

OCTOBER 2026

VISITING HOURS

ARE ALWAYS OPEN ON THE INTERNET

What hackers see when they "drop by" America's hospitals and clinics



PROJECT MERIDIAN: U.S. HEALTHCARE CYBER SNAPSHOT

BY MICHAEL CENTRELLA · RICHARD HUMMEL · DR. MIKE MYLREA · DR. ALEKSANDR YAMPOLSKIY

PROJECT MERIDIAN DATA · OCTOBER 2026 · FACILITIES ARE NOT NAMED

CONTENTS

	The Short Version: Key Findings at a Glance	3
SECTION 1	Meet the Patient: Who Is in Our Data, and Why It Matters	4
SECTION 2	The Report Card: How Healthcare Grades	9
SECTION 3	Warning Lights: Four Flags Across U.S. Healthcare	11
SECTION 4	Texas Under the Microscope: What One State Shows About Healthcare Risk	14
SECTION 5	Far From Help: Why the Same Cyberattack Hurts Rural Care More	18
SECTION 6	Stolen Keys: How Attackers Can Walk In Through the Front Door	20
SECTION 7	What Could Go Wrong	21
	• What to Do Next: A 30-Day Plan	22
	• What Lawmakers Can Do	23
	About this Report and SecurityScorecard	24

Why We Wrote This

We rely on hospitals in our hardest moments. When hackers lock up a hospital's systems, ambulances are diverted, surgeries are delayed, and nurses go back to paper. This delays treatment and puts lives at risk.

SecurityScorecard set out to answer one simple question: **What does America's healthcare system look like to a hacker today?**

SecurityScorecard's Project Meridian platform maps cyber threats geographically, making it easy to see where risk is concentrated and how one breach can ripple outward. Our goal is to turn that map into clear answers anyone can grasp in one sitting.

WRITTEN BY

Michael Centrella

Richard Hummel

Dr. Mike Mylrea

Dr. Aleksandr Yampolskiy

HOW TO READ IT

Every section starts with a question. Charts come with a plain-English "so what." Gold boxes hold the one thing to remember. Gray boxes tell you what the data *can't* say.

39,319

U.S. HEALTHCARE RECORDS
the whole picture

12

TEXAS HOSPITAL GROUPS
our close-up case study

24

PAGES
about a 20-minute read

The Short Version: Key Findings at a Glance

A hospital's front door has a lock, but the front door to a hospital's internet-connected systems is open 24/7. Anyone can look for a way inside. Hackers do this all the time. They scan for old software, weak logins, and leaked passwords, and then pick the easiest target. We did the same thing, on purpose, so hospitals and lawmakers can see what the hackers see.

39,319

HEALTHCARE RECORDS

every U.S. healthcare record in our Project Meridian data

1 in 7

HAS A KNOWN EXPLOITED VULNERABILITY FLAG

bugs criminals are already using

3,767

RECORDS WITH LEAKED-PASSWORD SIGNALS

9.6% of all records

Six Key Findings



America's healthcare footprint is vast. In Project Meridian, we analyzed **39,319** healthcare records across 2,979 counties. Hospital records account for 29% of them. Rural clinics account for 7%.



Most healthcare facilities have decent grades. Of the 7,818 records that have a security grade, **62.5%** earn an A or B. But **1 in 6** gets a D or F.



About **1 in 7 records** shows a serious warning sign: 5,862 have a vulnerability that criminals are already exploiting in real attacks.



A good grade does not equal a clean bill of health. In our Texas deep dive, one hospital system earned an **A** despite having the most dangerous vulnerabilities on live systems.



Hospitals tend to buy from the same suppliers. In Texas, **11 of 12** hospital groups use Microsoft, and the same older web vulnerability appeared at **5** of them. A single supplier failure can ripple across many hospitals at once.



Rural clinics face higher risk and have less backup. **16.7%** score a D or F versus **15.2%** of hospitals. A clinic outage can leave patients with nowhere close to turn.

Meet the Patient: Who Is in Our Data, and Why It Matters

Who is the patient? Every healthcare record we could find in the U.S.

Before we can assess anyone's health, we need to know who is in the waiting room. **Project Meridian's** data lists 39,319 U.S. healthcare records. Each record is one facility or site, such as a large hospital, a small clinic, a surgery center, or a mental health center. The records span the 50 states, Washington, D.C., and the U.S. territories, and cover 2,979 counties.

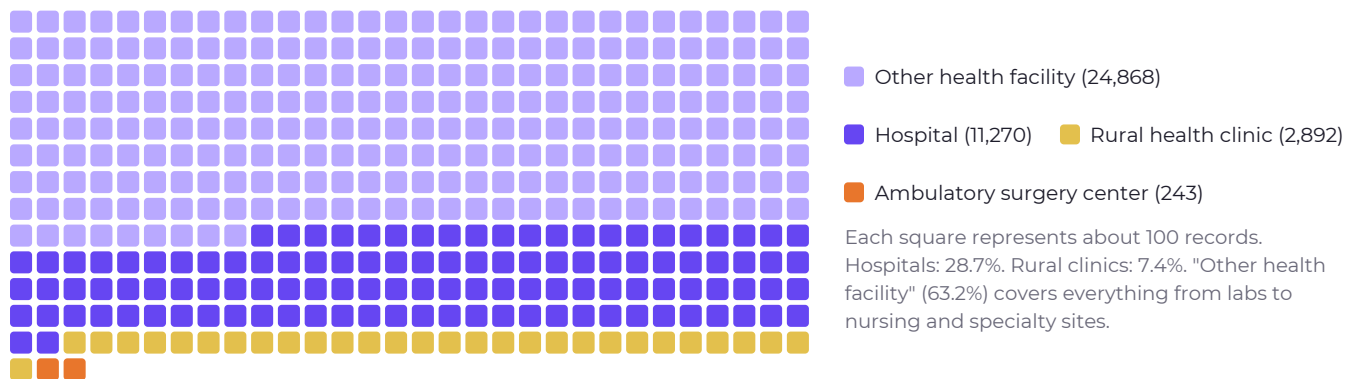


Figure 1: Selected U.S. healthcare records by type of care. One square represents ~100 records.

82.1%

HAVE A WEBSITE DOMAIN

32,294 records point to a domain hackers can look up

2,979

COUNTIES COVERED

rural and urban

7,873

HAVE A SECURITY GRADE

20.0% of all records

Why does this matter? Attackers begin with **internet addresses**, not hospital names. More than 8 in 10 of these records (32,248 of 39,319, or 82%) point to a website or domain, and each one is a point of entry that an attacker can probe.

A Hospital Is a Small City on the Internet

When you picture a hospital, you picture beds, doctors, and ambulances. A hacker pictures something else: email servers, patient portals, websites, cloud apps, staff logins, and the companies that sell all of it. Every one of those connections is useful to the hospital. Every one is also a possible entry point.

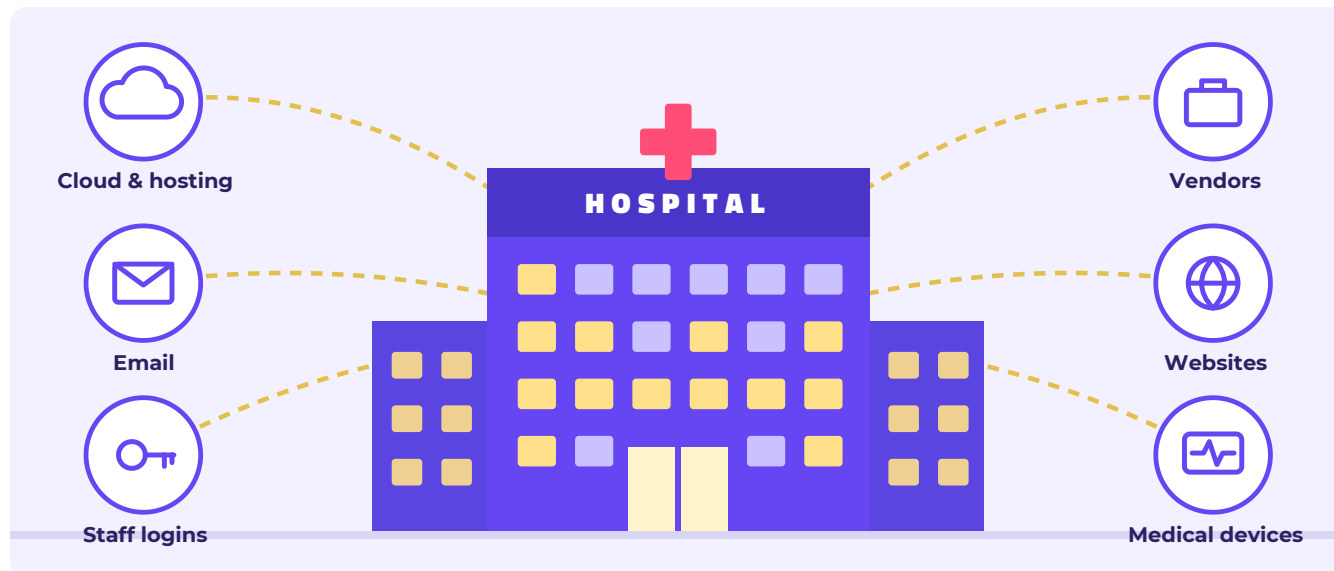


Figure 2: What a hacker sees when they look at a hospital from the outside.

The key idea behind this report is an **outside-in view**, the vantage point an attacker has. We do not break into any system or use a password. We collect what any stranger on the internet could see, then measure it.

WORDS YOU'LL SEE IN THIS REPORT

Security grade (A to F)

Like a school report card for a company's internet security. SecurityScorecard grades security from the outside in, just as a hacker does.

Known Exploited Vulnerability (KEV)

A bug that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) says criminals are *already* using in real attacks. This is the most urgent kind.

Leaked credentials

Stolen usernames and passwords that are posted or sold online, often harvested by malware on a user's device.

Bug (CVE)

Each gets a unique ID, like CVE-2020-11023, so everyone refers to the same issue.

Exploit Prediction Scoring System (EPSS) score

A forecast from 0 to 1 of how likely a bug is to be exploited in the next 30 days. 0.99 means "very likely."

Ransomware

Malware that can lock a computer, encrypt, or delete files until a hospital pays a ransom. It can force ambulances to go to other hospitals.

Where are They?

Healthcare is present in every part of the country, but some states hold far more of it in our data, California has **3,334** healthcare records, the most of any state shown here, and Texas follows with **3,297**. Together they account for about **1 in 6** of all records nationwide (16.9%).



Figure 3: Healthcare records for 10 states shown here. Gray represents other states.

Rural Care, State by State

The chart below shows where rural clinics are most concentrated: the states with the most rural clinic records in our U.S. healthcare inventory.

RURAL HEALTHCLINICS

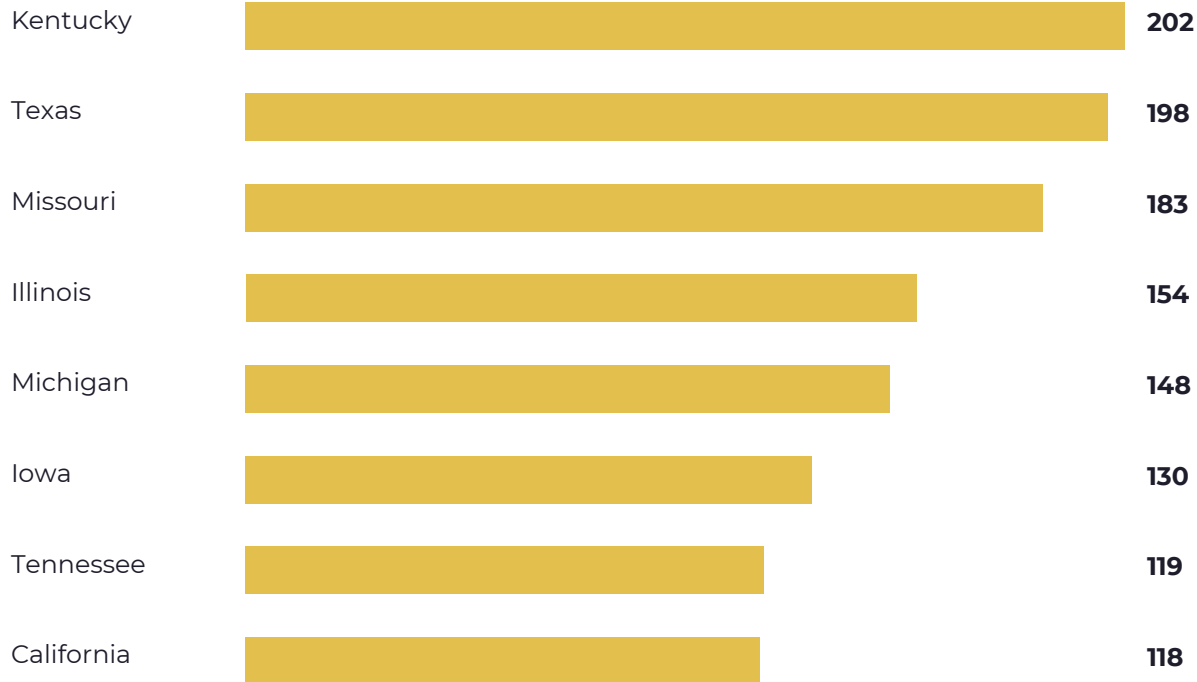


Figure 4: Rural clinic records by state. October 23 data.

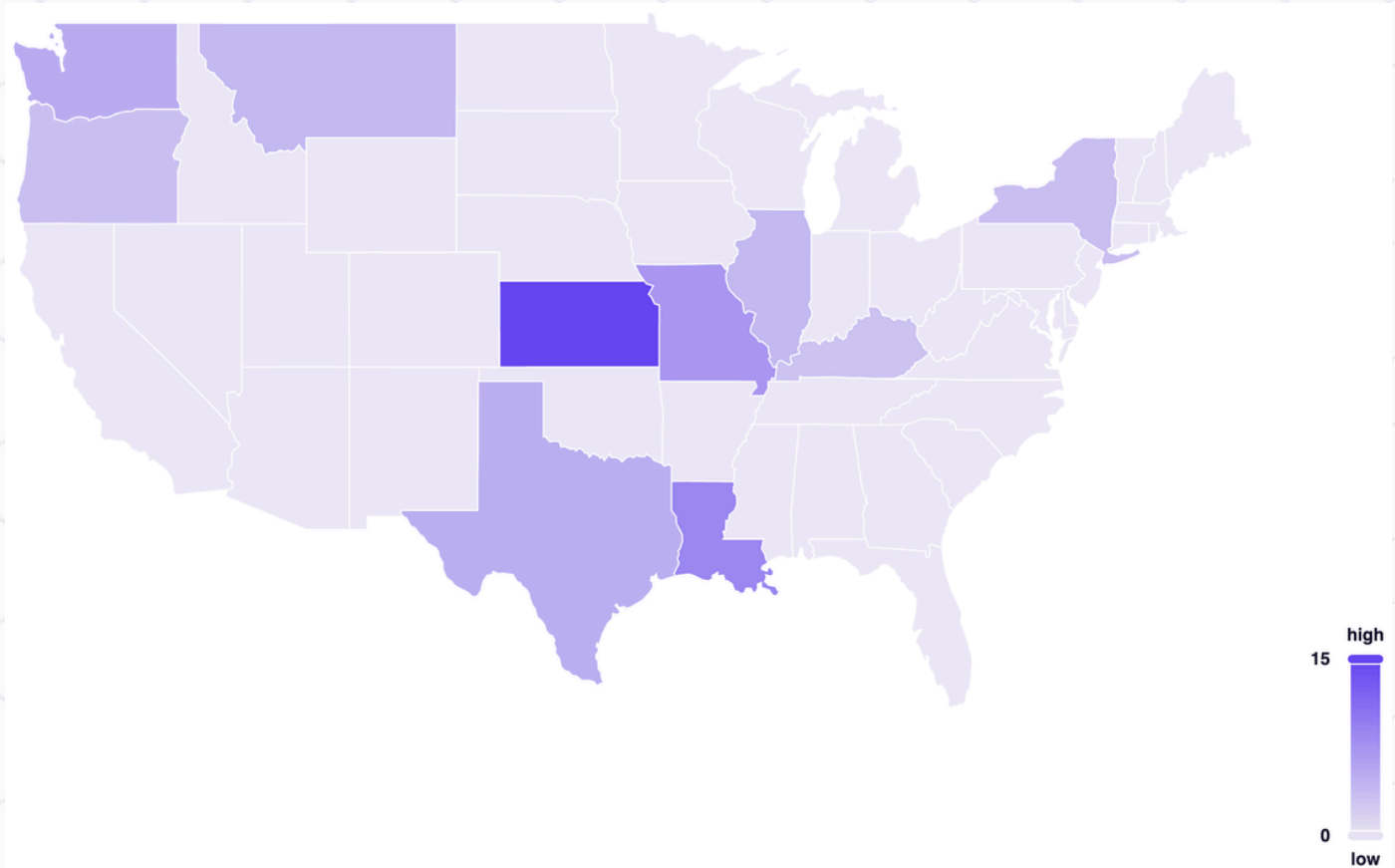
Rural Clinics Carry the Highest Stakes

Kentucky, Texas, and Missouri have the most rural clinic records in this inventory. When an urban hospital goes down, another is usually nearby. When a rural clinic goes down, the next facility can be miles away, turning a technology disruption into a gap in patient care. Section 5 explores this further.

Facility counts describe mapped records, not unique organizations. Care travel times and backup capacity require local verification.

Where D Grades Are Concentrated

Share of graded records earning a D in 10 states with at least 100 graded records.



D-grade share within each state's graded records. October 23 data.

Kansas	14.7%	Illinois	4.1%
Louisiana	8.7%	Montana	4.1%
Missouri	7.1%	New York	3.4%
Washington	5.1%	Oregon	3.2%
Texas	4.9%	Kentucky	3.1%

Pale states are outside this 10-state display. The map does not indicate zero risk. D-share is among graded records, not all facilities in a state.

The Report Card: How Healthcare Grades

If healthcare brought home a report card, what would it say?

SecurityScorecard gives organizations a grade from **A** (great) to **F** (failing), based on what we can see from the outside: things like old software, open doors (ports), and leaked passwords. **7,818** of the healthcare records in our data have a grade. Here's how they did.

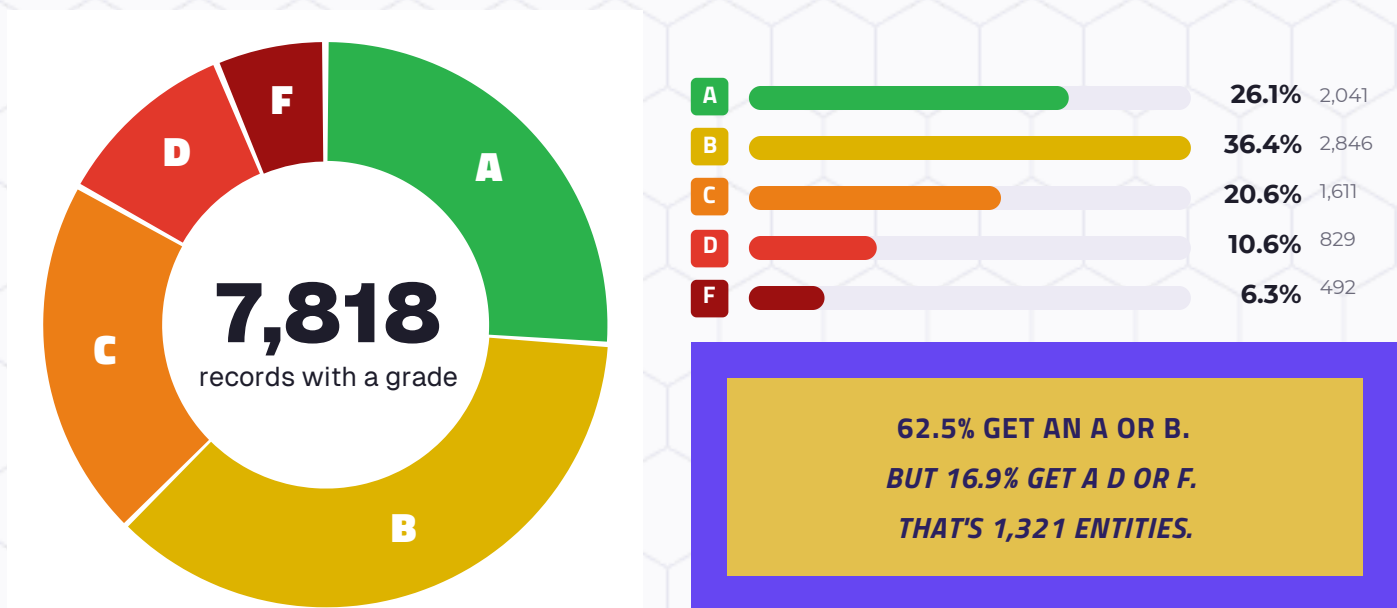


Figure 5: Security grades for the 7,818 graded records.

So, is healthcare passing?

Mostly, yes. A majority of graded records land in A or B. But think about it this way: if 1 in 6 students in a class failed, the teacher would want to know why, and fast. In healthcare, a failing grade isn't just embarrassing; it impacts patient care. SecurityScorecard research has found that organizations with poor grades are much more likely to suffer a breach.

Among 7,818 graded records in the October 23 A-F snapshot, 62.5% earned A or B and 16.9% earned D or F. This pattern may persist as more healthcare entities are graded; it is not a measured rate for every facility.

Does the Type of Care Change the Grade?

A little. Surgery centers do best: 70% get an A or B. Hospitals and rural clinics land in the middle. The "other health facility" group, which covers lots of small specialty sites, has the most F grades: **11.5%**, more than double the hospital rate.

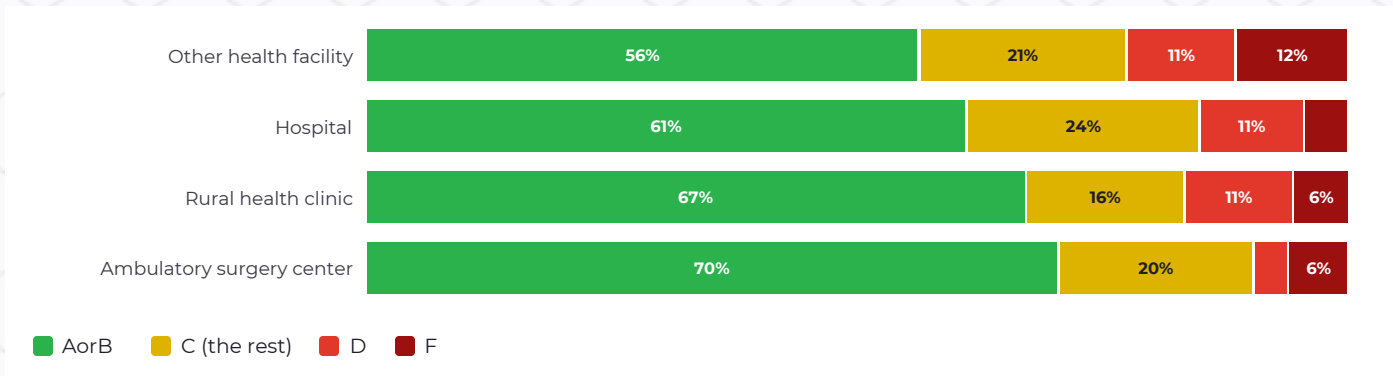


Figure 6: Grade mix by type of care (share of graded records). C is everything not shown as A, B, D or F.

How Grades Differ by Care Setting

Care setting	Graded	A or B	D	F
Other health facility	1,483	56.3%	11.1%	11.5%
Hospital	3,506	61.1%	10.6%	4.6%
Rural health clinic	2,607	67.1%	11.0%	5.7%
Surgery center	226	70.4%	3.5%	6.2%

Figure 7: A or B, D and F shares within each graded care setting.

October 23, 2026 snapshot. Percentages describe graded records in each group.

Warning Lights: Four Flags Across U.S. Healthcare

Which healthcare records have a warning light on the dashboard?

A car's dashboard has warning lights, and our data has them too. Each one is a **flag** on a record that says, "something here deserves a look." Four flags appear most often across all 39,319 U.S. healthcare records.



Figure 8: Records with warning flags, out of 39,319. One record can have several.

About 1 in 7 healthcare records



What each flag means

KEY: software with a flaw on the government's list of bugs that attackers are already exploiting (14.9%).

EPSS: a bug with a high likelihood of being attacked soon (15.2%).

Open ports: doors on a server that are open to the whole internet (11.8%).

Remote access: a way to log in from home that hackers often target (10.0%).

A flag isn't a break-in

"A warning light doesn't mean the engine is on fire. It means 'check this.' Some flags will turn out to be harmless. But when 1 in 7 records carries a critical-severity flag, teams face a long list of items to review, in a sector where every hour of downtime affects patient care.

5,862 HEALTHCARE RECORDS CARRY A KNOWN EXPLOITED BUG FLAG.

THAT'S THE PLACE TO START.

PHP2Shell: A New Web-Service Risk

Two PHP vulnerabilities disclosed in October 2026 let attackers run code on a web server without logging in. Healthcare organizations should first check whether any patient-facing or vendor-managed service runs an affected PHP version.

5 of 12

Texas hospital groups had a PHP technology label in the October 7 study.

This figure represents 41.7% of the sample, not a PHP2Shell rate.

7.67 Million

Distinct IPs tagged PHP in a 30-day internet scan.

This is not a vulnerable-installation count.

What Changed on October 21

PHP disclosed CVE-2026-109618 and CVE-2026-109619, two critical remote-code-execution flaws in installations serving web requests. The earlier Texas finding, CVE-2024-4577, is a different PHP CGI flaw. The Texas PHP label does not establish exposure to either new CVE.

Why It Matters to Healthcare

Patient portals, appointment tools, referral systems, and supplier services often depend on web software. If one of them runs an affected PHP version, a server compromise could interrupt access or expose data. Healthcare organizations should map the service and its owner before treating an internet scan as a hospital finding.

What Teams Should Do Now

- 1 FindPHP-backed public services, including vendor-run portals and APIs.
- 2 Confirm runtime version or vendor backport and the service owner.
- 3 Patch, restart workers, verify the service, and review relevant logs.

PHP's fixed releases: 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Linux and long-term-support vendors may ship backported fixes. Verify the package advisory. Patching the PHP runtime is the primary remedy, and it is not the whole response. Review [SecurityScorecard's advisory](#) on [securityscorecard.com](#).

Sources: PHP security advisory, 21 Oct 2026; Driftnet product-tag:php IP cardinality, 22 Sep-22 Oct 2026, 21:30 UTC; Visiting Hours Texas study, 7 Oct 2026.

Which Flaws Need Action First? Filtering Through 316 Vulnerabilities

Flags are a starting point. To see how they become a working to-do list, we examined **12 Texas hospital groups** (see Section 4). Their records listed 316 distinct vulnerabilities, a number that may sound alarming. Most of those entries are inferred from the software a facility appears to run, and none is confirmed on a specific machine. We kept only the vulnerabilities tied to a live host and listed in the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog. That filter cuts the list from 316 to 9.

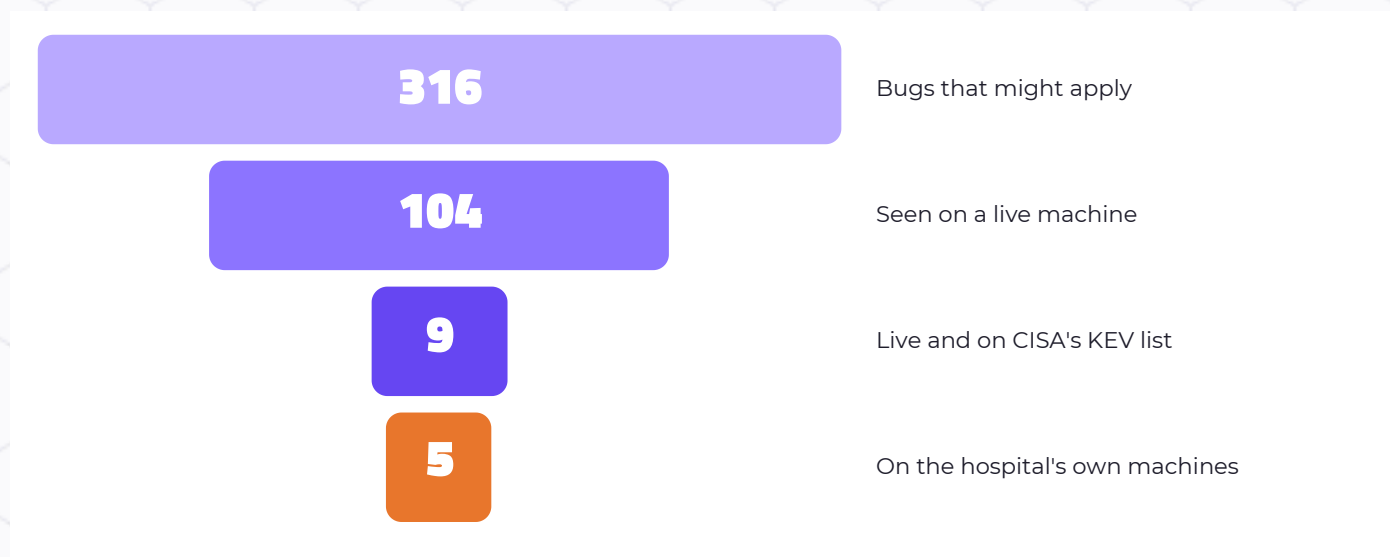


Figure 9: How 316 possible bugs shrink to 9 urgent ones across 12 Texas hospital groups.

**316 POSSIBLE PROBLEMS. 9 URGENT
ONES. 5 THE HOSPITALS CAN FIX
THEMSELVES.**

THAT'S A TO-DO LIST, NOT A DISASTER.

This is the most encouraging finding in the report. The large number of flagged vulnerabilities overstates the problem, because most entries are inferred from software a facility appears to run, not confirmed on a live system. The confirmed list is short enough that a small team could work through it in weeks.

There are urgent findings within that list. Three of the five confirmed vulnerabilities are ones the Cybersecurity and Infrastructure Security Agency (CISA) reports ransomware groups have used in attacks. Security teams should fix those first.

Texas Under the Microscope: What One State Shows About Healthcare Risk

What happens when you look closely at one state?

National numbers are useful, but they can feel distant. To illuminate how risk plays out locally, we examined one large state, Texas, which has 3,297 healthcare records in our data. We selected the 12 hospital groups with the largest internet footprints and studied each one. They range from large multi-state health systems to small rural clinics. We do not name them, because the aim of this analysis is to learn from the data.

Hospital group anonymized	Sites	Suppliers vendors seen	Urgent bugs on live machines orange represents they are on its own machines	Leaked passwords	Grade
System A Big multi-state system	4	354	●●●● 4	105	C
System B Big health system	8	614	●● 2	96	A
System C Big multi-state system	11	564	●●●●●●●● 8	17	A
Hospital D Regional hospital	5	41	0	0	A
Hospital E Rural hospital	2	6	● 1	not returned	C
Clinic F Children's clinic	2	2	0	0	A
Hospital G Rural hospital district	1	28	●● 2	0	B
Hospital H Community hospital	1	36	0	507	B
Hospital I Rural hospital	3	28	0	0	B
Hospital J Rural county hospital	2	11	0	0	A
System K Big health system	2	97	0	54	B
Clinic L Rural children's clinic	2	38	● 1	0	A

Figure 10: The 12 Texas hospital groups in our deep dive.

43

SITES

hospitals, clinics, and offices

232

INTERNET-FACING MACHINES

what a hacker can reach

313

DIFFERENT SUPPLIERS

72 used by 2+ groups

779

LEAKED LOGINS

across all 12 groups

Data collected October 7, 2026. Groups chosen by the size of their internet footprint among Project Meridian's 3,297 Texas healthcare records.

A Strong Grade Can Still Hide a Dangerous Server

You might expect the best-graded hospitals to have the fewest urgent vulnerabilities. That is not always the case. Figure 11 pairs each Texas group's grade with the urgent vulnerabilities found on its live machines. Six of the 12 groups earn an **A**. One of those A-rated groups has **eight urgent vulnerabilities**, the most of any group, and four sit on their own machines.

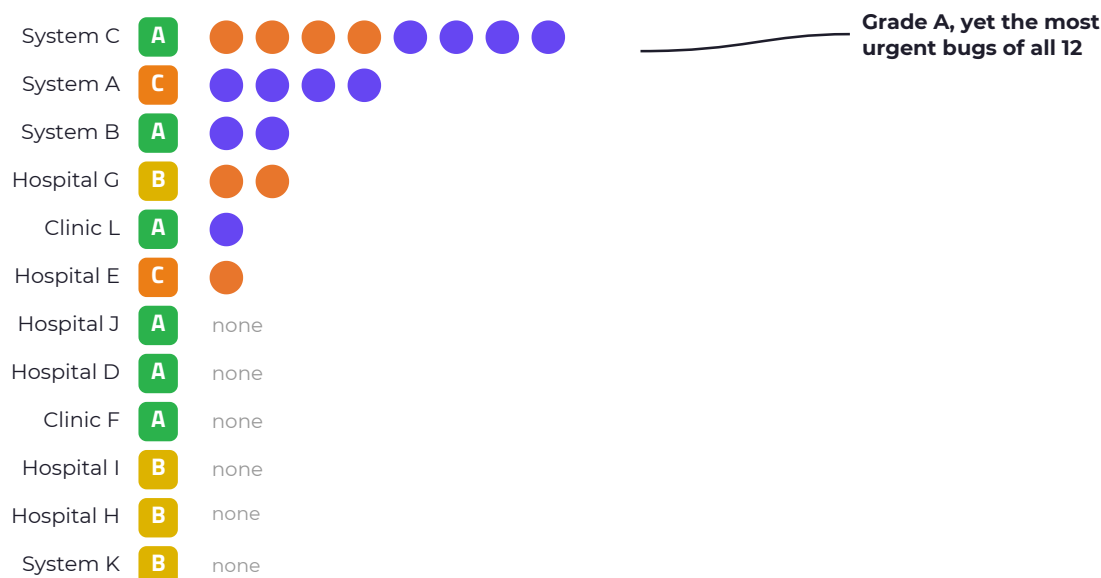


Figure 11: Grade vs. urgent (KEV) bugs on live machines. Orange represents that they are on the hospital's own machines.

How can that happen? A grade summarizes a large system's overall posture across thousands of machines. A system can be well run overall and still have a few dangerous servers in a corner. **For lawmakers, that's the lesson: a grade is where the questions start, not where they end. Verification has to follow.**

THE FIVE URGENT BUGS ON HOSPITALS' OWN MACHINES AND WHY THEY MATTER

CVE-2021-40438 · attack forecast 99% · CISA ransomware use: **Known**
Web server flaw that can trick it into reaching inside the network.

CVE-2025-10035 · attack forecast 99% · CISA ransomware use: **Known**
File-transfer tool flaw. Ransomware gangs have used it.

CVE-2020-11023 · attack forecast 84% · CISA ransomware use: **Unknown**
Old web page code flaw. Found at 5 different hospital groups.

CVE-2024-38475 · attack forecast 99% · CISA ransomware use: **No**
web server flaw

CVE-2024-4577 · attack forecast 99% · CISA ransomware use: **Known**
Flaw that lets an attacker run commands through PHP

Shared Suppliers: How One Vendor's Bad Day Reaches Many Hospitals

If one supplier has a bad day, how many hospitals have a bad day with it?

Hospitals don't build their own software. They buy it, just like you buy a phone instead of building one. That means many hospitals end up relying on the same ones. The 12 Texas groups use 313 different vendors between them, and **72 of those (about 23%) appear at two or more groups**. A problem at one of those shared vendors can reach several hospitals at once.

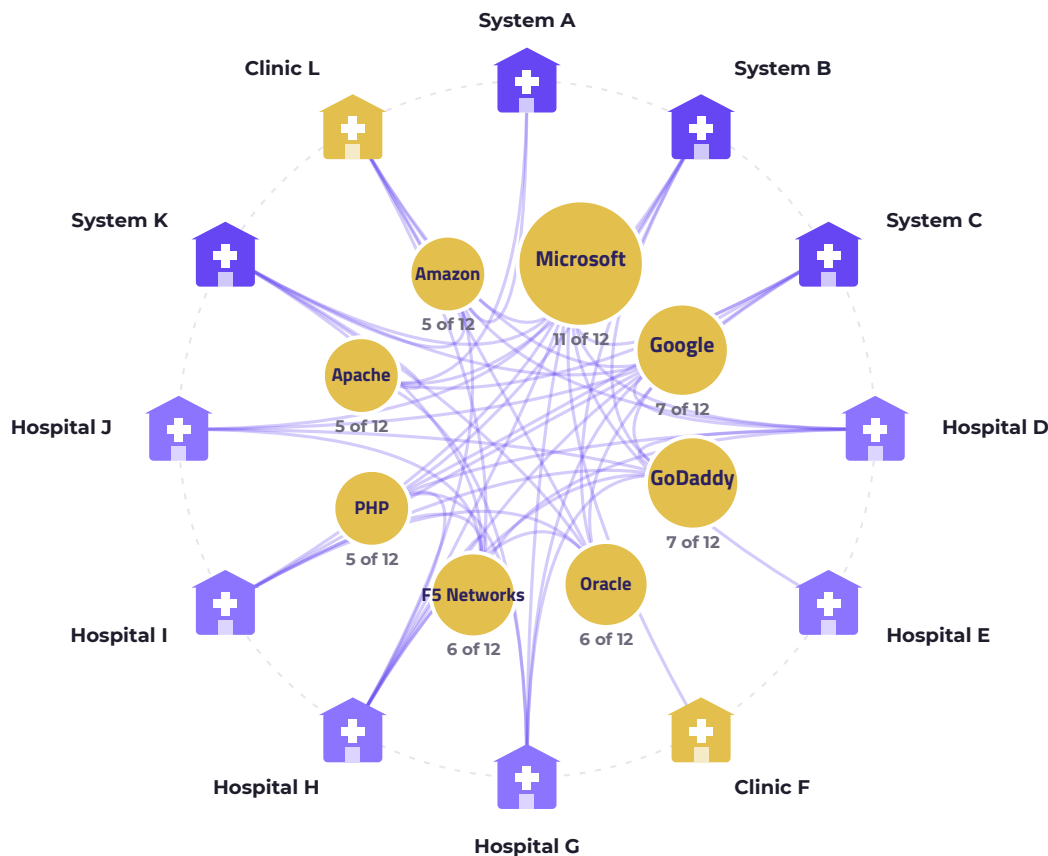


Figure 12: The 8 most-shared suppliers (gold) and the Texas hospital groups that use them. Bigger circle represents more hospitals.

Hospitals don't have to be hacked to go down. Their supplier does.

In 2024, a ransomware attack on Change Healthcare, a UnitedHealth Group subsidiary that processes payments and insurance claims, disrupted pharmacies and hospital billing across the country for weeks. Most of the affected hospitals were not breached themselves. Their shared supplier was. Figure 12 shows how closely Texas hospitals are tied to the same few companies.

Stolen Keys and Noisy Neighbors: Two Warning Signs in the Texas Data

Leaked passwords

Across the 12 Texas groups, **we found 779 leaked login records**. One community hospital accounts for 507 of them, or 65% of the total. That is more than the three biggest systems combined.

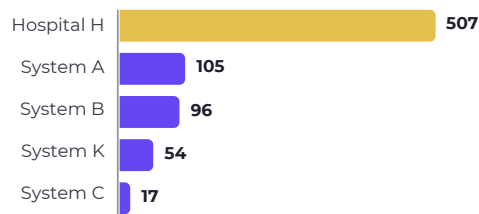


Figure 13: Leaked login records per hospital group (groups with zero not shown).

Ransomware gang names nearby

Twelve of the 232 hospital machines sit on an internet address that is also linked to a ransomware gang's name. LockBit 3.0 appears most often.

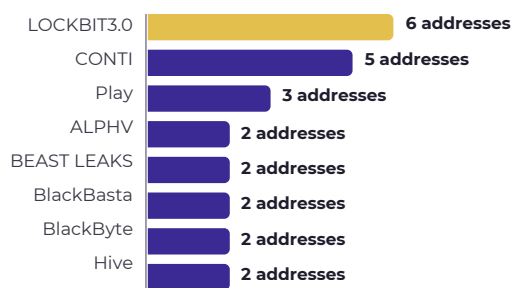


Figure 14: Ransomware gang names seen on the same shared addresses.

Important Context: Every one of those 12 addresses belongs to a large shared platform, such as a big cloud or web hosting company, where 1,000 or more customers share the same address. It is like living in a huge apartment building where one tenant is a criminal. The label does not mean the hospital is involved, and none of the hospitals' own machines carried a gang name.

**ONE COMMUNITY HOSPITAL
ACCOUNTS FOR 65% OF LEAKED
PASSWORDS IN THE TEXAS SAMPLE.**

Leaked passwords are one of the cheapest ways into an organization. They trigger no alarms, because the system sees a valid login and treats the attacker like a normal employee. One low-cost step cuts the risk: require **multi-factor authentication** (a second proof of identity, such as a code sent to your phone) on every remote login, email account, and patient portal.

Far From Help: Why the Same Cyberattack Hurts Rural Care More

What happens when the only clinic for miles goes dark?

There are **2,892** rural clinic records in our data. In a city, when one hospital's computers fail, an ambulance can drive across town. In the country, the next clinic or emergency room can be a long drive away. **The same cyberattack does more damage when the backup is far.**

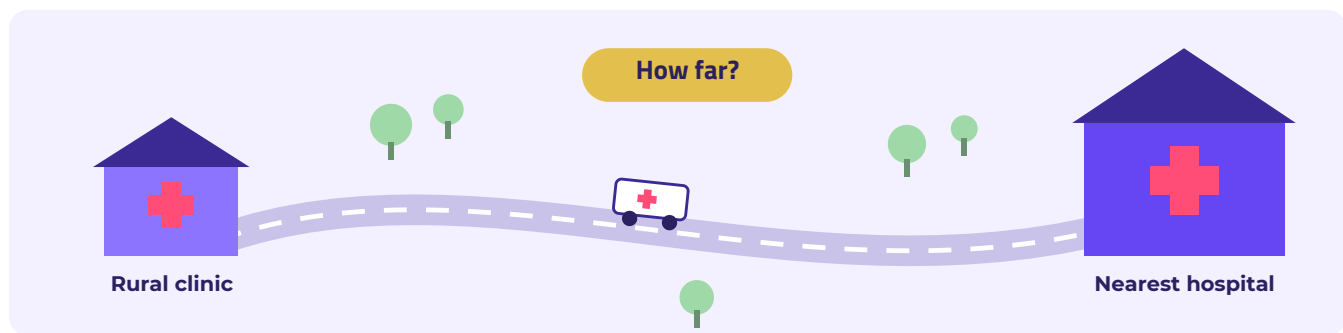


Figure 15: In rural America, distance turns a computer problem into a patient problem.

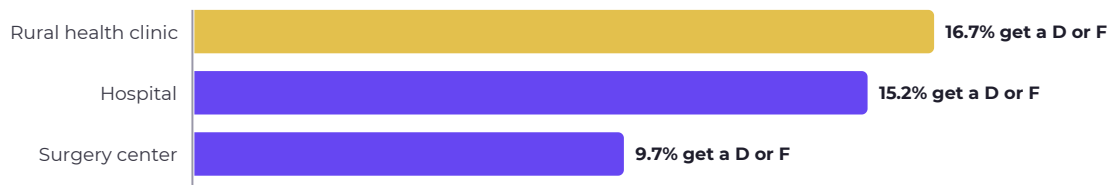


Figure 16: Share of graded records that get a D or F, by type of care.

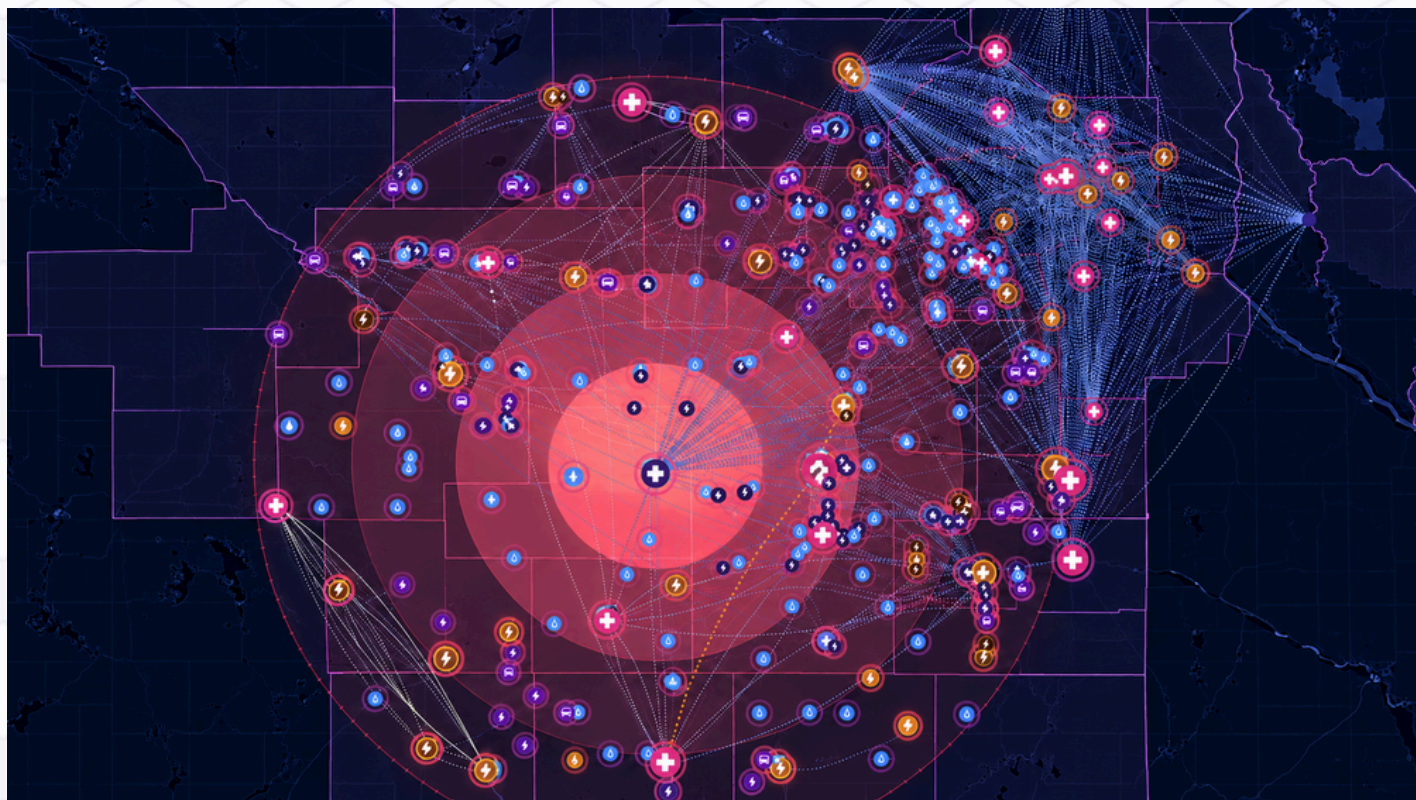
Among graded records, rural clinics have a slightly higher share of D or F grades than hospitals: 16.7% against 15.2% in the October 23 snapshot. These grades measure cyber posture and say nothing about how often clinics fail. The practical risk is the distance. A rural disruption is harder to absorb when staff, backup systems, and alternate care sit farther away.

16.7% OF RURAL CLINICS HAVE A D OR F.

THEY ALSO HAVE SMALLER TEAMS, FEWER BACKUPS, AND LONGER DRIVES.

Far From Help: The Connected Map

A rural clinic is part of a wider network of care and infrastructure. Meridian's view shows why a local disruption can require a regional continuity plan.



Project Meridian View: A 60-mile assessment radius centered on a single, representative hospital.

What the Connections Reveal

Project Meridian shows relationships between critical sectors, the shared vendors, shared digital infrastructure, and even shared vulnerabilities. This inter-connected view allows cyber defenders to identify the most at risk systems, vendors, and connections to remediate them first. It may not always be the highest severity vulnerability, but an attack targeting an older vulnerability sharing infrastructure and connection with five other hospitals has **a cascade effect that will ripple through the healthcare system** if successful. Prioritizing defense based on reach becomes the top priority for defenders.

- **Care routes:** Nearby hospitals and clinics that may be asked to receive patients.
- **Essential services:** Power and water assets worth checking in a downtime plan.
- **Shared technology:** Common domains, suppliers, and access paths that can span sites.

A mapped connection is a lead to validate. It does not confirm a live dependency, an outage, or patient impact. The blast-radius view (how far one failure could spread) is useful because it shows which owners must confirm the care route and shared services before a crisis.

Stolen Keys: How Attackers Can Walk In Through the Front Door

Are hackers already holding keys to healthcare?

Software flaws are one way in. Stolen credentials are another, and often easier. Our data flags records with **leaked passwords**, **hints of ransomware**, **evidence of attack traffic**, and, in a very few cases, signs that an attacker's command-and-control server is communicating with a machine.

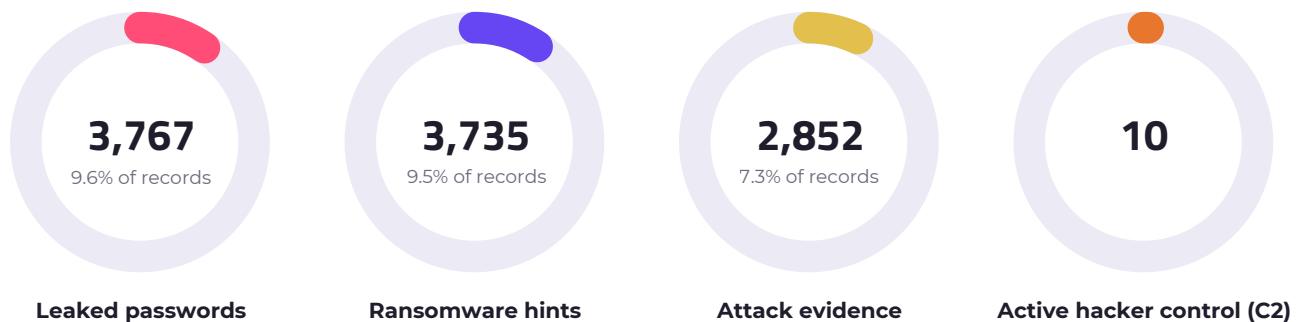


Figure 17: Identity and threat signals across all 39,319 U.S. healthcare records in Project Meridian.
Rings show share of all records.

Almost 1 in 10 has a leaked-password signal

A total of 3,767 records or **9.6%** carry a leaked-credential signal. Some are old passwords that were changed long ago, and some may still work. The only way to know is to check. Either way, multi-factor authentication is the safest protection.

Only 10 show "active control." Good.

Command-and-control (C2) means a hacked machine may be taking orders from an attacker. **Only 10** of nearly 40,000 records show that signal. Each one is worth a phone call this week.

READ WITH CARE: These are signals on records. They do not confirm a break-in. "Ransomware hints" means our sources saw ransomware-related activity connected to a record's internet footprint, which can include shared platforms. A person needs to check each one.

NEARLY 1 IN 10 HEALTHCARE RECORDS SHOWS A LEAKED-PASSWORD SIGNAL.
MULTI-FACTOR AUTHENTICATION IS ONE OF THE LOWEST-COST REMEDIES IN THIS REPORT.

What Could Go Wrong

What happens when a cyberattack and a physical attack hit together?

Here are three short scenarios built from our data. They are not predictions. They are “what if” stories of the kind emergency planners use to practice, and each one starts from something real in our data.

Story 1: The clinic that went quiet · a rural clinic

What's true today	2,892 rural clinic records with 16.7% of graded ones receiving a D or F.
Monday 7 a.m.	Staff can't log in. The patient system is locked by ransomware. Phones still work.
Monday noon	Appointments are cancelled. An ambulance call goes to a hospital far away instead.
Day 3	Paper charts. The one IT contractor is overwhelmed. Nobody knows which nearby clinic can take extra patients.
What would have helped	A tested backup plan, a list of who takes patients, and MFA on every login.

Story 2: The A-grade hospital with a bad corner · a large health system

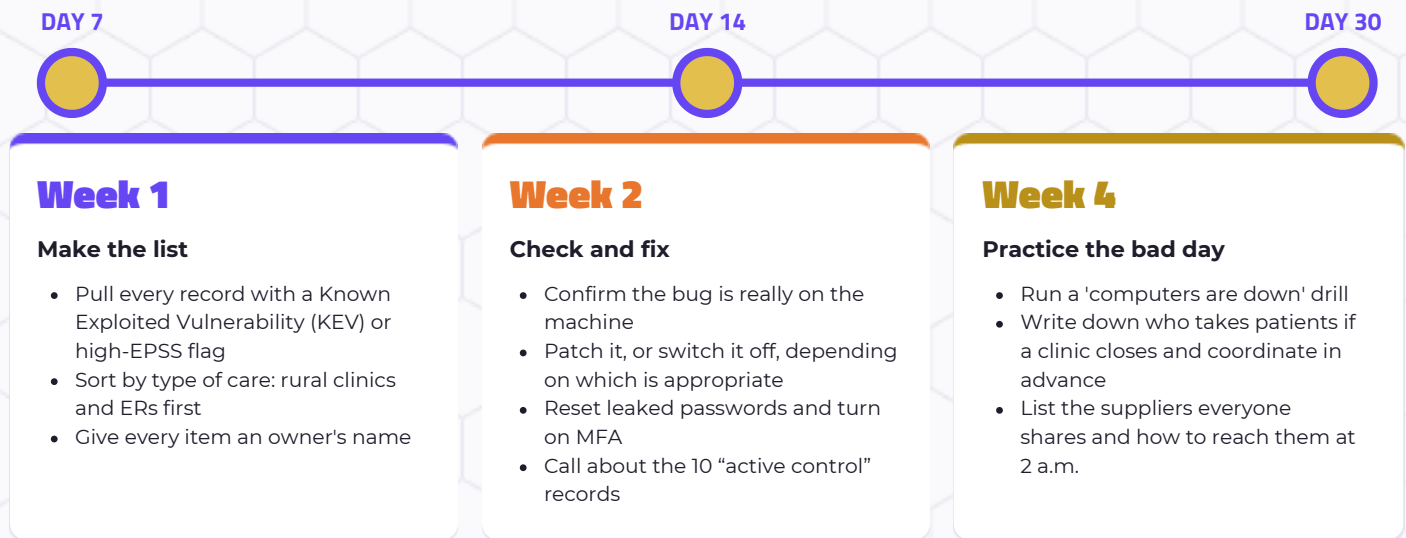
What's true today	An A-rated Texas system has eight urgent bugs on live machines, four on its own network.
Week 1	A criminal group scans the internet for one of those bugs. It finds this hospital's research server.
Week 2	They get in, probe around, and copy files.
Week 3	A ransom note appears. The good grade didn't protect the one forgotten server.
What would have helped	Fixing the five urgent bugs on the hospital's own machines first.

Story 3: The supplier domino · many hospitals at once

What's true today	Eleven of the 12 Texas groups share Microsoft, and one old web flaw sits at five of them.
Day 1	A widely used healthcare supplier is hit by an attack. The hospitals themselves are fine.
Day 2	Billing, prescriptions, or scheduling stop working at hundreds of sites. Each hospital decides alone what to do.
Week 2+	The 2024 Change Healthcare incident showed this can last for weeks.
What would have helped	Knowing which suppliers every hospital depends on, and a shared plan.

What to Do Next: A 30-Day Plan

Most of the technical risks in this report can be addressed with practical steps. The plan below gives state health departments, hospital groups, and rural clinic networks a way to begin this month.



How to Tell If It's Working

Track three numbers every month and share them with leadership:

% assigned

OF FLAGGED RECORDS

has an owner's name next to it

% fixed

OF URGENT BUGS

devices confirmed patched or switched off

% practiced

OF CARE REGIONS

have run a downtime drill

WEEK 1 MAKES THE LIST. WEEK 2 FIXES THE WORST. WEEK 4 PRACTICES THE BAD DAY.

Who Does What Next

Proposed owners and proof of completion for the 30-day plan:

WHEN	PROPOSED OWNER AND ACTION	EVIDENCE
Day 7	Project Meridian research: route a dated priority list by KEV, EPSS, and care setting.	Named owner and source date
Day 14	Provider security: verify product, version, and care service; fix priority hosts.	Dated host disposition
Day 14	Identity teams: review leaked logins and remote access with domain owners.	Account response log
Day 30	State and care networks: rehearse rural downtime, referral, and transport.	Receiving site; call tree
Day 30	Suppliers: confirm live service dependencies and fallback with each provider.	Tested escalation path

These are recommended assignments. Local operators must confirm ownership and dependencies.

What Lawmakers Can Do

1. Direct funding to where it matters most.

Provide grants and shared security services for rural clinics and small hospitals, tied to fixing Known Exploited Vulnerabilities. These facilities have the smallest teams and the fewest resources.

2. Treat major healthcare suppliers like critical infrastructure

When one supplier serves thousands of hospitals, its security affects every hospital that depends on it. Oversight of key suppliers protects many facilities at once.

3. Set MFA as the minimum standard

Of 39,319 healthcare records, 3,767 carry a leaked-credential signal. Requiring multi-factor authentication (MFA) on remote access, email, and patient portals is a low-cost control that addresses this risk.

4. Measure from the outside, not just with surveys

An A-rated hospital had the most urgent vulnerabilities in our Texas sample. Outside-in measurement gives an ongoing, independent view that does not depend on self-reporting.

5. Fund rural downtime planning

Support state-led drills that answer one question: if this clinic's computers go dark, where do its patients go, and how do they get there?

The bottom line

Visiting hours on the internet never end. Attackers will keep probing healthcare systems continuously, and that pressure will not ease. The data offers an encouraging finding, though: the most urgent problems form a short list can be addressed. The work ahead is to ensure that every hospital and clinic, especially the small ones, has the support to work through it.

About SecurityScorecard

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard is the global leader in threat-informed third-party risk management (TPRM), securing the world's supply chains. The company delivers a threat-informed approach to TPRM that enables organizations to drive out risk at the source. The platform uses continuous visibility and AI-accelerated workflows to help organizations reduce third-party risk before incidents occur and respond with confidence when they do.

Trusted by 3,000 organizations, including over 70% of the Fortune 100, and recognized as a trusted resource by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

SecurityScorecard's mission is to make the world a safer place by transforming the way organizations understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. Every organization has the right to its own trusted and transparent security rating. **Project Meridian** applies SecurityScorecard's outside-in data to critical infrastructure, mapping facilities, the suppliers they share and the exposures attackers can see.

Protect the supply chain behind your business. Learn more at securityscorecard.com.

About the authors

Michael Centrella — Head of Public Policy. He is a former Assistant Director of the U.S. Secret Service with more than 25 years of experience in federal law enforcement and national security.

Richard Hummel — Vice President of Threat Intelligence & Research. He specializes in malware and network operations.

Dr. Michael Mylrea — Chief AI Officer and Chief Information Security Officer (CISO). He previously worked at Arctic Wolf and GE Research and holds a Ph.D. in applied AI.

Dr. Aleksandr Yampolskiy — Co-Founder and CEO. He previously served as CISO of Gilt Groupe and holds a Ph.D. in cryptography from Yale University.

About the data

National inventory: 39,319 U.S. healthcare records (October 23, 2026). The A-F distribution covers 7,818 graded records from that snapshot. Signal counts and the provider-graded total of 7,873 were refreshed October 27, 2026. The Texas study covers 12 hospital groups on October 7, 2026. Bug flags use CISA KEV and FIRST EPSS. These outside-in observations invite verification; they do not establish breach, live dependency or patient harm. Facility names are withheld.

Methodology:

Scope and Data Sources: This report uses outside-in observations of U.S. healthcare organizations, gathered from public internet data. It draws on Project Meridian's national inventory of 39,319 healthcare records, as of October 23, 2026. Each record is a mapped site, not a unique health system or patient, and counts are records, not organizations or people.

Grades: The A to F distribution covers 7,818 graded records from the October 23 snapshot. Signal counts and the provider-graded total of 7,873 were refreshed on October 27, 2026. Grades describe measured cyber posture among sites with a provider grade. They support a general expectation about the sector, not a forecast for sites that are not yet graded.

Vulnerability Flags: Flags use two public sources.

- The Cybersecurity and Infrastructure Security Agency's (CISA's) Known Exploited Vulnerabilities (KEV) catalog, which lists vulnerabilities that attackers are known to have exploited.
- The Forum of Incident Response and Security Teams' (FIRST's) Exploit Prediction Scoring System (EPSS), which estimates the chance that a vulnerability will be exploited in the next 30 days.

A site can carry more than one flag, so flag counts overlap and should not be added together.

Texas Case Study

The Texas study examines 12 hospital groups, as of October 7, 2026. Facility names are withheld.

Limits

These observations come from outside each organization and invite verification. They do not establish a breach, a live dependency, or patient harm. An owner must confirm the affected host, product, version, and clinical service before treating a flag as a finding.