affected unless and until you have reliable information showing their data was involved.*

Step 9 — If You Are Unsure, Escalate Early
If you lack clarity about:
a) Whether HIPAA breach notification is required for your practice,
b) What timelines apply, or
c) What exactly TriZetto/Kroll is doing on your behalf,
consult a **HIPAA compliance professional** or **qualified legal counsel** promptly.

Delays and inaction create enforcement problems. Asking for help does not.

Protecting Your Practice In the Future

Cyberattacks—including ransomware and large-scale data theft—are increasing in both **frequency and sophistication**. At the same time, the federal government has signaled a growing focus on **random HIPAA audits**, including audits of **small private practices**, to encourage stronger protections. This was already in motion before the TriZetto breach.

The practices that fare best over time tend to do four things consistently.

1) Keep Your HIPAA Program Current

- Perform and document **annual reviews, evaluations, and internal audits**.
- Maintain a current, documented **risk analysis*** and **risk management plan**.
- Ensure your **incident response and breach notification policies** are up to date and realistic for your office.

Risk Analysis: One of the Most Important Documents to Keep Current

One of the strongest ways to improve your HIPAA posture is to maintain a **current, documented Security Rule risk analysis** and follow it with a practical risk management plan. OCR enforcement materials and resolution agreements frequently emphasize whether an organization completed a meaningful Security Rule risk analysis and maintained it over time. As a best practice, your office should be able to quickly produce a recent risk analysis, document updates when technology or workflows change, and show progress on addressing identified risks.

Remember: the law requires not just written policies, but **proof** that you perform the required updates and follow those policies in practice.

2) Train Your Staff Continuously

- Provide **new hire** HIPAA training.
- Conduct **annual refresher training** for all workforce members.
- Include **cyber hygiene** topics such as phishing awareness, password management, and incident reporting.
- **Document** all training sessions (dates, attendees, topics covered).

3) Tighten Business Associate Oversight

- Maintain **current BAAs** with all vendors that handle PHI: billing companies, IT providers, EHR vendors, cloud and backup services, shredding companies, etc.
- Keep an **updated inventory** of all vendors that access PHI and what they do.
- Periodically review vendors' **security practices** and **incident-response expectations**; know who to call and what to expect if something goes wrong.

4) Stay Audit-Ready

- Maintain organized, easily accessible **HIPAA documentation**, including:
    a) Policies and procedures
    b) Risk analyses and risk management plans
    c) Training records
    d) Business Associate Agreements
    e) Breach and incident response files
- Conduct an annual **tabletop exercise** (a practice scenario) so you and your staff know what to do when—not if—a cyber incident occurs.
- Keep your "**audit-ready**" files up to date so you can respond quickly if regulators request information.

Why Professional Help Is Often Essential

Most chiropractors are extremely busy business owners. Keeping up with changing HIPAA regulations, evolving cyber threats, and documentation requirements is difficult—and trying to manage it alone often leads to **unintentional noncompliance**.

Working with a qualified **HIPAA compliance professional** can help you:

- Build and maintain a **comprehensive, dynamic, and practical** compliance program.
- Navigate **complex breach response requirements and timelines**.
- **Organize and document** your response to incidents like the TriZetto breach.
- Reduce your risk of **hefty fines, investigations, and reputation damage**.
- Free up time and energy so you can focus on **patient care** while knowing your compliance program is on solid ground.

Conclusion

The TriZetto / ChiroTouch incident is a powerful reminder that even if a cyberattack never hits your office directly, your patients' data—and your practice—can still be at risk through your **business associates**.

You cannot control every vendor's security environment. But you **can** control:

- **How quickly you act** when you are notified of a breach.
- **Whether you document your response** in a clear, organized way.
- **Whether your HIPAA program is current, implemented, and defensible.**

If you:

- Take **immediate action** if you have been notified,
- Leverage TriZetto/Kroll services where appropriate,
- Strengthen (or implement) your **HIPAA compliance program**,
- Train your staff and **document** your efforts, and
- Close any gaps in your **business associate oversight**,

…you can protect your patients, demonstrate good-faith compliance, and significantly reduce your exposure to regulatory and financial harm.

This situation is **evolving**, and additional updates may become available. Stay informed and, when in doubt, seek qualified guidance.

For further information, resources, and assistance with chiropractic HIPAA compliance, stay in contact with **drtythecomplianceguy.com**.

About the Author: Dr. Ty Talcott, CHPSE, is the CEO of *HIPAA Compliance Services* and *DrTyTheComplianceGuy.com* and a nationally recognized expert in chiropractic compliance education. He helps chiropractic offices implement and maintain practical, audit-ready HIPAA compliance programs—including policies and procedures, risk analysis support, workforce training, incident response organization, and business associate management—so doctors can focus on patient care while reducing regulatory risk.

Dr. Talcott has advised over 10,000 doctors through more than 300 webinars and 200 live events, delivering tailored pre-recorded and live training for associations in 48 states and six colleges. His educational programs empower practitioners to prevent HIPAA complaints, errors, and cyberattacks, while also navigating other critical regulations such as the No Surprises Act, 21st Century Cures, and Medicare/OIG—for both doctors and CAs.

Drawing on decades of real-world experience, Dr. Talcott has:

- Run one of the highest-grossing chiropractic practices in the country, managing a daily patient volume of hundreds.
- Served as a compliance advisor to the Texas Workers' Compensation Commission.
- Chaired two chiropractic hospital departments and contributed to regulatory and compliance policies.
- Mentored chiropractors in building successful, enjoyable, and profitable practices.
- Authored more than 30 managed care and 25 HIPAA articles.

Dr. Talcott's distinctive "HANDS FREE" HIPAA compliance product has helped position *HIPAA* Compliance Services as a leader in chiropractic compliance program development. His ongoing participation in the annual HIPAA/Cybersecurity symposium in Washington, D.C., keeps him at the forefront of evolving enforcement tactics, enabling him to deliver practical, implementation-focused strategies to chiropractors nationwide.

Dr. Ty Talcott, CHPSE
President, HIPAA Compliance Services
Dr. Ty The Compliance Guy
HIPAA - OIG - FEE
(469) 371-8804
Ty.Talcott@gmail.com
www.drtythecomplianceguy.com

Appendix: One-Page Office Action Checklist

You can use this page as a quick internal reference.

TriZetto Breach – Office Action Checklist

1. _____ Check inbox/spam/mail/portals for notice from TriZetto / Cognizant / Kroll / ChiroTouch / billing vendor.
2. _____ Verify the authenticity of any notice (do **not** click unknown links).
3. _____ Record your **Day 0** notification date and who received it.
4. _____ Decide whether to enroll in TriZetto/Kroll services; if yes, enroll and **save confirmation**.
5. _____ Create a **"TriZetto Breach Response – [Practice Name] – 2025/2026"** folder.
6. _____ Save all notices, affected-individual lists, and service descriptions into that folder.
7. _____ Save copies of patient letters and proof of mailing/completion (when available).
8. _____ Obtain and save proof of OCR/state/media reporting (if applicable or done on your behalf).
9. _____ Confirm BAAs are current and retrievable for ChiroTouch, TriZetto, and all PHI-handling vendors.
10. _____ Brief staff and use a prepared script for patient calls.
11. _____ Log patient inquiries and key decisions in your incident response file.
12. _____ Review and update your breach notification policy, training log, and risk analysis status.
13. _____ Reach out for help as you need it