ELEVATED	FINANCIAL EXTORTION	CARE DISRUPTION + MASS DATA EXPOSURE
RISK LEVEL	PRIMARY THREAT	PRIMARY CONSEQUENCE

Q3 Threat Lens

Extortion is creating two forms of healthcare leverage

Recent U.S. healthcare incidents demonstrate how financially motivated cyber actors can create significant consequences through two distinct pathways: large-scale theft of sensitive healthcare data and disruption of technology-dependent care delivery.

ANMED	DENTAQUEST
CARE DISRUPTION	**DATA AT SCALE**
JUL 2026	**MAY 2026**
83 care locations initially closed	**~15M individuals affected**
Claimed Actor: The Gentlemen / Storm-2697	**Claimed Actor:** ShinyHunters
Motive: Financial extortion	**Motive:** Financial extortion
Impact: EHR, phones, internet, appointments and regional care coordination	**Impact:** PHI/PII exposure spanning patients, providers and government programs
Status: Services restored progressively; investigation and data-impact assessment continued	**Status:** Operations maintained; notification and downstream patient/regulatory impacts continued

WHAT THIS MEANS FOR INDIANA

Financially motivated actors do not require a single attack model to generate leverage against healthcare. Recent incidents demonstrate that both disruption of care and theft of sensitive data can produce prolonged consequences extending beyond technical containment.

Top Q3 Scenarios

01 — CLINICAL DISRUPTION

EHR • scheduling • imaging • communications

02 — DATA THEFT AT SCALE

PHI • insurance • billing • government identifiers

03 — DOUBLE EXTORTION

Disruption + stolen-data disclosure

04 — DOWNSTREAM IMPACT

Payers • vendors • benefits administrators • providers

Immediate Actions for Leadership

01 KEEP CARE MOVING

Define minimum viable clinical operations

Know what must remain available to safely sustain priority care.

Plan for regional spillover

Account for diversion, displaced appointments and demand shifting to neighboring providers.

02 REDUCE ATTACKER LEVERAGE

Map high-consequence data concentrations

Know where compromise creates the greatest patient and organizational exposure.

Pre-establish extortion authority

Determine who owns ransom, disclosure, law-enforcement and communications decisions.

03 CONTROL THE RECOVERY

Set restoration priorities before an attack

Pre-approve the sequence for restoring critical clinical and business capabilities.

Prepare for attacker-controlled communications

Plan for leak-site claims, direct victim contact and compromised organizational channels.