

PQC in Healthcare: From Data Risk to Migration Readiness



Exploring Today's Security Threats in Healthcare and the Challenges of PQC Migration

Key Findings

- Healthcare organizations rely on thousands of specialized connected devices that are significantly less prepared for post-quantum cryptography (PQC) than traditional IT systems.
 - Only 6% of IoMT devices and 16% of OT devices currently use SSH implementations that support post-quantum cryptography, compared to 50% of IT devices.
- The devices that are hardest to upgrade are often those that healthcare organizations depend on most for patient care.
 - More than 5,500 internet-exposed healthcare systems were identified, including EMR and PACS platforms containing healthcare data.
 - Across exposed healthcare systems, only 31% support TLS 1.3, the only TLS version capable of supporting standardized post-quantum cryptography.
- Healthcare data – including medical histories, diagnostic images, lab results, and prescription records – remains valuable for a lifetime, making the sector especially vulnerable to harvest-now, decrypt-later (HNDL) attacks. Data most at risk for quantum attacks is that which:
 - Is commonly transported over TLS or other cryptographic protocols using quantum-unsafe RSA or elliptic curve cryptography for authentication and key establishment today.
 - Has long confidentiality lifetime, making HNDL attacks relevant
 - Is likely to be recorded or intercepted when traversing external networks, including the internet, partner links, remote access solutions, cloud applications, and others.
- Based on network presence, data processed or stored, and exposure, the five data types currently most at risk for quantum attacks in healthcare organizations are: electronic medical records, medical imaging, laboratory results, medication and prescription data and financial/payment data.

Recommendations Summary

Healthcare PQC planning goes beyond a simple device or protocol checklist — it requires understanding which assets can be upgraded, which cannot, and what sensitive data each one protects.

Our full Recommendations section outlines a phased approach HDOs can take over the next 6, 12, and 24+ months to map risk, prioritize exposed assets, update infrastructure, and build long-term resilience ahead of PQC mandates or practical quantum attacks. Read the full Recommendations section ([#recommendations](#)) for detailed, phase-by-phase guidance.

Introduction

Healthcare delivery organizations (HDOs), such as hospitals, clinics, urgent care facilities, rehabilitation centers, long-term care, and skilled nursing facilities, rely on a diverse array of Information Technology (IT), Internet of Medical Things (IoMT), Operational Technology (OT), and Internet of Things (IoT) devices that are increasingly integral to the delivery of patient care.

The growing number and variety of these devices have introduced significant cybersecurity risks to HDOs in the past decade. Threat actors are increasingly exploiting these devices to deploy ransomware, demand large payments, and monetize stolen patient data. We have seen a sharp increase in number and sophistication of cyberattacks targeting healthcare with severe consequences including data breaches, disruption of critical healthcare functions, and, in the worst cases, direct threats to patient safety. Regardless of attack type, patients are impacted most, through delayed or denied care or loss of privacy due to exposed data.

Between January 1 and August 31, 2026, we tracked 461 public ransomware claims against healthcare providers globally, a 47% increase over the 313 claims observed in the same period last year. 299 of these claims (65%) were against US organizations. Between January and August 2026, we also tracked 300 hacktivist attack claims against organizations in the same sector globally. These hacktivist attacks were split as follows:

- 31% attempts to control or disrupt systems such as IoT, OT and IoMT
- 30% distributed denials of service (DDoS)
- 27% data breaches
- 11% defacements

To maintain patient privacy and safety, healthcare providers must continue strengthening defenses against today's threats and prepare for emerging challenges and risks. While most security leaders are closely watching adversarial use of artificial intelligence, another dual-use technology has been advancing rapidly (<https://www.forescout.com/blog/countdown-to-q-day-what-pqc-ciphers-are-you-using-today/>) without the same level of widespread awareness: quantum computing. Governments and organizations are now concerned that a quantum computer could break traditional asymmetric encryption as early as 2029 (<https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/>). HDOs already operate under strict regulatory frameworks such as HIPAA, and regulators are expected to interpret "appropriate security" for HDOs as requiring quantum resilience. This shift in regulatory requirements will likely come much sooner than many healthcare organizations expect.

The most often discussed quantum threat is "harvest now, decrypt later (https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later)" (HNDL) where attackers intercept encrypted data today and store it for quantum computers to decrypt it in the future. This is particularly relevant for HDOs given the value and longevity of patient information. While data like financial transactions can be short-lived, healthcare data is lifelong. Medical histories, imaging archives, diagnoses, mental health notes, and genetic biomarkers follow you from birth, and their sensitivity doesn't diminish over time. Furthermore, healthcare datasets combine personal information, financial and insurance data, clinical history and other sensitive information. These datasets are monetizable and irreversible if exposed. They are often more valuable than credit cards or account numbers in underground markets because they cannot be "reset."

PQC migration in healthcare is not just about data confidentiality, but also patient safety (<https://www.mitre.org/sites/default/files/2026-04/PR-26-0682-Cybersecurity-Risk-Analysis.pdf>). Cryptography protects commands sent to medical devices, telemetry received from those devices for diagnostic purposes, medication orders, and other sensitive interactions. Quantum threats include unauthorized remote access by exploiting public keys for authentication, tampering with device-to-device communication by decrypting traffic, and sophisticated malware exploiting firmware integrity signatures.

The good news is that PQC (<https://www.forescout.com/solutions/post-quantum-cryptography-risk/>), which is not susceptible to quantum threats, already exists. In August 2024 (<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>), NIST standardized one algorithm for key exchange (ML-KEM) and two for digital signatures. The most popular cryptographic protocol, Transport Layer Security (TLS) – which forms the basis of services such as HTTPS, FTPS and others for data transfer – already supports ML-KEM in TLSv1.3 (<https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>). So does Secure Shell (SSH), which is used for remote management of devices.

However, migrating assets to adopt PQC is not a simple task. It includes updating or replacing IT, OT, IoT, medical devices, and other network-connected assets. Our tracking (<https://www.forescout.com/blog/pqc-adoption-gaps-90-percent-of-systems-are-still-not-quantum-safe/>) of PQC adoption reveals a widening readiness gap across device types:

- Only 11.8% of SSH servers on the internet are PQC-capable. That number falls to 3% when considering Dropbear servers, a common SSH implementation for embedded devices.
- In enterprise networks, 50% of IT devices use OpenSSH versions that support PQC, but only 28% of IoT, 16% of OT, and 6% of IoMT devices use these same versions.
- TLSv1.3 – the only version that supports PQC – only runs on 30% of identified servers on the internet.
- In enterprise networks, IT devices most commonly support PQC on TLS (8%), while specialized devices are again left behind (5.6% for IoT and IoMT, 0.8% for OT)

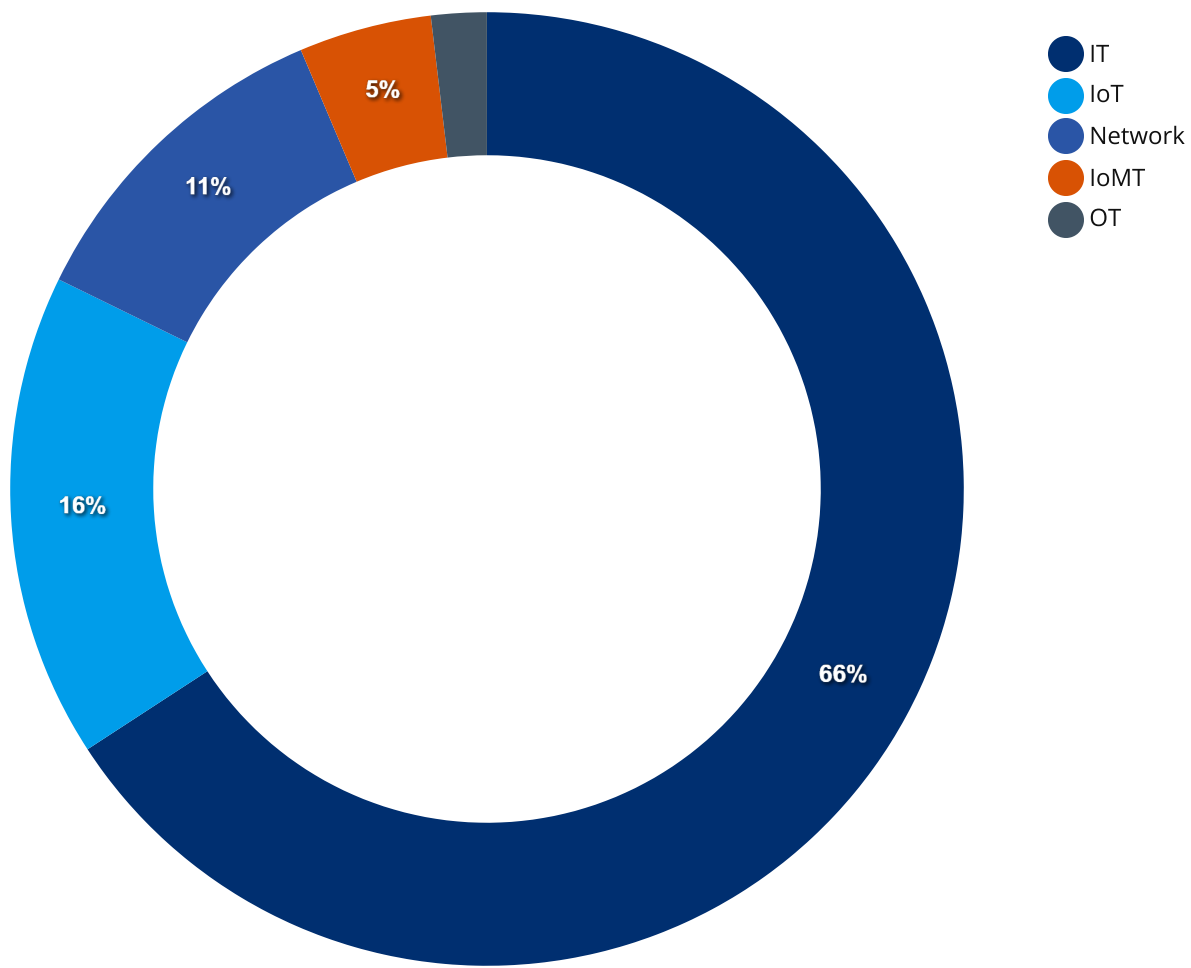
Specialized devices are unlikely to be fully migrated this decade if we keep going at the current pace, delaying broader PQC migration efforts and quantum readiness. Unfortunately, medical devices are among those with the lowest adoption rates and the hardest challenges for adopting PQC (<https://www.mitre.org/news-insights/publication/cybersecurity-risk-analysis-medical-devices-era-evolving-technologies>) .

In this report, we explore the devices currently present in healthcare networks, what kind of data they generate, transmit, process, or store, which of those assets are most commonly exposed, and what that means for quantum threats in healthcare.

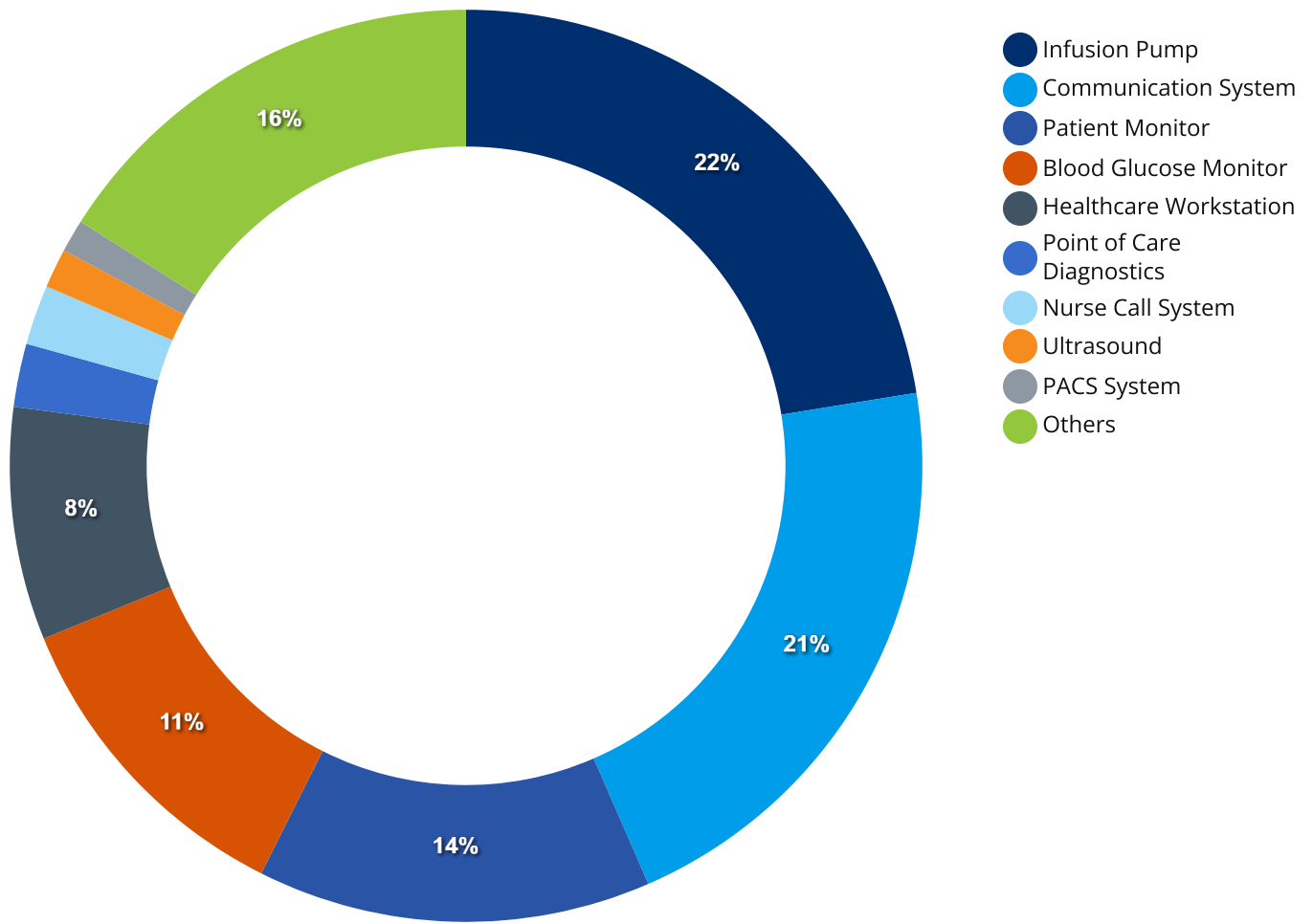
Assets and Threats

Using a Forescout Device Cloud dataset containing more than 2.5 million devices across more than 50 HDO networks – an average of around 50,000 devices per HDO – we see the following distribution of device types.

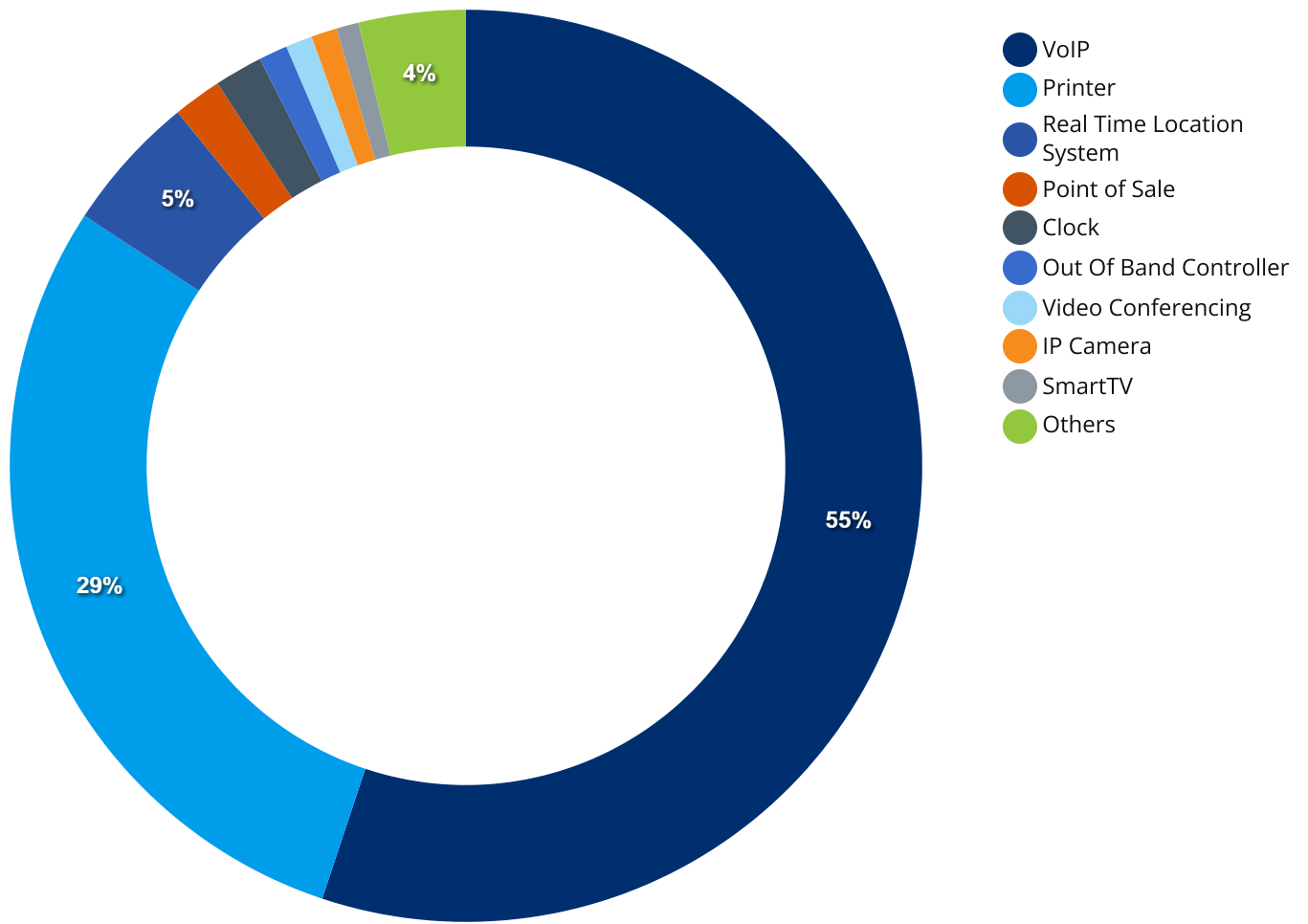
Device Types in HDOs



Most Common IoMT Device Functions



Most Common IoT Device Functions



While IT assets account for most devices in HDOs (66%), healthcare environments also rely on a wide variety of specialized IoT, IoMT, and OT technologies. From infusion pumps and patient monitors to communication systems and real-time location systems, many of these purpose-built devices have long operational lifecycles and are difficult to patch or upgrade. Because of this, the PQC transition is expected to be long and complex for these assets. Not only does our data show that they are being left behind, but related research (<https://arxiv.org/abs/2508.16078>) shows that planned PQC support across several cryptographic libraries used for embedded devices is uneven.

IT and Network Devices

About two-thirds of connected assets in HDOs are IT (66%), such as general-purpose workstations and servers. These devices exchange highly sensitive data such as patient health records and financial information. They also host Electronic Health Records (EHR) and Electronic Medical Records (EMR). From a threat perspective, these devices are the primary data store. That's where the Personal Health Information (PHI), payment information, and all the data required to generate patient bills are stored.

IT devices are the primary targets of ransomware gangs and data breaches. The HHS's HIPAA breach (https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf) portal shows that nearly 70% of data breaches in US healthcare in 2026 involved data stored on network servers. The figure below shows a redacted example of a healthcare dataset exfiltrated by the ransomware-as-a-service group, BQTlock, from a hospital in the US and shared on Telegram in April 2026.

April 3

BQTLock RaaS بقية

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
43	patient_id	id_mrn	full_name	first_name	last_name	date_of_birth	sex	ssn	address	phone	email	blood_type	insurance	insurance_primary	crossfunding	diagnoses	medication	last_visit	u
1	PT-100000	MRN-2539	Corey Will Corey	Williams	10/23/1951	M	214-83-0784	265 Sande	(702)938-1234	amara821@b-		Humana	POL-DX01	Westfield	Dr. Thomas	Rheumatoid	Tramadol	3/8/20	#####
2	PT-100000	MRN-4936	Michelle H Michelle	Huang	1/28/1952	F	397-79-2292	PSC 2944	912-392-0	nigginbar AB-		Aetna	POL-kg63	Cleanwater	Dr. Soles	Epilepsy	Atorvastatin	#####	#####
3	PT-100000	MRN-9777	Ronald B Ronald	Beardt	8/23/1913	M	824-31-2517	203 Jewell	599-249-0	donaldsher B-		UnitedHx	POL-KD57	Harbor Vie	Dr. William	Type 2 Dia	Sertraline	#####	#####
4	PT-100000	MRN-9111	Karen Ais Karen	Alexander	9/23/1967	F	626-91-4488	95423 Cra	949-513-0	mariewuzg B+		BlueCross	POL-4D3K	Metro East	Dr. Lowery	Atrial Fibril	Sertraline	#####	#####
5	PT-100000	MRN-6480	James Car James	Castillo	12/7/1959	M	279-84-0614	80865 Jam	929-665-4	jameswuzg A-		Humana	POL-pi77	St. Mary's	Dr. Connor	Atrial Fibril	Omegrazo	#####	#####
6	PT-100000	MRN-8651	Thomas R Thomas	Fleming	6/8/1949	M	215-63-6549	Unit 9471	(203)327-1	thomasj A+		BlueCross	POL-pi047	Cleanwater	Dr. Brown	Type 2 Dia	Pantopraz	#####	#####
7	PT-100000	MRN-0476	Andrew P Andrew	Pitts	10/26/2022	M	628-65-8755	560 Hump	+1-723-28	andrewmay O-		Centene	POL-UR45	Lakewood	Dr. West	Psoriasis	Abutrol	3/5/20	#####
8	PT-100000	MRN-6407	George C George	Curtis	10/17/2018	M	631-85-6750	97627 Ells	(987)946-4	joseph196 B+		Cigna	POL-qe99	Riverside	Dr. Estes	Chronic	Albuterol	2/8/20	#####
9	PT-100000	MRN-7379	Jessica A Jessica	Alvarado	12/8/2017	F	672-11-3014	988 Mills	P 743-505-2	jacksonjet A-		Centene	POL-JD35	Westfield	Dr. Hadson	Chronic	Glucoprofen	4/9/20	#####
10	PT-100000	MRN-6254	Stacie F Stacie	Fisher	2/8/1923	F	482-77-8125	820 Rivers	(358)991-0	keithbrown B-		Cigna	POL-ku331	Sanrise	Be Dr. Alexan	Hypothyroid	Sertraline	#####	#####
11	PT-100000	MRN-8325	David Jam David	James	9/19/1950	M	698-07-4252	527 Steele	+1-616-37	thomasj B-		Kaiser Pen	POL-IE07	Sanrise	Be Dr. Hall	Celiac	Dia Escitalop	#####	#####
12	PT-100000	MRN-5680	Crystal B Crystal	Baker	8/6/1965	F	632-06-0919	PSC 6943	3-066+09	rmann@gm B+		UnitedHx	POL-LV021	Sanrise	Be Dr. Harris	Iron Defici	Monteluk	#####	#####
13	PT-100000	MRN-6129	Adam S Adam	Scott	6/29/1953	M	408-33-3405	Unit 9583	-1525	smithadam B-		Cigna	POL-x1773	Riverside	Dr. Davis	Major Dep	Omegrazo	5/8/20	#####
14	PT-100000	MRN-1701	Jared Dan Jared	Davis	1/25/1925	M	746-85-3211	6928 Carr	(203)778-4	michael54 AB-		Cigna	POL-TU54	Cleanwater	Dr. Ball	Psoriasis	Meloprolo	#####	#####
15	PT-100000	MRN-8910	Bruce W Bruce	Woods	4/27/1924	M	040-24-9529	1267 Carr	(727)622-4	amy20@h AB-		Centene	POL-mQ01	Sanrise	Be Dr. Avery	Osteoarthritis	Bupropion	#####	#####
16	PT-100000	MRN-2380	Shaun R Shaun	Robinson	2/21/1922	M	484-92-7723	72307 May	+1-730-29	kochodyt B+		Humana	POL-JD57	Cleanwater	Dr. Davis	Hypothyroid	Gabapenti	6/4/20	#####
17	PT-100000	MRN-6043	Manuel C Manuel	Carter	2/5/2016	M	799-44-5454	4331 Chen	434-691	enderic38@ AB-		BlueCross	POL-TL658	Metro East	Dr. Harris	Hypothyroid	Sertraline	#####	#####
18	PT-100000	MRN-2705	Leslie W Leslie	Wilkins	6/21/1985	F	011-87-8556	5582 Simm	(445)630-0	chawakong O-		Centene	POL-pe48	Pine Valley	Dr. Hogan	Celiac	Dia Bupropion	#####	#####
19	PT-100000	MRN-7017	Alexandra A Alexandra	Flores	3/17/1977	F	146-11-5891	591 Marqu	254-776-6	klaraebor O+		BlueCross	POL-4Z307	Summit	Dr. Hall	Chronic	B. Lorazodine	#####	#####
20	PT-100000	MRN-2594	Anthony W Anthony	Williams	11/15/1960	M	604-58-0681	475 Edwar	521-653-0	stelecon B+		Molina Hx	POL-xU52	St. Mary's	Dr. Thomas	Chronic	Glucoprofen	#####	#####
21	PT-100000	MRN-1411	Lauren M Lauren	Meyden	3/3/1989	F	413-96-5162	540 Pengu	599-837	laurens@h O+		Kaiser Pen	POL-VP25	Sanrise	Be Dr. Perez	Asthma	Lorazodine	#####	#####
22	PT-100000	MRN-6706	Kyle E Kyle	Flores	2/22/1949	M	355-84-9984	USCOC Mi	481-226-3	jacqueline O+		BlueCross	POL-Am5C	Summit	Dr. Hanco	CERD	Act Lorazodine	#####	#####

Hospital usa 🇺🇸

hospital (Internet Site - before it went down)

hospital.net (internal facing nomenclature and used previously for business email)

5.355TB of files to include scripts, radiology, eKG, MRI, ultrasound, and blood work of 123,458 patients.

Also have emails, SonicWall access, and other information

1.35K 21:21

BQTLock RaaS بقية

hospital.sample.zip

114.4 MB

706 21:22

With the arrival of quantum threats, the same kind of data could be extracted from weakly encrypted network communications, without needing to compromise endpoints.

Network devices make up 11% of HDO devices and include routers, switches, firewalls and others that provide and manage connectivity for every type of asset on the network. Because they serve as traffic hubs for virtually all communications across the network, they uniquely provide access to large volumes of data moving through the environment. Routers directing network traffic between internal and external networks, such as the internet, VPN concentrators, and other choke points on the network handle much of the ingress and egress data. Currently, these devices are favored as initial access points (<https://www.forescout.com/research-labs/the-riskiest-devices-of-2026/>) by threat actors due to exploitable vulnerabilities. In the future, tapping these would allow threat actors to collect huge amounts of sensitive data, making them primary targets for HNDL attacks.

IoT and OT Devices

IoT and OT devices represent 18% of the risk surface in HDOs and are used for a wide array of functions from building automation to guest entertainment. These devices include the common VoIP phones and printers shown in the figure but also cafeteria and pharmacy point-of-sale systems, vending machines, ATMs, gift shop kiosks, physical security devices, smart building systems for energy and power management, HVAC, and backup generators. While these devices are not the primary concern when thinking about cryptographic risk in healthcare, some handle financial and other sensitive data – such as video conferencing systems.

These devices are often targeted by hackers when they are accessible online. Examples of real attacks, shown in the images below, include the pro-Russian hacker group Z-Pentest Alliance gaining control over – and tampering with – HVAC systems and IP cameras in Polish healthcare facilities.

We gained unauthorized access to the Geo-Eko BMS hospital ventilation control and management system in Poland, which services key areas of a medical facility.

The ventilation, temperature, humidity, and operating modes of the following critical areas are fully controlled:

- Surgical Unit (Chirurgia)
- Laryngology Department (Laryngologia)
- Vascular Surgery Department (Naczyniowa)
- Operating Room Unit (Blok Operacyjny)
- Sterile Clean Zone (Steryl. Czysta)
- Sterile Back Shoulder Zone (Steryl. Zaplecze)
- Sterile Dirty Zone (Steryl. Brudna)
- Emergency Department (SOR)
- Laboratory Complex (Laboratoria)
- Recovery Room (Sala Wybudzen)
- Operating Room Changing Room (Blok Oper. Szatnia)
- Cardiology Changing Room (Kardio Szatnia)
- Cardiology Intensive Care Unit (Kardio OIOM)
- Cardiology Department (Kardio Oddzial)
- Alarm Logging and Acknowledgment System

The interface allows for arbitrary changes to preset parameters for temperature, air handling unit performance, and humidity, as well as manual activation and deactivation of ventilation.

The consequences of such interference are obvious: compromised sterility in operating rooms, disruption of temperature and humidity control in intensive care and postoperative wards, and the creation of emergency situations with complete interruption of air exchange in areas with critically ill patients. Medical personnel have no visible means of detecting unauthorized control.

Authentication is absent. Action logging is not recorded at a level sufficient to prevent re-intrusion.

The system, designed to ensure security, has itself become a direct threat to the lives and health of patients.

Access granted. Full control confirmed.

22/04/26
13:14

BMS WENTYLACJA

WSTECZ

SERWIS

AWARIE

ORTOPEDIA

UROLOGIA

CHIR. OGOLNA

LARYNGOLOGICZNA

NACZYNIOWA

SWEGON NW13

TOMOGRAF NW14

SOR NW15

SOR NW16

LOGOWANIE

WYLOGUJ

ZALOGUJ

GEO-EKO

ALARMY

ALARM OGOLNY

SOR KNW1

PODGLAD

MENU

TEMPERATURA	WYDAJNOŚĆ	WILGOTNOŚĆ	TRYBY PRACY
NAWIEW 18.4 °C	NAWIEW 100 %	NAWIEW 0 °C	PRACA III
WYWIEW 25.5 °C	WYWIEW 100 %	WYWIEW 0 °C	PRACA III
ZEWNET. 16.4 °C		NAWILŻANIE 0 %	GRZANIE 0 %
ODZYSK 20.4 °C		OSUSZANIE 0 %	GRZANIE II 0 %
WODY 18.7 °C			CHŁODZENIE 0 %
			ODZYSK 46 %

ZADANA TEMP.

ZAD. WYDAJNOŚĆ

ZAD. WILGOTNOŚĆ

TRYBY PRACY

28.0 °C

I BIEG

II BIEG

90.0 %

STOP

START

III BIEG

We gained access to a laboratory's video surveillance system in Poland. The cameras showed us everything that goes on inside.

Here's what the video shows:

This is a BSL-2 cleanroom (or a cleanroom close to it).

- The main equipment is Thermo Scientific Class II Laminar Flow Cabinets. They glow blue—they're used for working with cell cultures, microorganisms, and biological samples to prevent contamination.
- Nearby are laboratory refrigerators and freezers (including Thermo models) for storing samples at low temperatures.
- Visible are sealed doors with windows, typical of cleanrooms, workbenches, chairs, centrifuges, and additional equipment for sterile work.

By all appearances, this is a molecular biology or microbiology lab—possibly a university lab, a research lab, or one associated with pharmaceuticals/medicine.

We see every room, every cabinet, and every movement inside. Your CCTV system has been compromised and we are now monitoring the site in real time.

#OpPoland 🇵🇵
#FuckEastwood 🇺🇸
#FuckRedCircus 🇵🇵
#FreeVictoriaDubranova ❤️

We are [The Z-Pentest Alliance](#) 🇵🇵

[t.me/zpentest_fucknato/1184](#) 14 👁 Мария, Apr 26 at 15:31



In most cases, these threat actors are not after data. They leverage control interfaces that either require no authentication or use default/weak credentials. In the future, sophisticated attackers with access to quantum computers could leverage quantum capabilities to decrypt strong credentials for these assets when they are communicated over the network.

Medical Devices

IoMT devices, used for patient monitoring and healthcare delivery, account for the remaining 5% of HDO assets. This gives a total of around 120,000 IoMT devices in our sample, an average of around 2,400 IoMT devices per HDO. These include connected medical devices in patient rooms, nurse stations, surgery centers, pharmacies, labs, and countless other locations. These devices may support clinical care, such as insulin pumps, heart defibrillators, ventilators, and any equipment saving or sustaining a life; or gather and monitor patient information such as vital signs and test results to alert and inform clinical staff. These include patient monitors, laboratory equipment, imaging devices, and more.

Again, these devices have been attacked by threat actors posting on Telegram how they can take control of exposed assets to intercept sensitive data or disrupt their functioning, such as in the examples below. Attackers usually describe how they can access patient databases with information such as full names and dates of birth; view, download or edit medical exams; and manage system settings.

Hello.

We have gained full and unrestricted access to the Visionix VX120 device used in an ophthalmology clinic in Madrid, Spain, for diagnostics and vision correction.

We can control the device, view, edit, export, and delete patient data, including client databases, medical histories, and all medical records.

We consciously decided not to interfere with the equipment's operation or cause harm to patients or the clinic.

However, we have demonstrated your vulnerability: deleting data and downloading the entire database for further use is effortless.

The administrator and operator have been warned about the potential consequences of negligence in information system security.

For additional information and contact information, we have invited them to visit our [Z-Pentest Alliance Telegram channel](#). This warning is not a threat, but a challenge.

Protect your patients' data from us and your reputation.

#FuckEastwood
#TimeOfRetribution
#OpSpain
#DesinformadorRuso

Sincerely,
Z-Pentest Alliance 
t.me/zpentest_fucknato/863

5 Мария, Apr 26 at 14:11



English translation:

Today we gained access in California to Philips CT medical equipment.

We are Z-ALLIANCE , and we managed to infiltrate the control of a modern Philips CT scanner used in medical institutions for performing computed tomography.

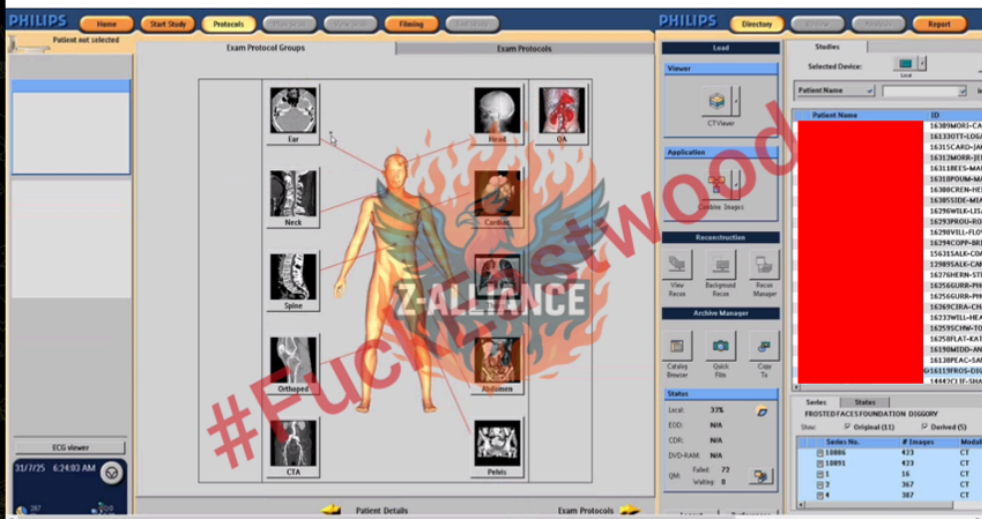
What we know and have access to:

- Full access to the patient database, including full names, dates of birth, weight, gender, language settings, and IDs
- Ability to create, edit, or delete patient records
- Control over patient positioning in the system (for example, decubitus — lateral position)
- Selection and modification of scanning protocols with choice of specific body parts: head, neck, spine, chest, abdomen, etc.
- Viewing, downloading, and editing of conducted studies and images, including the ability to change display and processing parameters of the scans.
- Access to the study archive, with sorting, searching, and series management features
- Ability to manage system settings, utilities, and equipment security parameters

Consequences and risks:

- Possible falsification of patient data and study results
- Potential interference with diagnostic protocols, posing a risk to patient health
- Threat of compromised confidential medical information
- Disruption of medical equipment functionality and diagnostic failures

Our intrusion highlights vulnerabilities in the cybersecurity of US medical systems.



Data at Risk

When discussing PQC migration in healthcare, it is not enough to discuss the types of devices that have to migrate their cryptographic implementations. HDOs must explicitly consider the heterogeneity of data types that these devices generate, transmit, store, and process.

HIPAA and other regulations mandate the use of appropriate administrative, physical, and technical safeguards for protected health information (PHI), including encryption where reasonable and appropriate. Clinical data such as electronic health records, imaging and lab results; operational data such as scheduled appointments; and real-time clinical data such as patient vital signs have distinct confidentiality, integrity, availability, and regulatory compliance requirements that directly influence cryptographic risk and migration urgency.

Long-lived, high-sensitivity data such as diagnostic images or patient records are prime candidates for HNDL attacks, while transient data streams such as session tokens may need to prioritize performance constraints over immediate cryptographic transition. Equally important, these data types are handled across a fragmented device landscape with different cryptographic capabilities, update mechanisms, and certification constraints.

Therefore, effective PQC migration requires mapping data classes to the specific device categories that generate, transmit, store, and process them, enabling risk-based prioritization and realistic deployment strategies aligned with both security requirements and operational limitations.

The table below lists several different data types in HDOs, their HIPAA category and common devices or systems that interact with this data. We will use this as a basis to understand what types of data in healthcare environments are most at risk today.

Data Type	Examples	HIPAA Category (Why?)	Common Devices / Systems Interacting with This Data
Patient Identifiers	Full name, date of birth, patient ID, national ID	PHI (Direct identifiers are explicitly listed in HIPAA)	EHR/EMR systems, registration kiosks, front-desk workstations, hospital information systems (HIS), identity management systems
Contact Information	Address, phone number, email	PHI (Identifies the individual and relates to healthcare services)	EHR systems, patient portals, appointment scheduling systems
Insurance & Payer Data	Insurance ID, policy number, coverage details	PHI (Payment-related health information under HIPAA)	Billing platforms, clearinghouse portals, claims processing servers
Financial & Payment Data	Credit/debit card number, bank details, billing history	PHI + PCI (Dual regulated: payment data linked to healthcare services is PHI also subject to PCI DSS)	Payment terminals (POS), billing systems, third-party payment gateways
Clinical Observations (Vitals)	Heart rate, blood pressure, oxygen levels, temperature	PHI (Individually identifiable health information)	Bedside monitors, wearable medical devices, nursing station dashboards
Diagnostic Data	Diagnoses, ICD codes, clinical assessments	PHI (Core “health information” under HIPAA)	EHRs, clinical decision support systems (CDSS), physician workstations
Medication & Prescription Data	Medication name, dosage, administration schedule	PHI (Medication history is explicitly protected health info)	Pharmacy information systems, medication

			dispensing systems, smart infusion pumps
Laboratory Results	Blood tests, pathology reports, microbiology results	PHI (Diagnostic health information tied to a patient)	Laboratory information systems (LIS), EHR interfaces, results portals
Medical Imaging Data	X-rays, CT scans, MRIs, ultrasound images	PHI (Images often contain identifiers and clinical data)	PACS systems, imaging modalities, radiology workstations, imaging servers
Physician & Clinician Identifiers	Physician name, NPI number, specialty, role	Not PHI alone because it identifies provider. Becomes PHI when linked to a patient encounter	EHRs, identity and access management (IAM) systems
Treatment & Procedure Records	Surgical notes, care plans, progress notes	PHI (documents diagnosis and treatment of an individual)	EHRs, physician workstations
Medical Device Telemetry	Alarms, Performance metrics, uptime, therapy settings	Not PHI alone, may become PHI when tied to a patient (e.g., therapy settings)	Several IoMT devices and device gateways
Remote Patient Monitoring Data	Glucose levels, ECG data, vitals	PHI (Individually identifiable health data)	Wearables, home monitoring devices, mobile health apps, cloud monitoring platforms
Research & Clinical Trial Data (de-identified)	De-identified patient data, outcomes. Stripped of HIPAA's 18 identifiers	Not PHI (Meets HIPAA de-identification standard)	Clinical data warehouses, research databases, analytics platforms
Operational & Scheduling Data	Appointment schedules, bed availability	PHI, if patient-linked. Not PHI, if not linked.	Scheduling systems, bed management systems, hospital operations dashboards
Public Health & Reporting Data	Disease reporting, vaccination records	PHI (permitted disclosure for public health purposes)	EHR reporting modules, public health interfaces, government reporting gateways

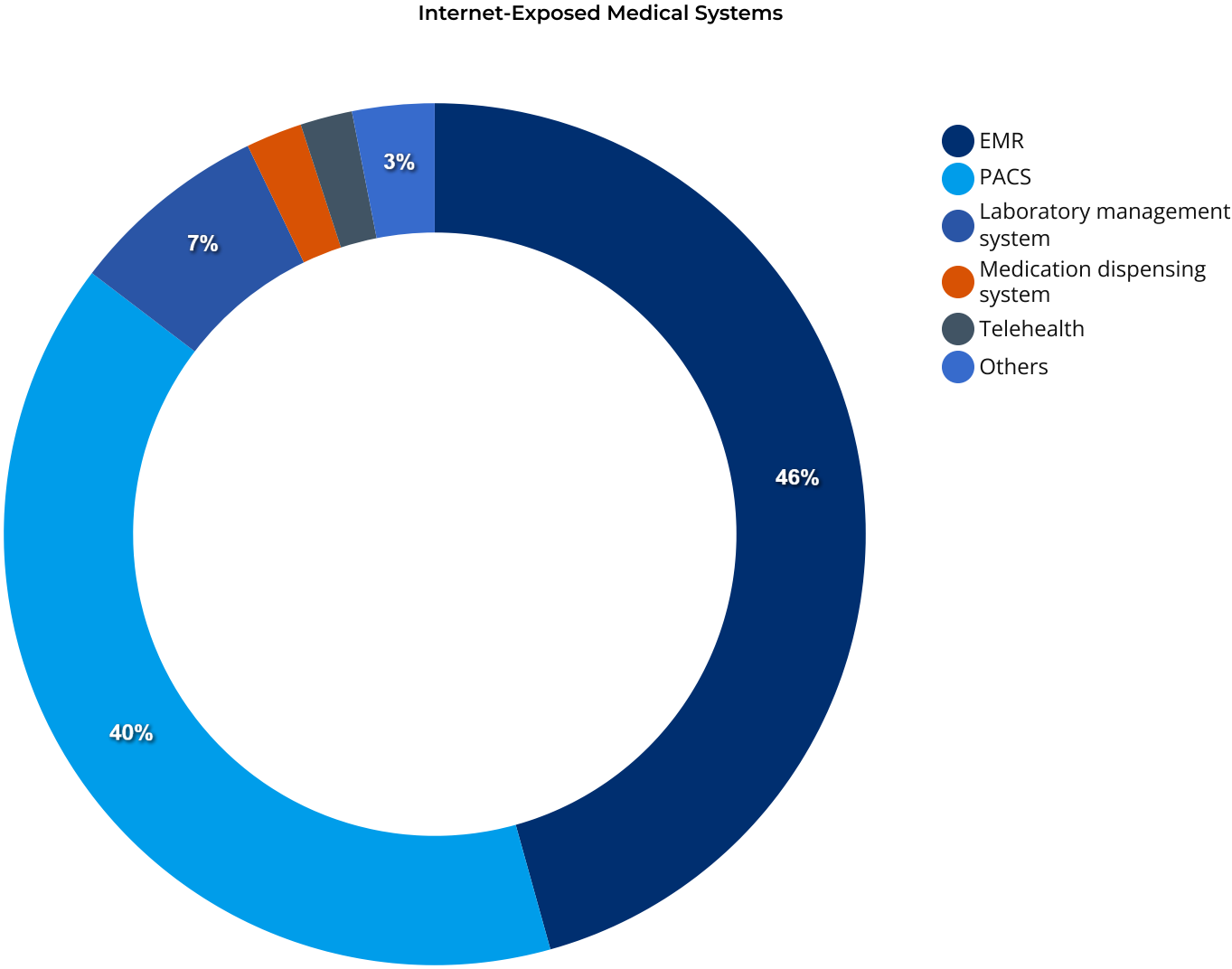
The biggest quantum risk in healthcare is data traversing public networks, so beyond common assets and data types we need to understand what kind of healthcare systems are usually accessible online.

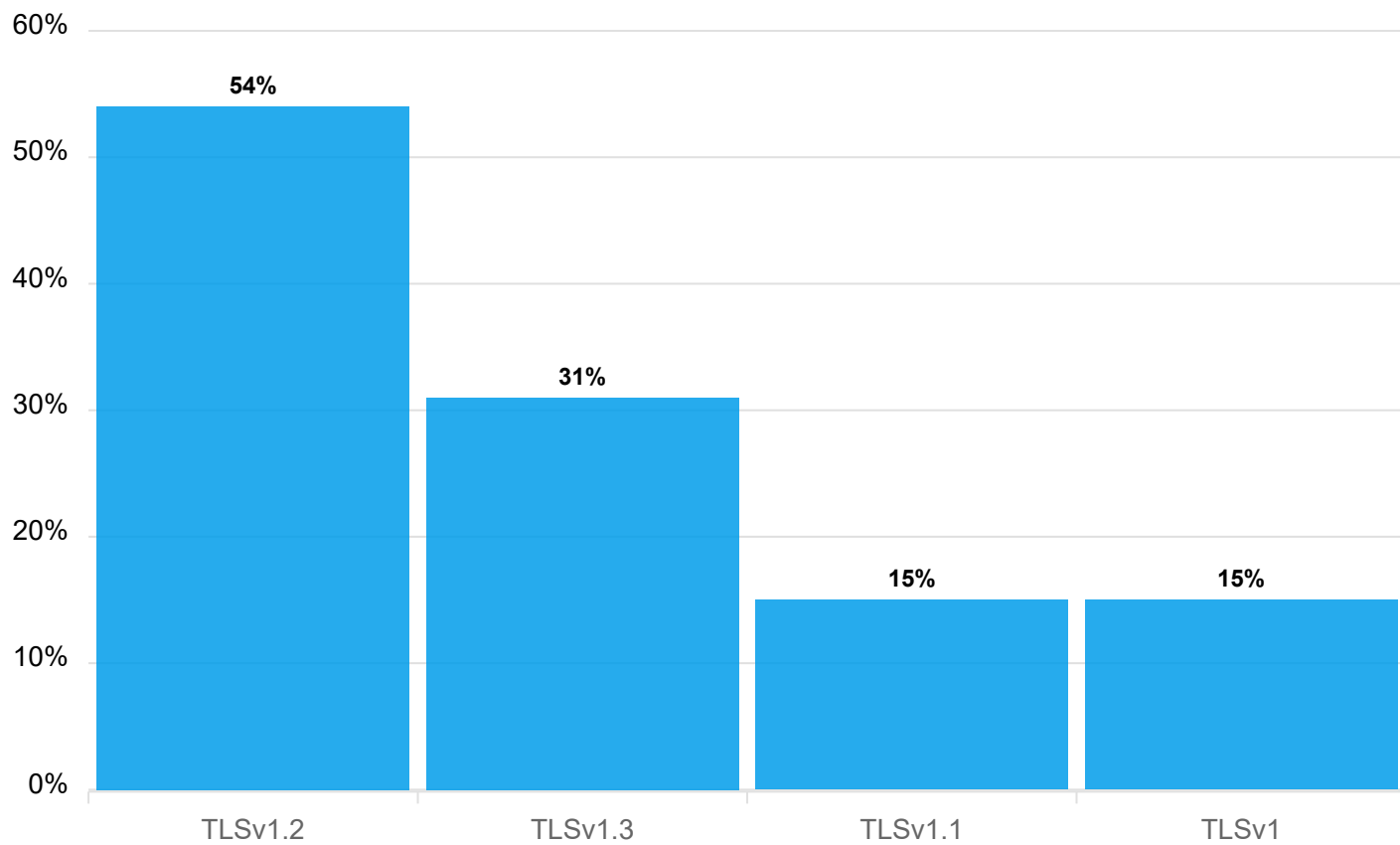
Medical devices are rarely connected directly to the internet, but they often communicate with information systems that are exposed. For instance, imaging modalities such as CT scanners communicate with picture archiving and communication systems (PACS), which in turn communicate with radiology information systems (RIS). Although CT scanners are not commonly found online, many PACS and some RIS are and thus may provide a path for attackers to access sensitive data from CT scanners.

Using a series of specific network fingerprints (<https://github.com/woj-ciech/Kamerka-GUI/blob/master/queries.md>) of medical systems (openly accessible to anyone, including attackers), we queried the Shodan (<https://www.shodan.io/>) search engine and found a total of over 5,500 instances of 50 different medical information systems exposed. As the figure below shows, the vast majority of these were either EMR (46%), storing medical records, or PACS (40%), storing medical images. Laboratory management systems, storing exam results, and medication dispensing systems, storing information about prescribed drugs are also among the most exposed.

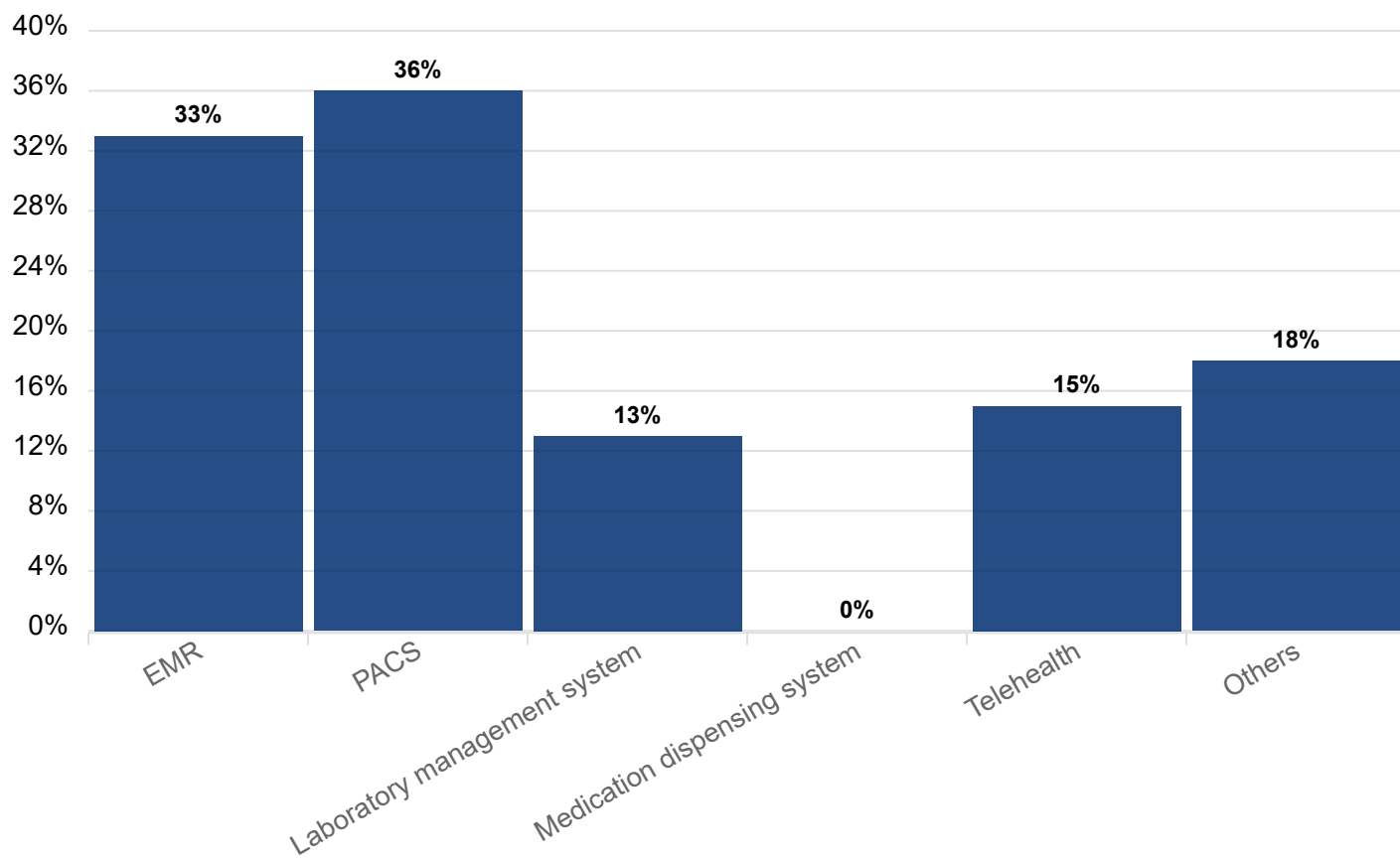
Vulnerable PACS systems – those lacking proper authentication and encryption – are a persistent risk (<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-hidden-vulnerability-in-healthcare-exposed-dicom-servers-and-the-risk-to-patient-data>) and we have explored real attacks targeting data from those systems in previous research (<https://www.forescout.com/research-labs/risk-of-connected-medical-devices/>) . Here, we draw attention to the fact that even for those PACS that use encryption, only 36% use TLSv1.3, the only version that supports PQC. The situation is similar for EMR (33% using TLSv1.3) and worse for laboratory management systems (13%) and others.

Across every type of exposed medical system, the average percentage of TLSv1.3 deployments is 31%. Even worse, 15% of systems still support TLSv1 or TLSv1.1, which are officially deprecated (<https://datatracker.ietf.org/doc/rfc8996/>) and disabled in modern browsers, due to lack of support for modern cryptographic algorithms, even before PQC.





Percentage of TLSv1.3 Deployments Across Internet-Exposed Medical Systems



Prioritizing Risk

Healthcare data most at risk for quantum attacks is that which:

- Is commonly transported over TLS or other cryptographic protocols using quantum-unsafe RSA or elliptic curve cryptography (ECC) for authentication and key establishment today
- Has long confidentiality lifetime, making HNDL attacks relevant
- Is likely to be recorded or intercepted when traversing external networks, including the internet, partner links, remote access solutions, cloud applications and others

This definition excludes some data types from Table 1, such as short-lived transactions that have low value once clinical context expires (e.g., the medical device telemetry), and information communicated over unencrypted legacy protocols, such as HL7v2, POCT01, LIS and others. The latter is already a confidentiality and integrity risk today, not a future one. However, this kind of traffic is usually limited to internal networks. See our previous research (<https://www.forescout.com/connected-medical-device-security-report/>) for examples of attacks leveraging unencrypted data in healthcare networks.

Combining the three datasets above – common assets, data and exposure in healthcare systems – with this definition of quantum risk, Table 2 shows the five data types currently most at risk for quantum attacks in HDOs:

#	Data Type	Why Is It Risky?
1	EHR / EMR	EHRs/EMRs often include complete clinical histories with patient identifiers, diagnoses, medication, lab results, appointment scheduling and other information. The data is presented on Internet-facing patient portals and communicated via APIs on Health Information Exchange (HIE) systems transporting it over TLS. Traffic traverses many boundaries, is easy to harvest on public networks and highly valuable long term.
2	Medical Imaging	Medical images contain metadata with lifelong sensitivity. They can be used for extortion (patient shaming) and are routinely included in cybercriminal data leak samples. This type of large volume data is often transferred across sites (e.g., replicated to clouds and teleradiology providers) using the DICOM protocol, which is by now well-known to attackers, and stored or accessed via PACS.

3	Laboratory Results	Laboratory results are commonly communicated across different institutions because reference laboratories perform complex, specialized or high-volume diagnostic testing that local HDOs cannot do. This includes not only clinical and commercial labs but also public health systems that investigate outbreaks or rare diseases. Lab results may contain very sensitive data such as biomarkers for HIV, cancer and other diseases, toxicology or drug screening results and genetic data.
4	Medication & Prescription Data	Medication data including medication history and use of controlled substances is not only generated and stored internally in HDOs, but also communicated via electronic prescribing (eRx) systems. These systems facilitate prescription, insurance verification and medication messaging between healthcare providers and retail pharmacies, so the data can traverse public networks and is particularly sensitive in cases of addiction or chronic diseases.
5	Financial/Payment Data	Not healthcare-specific but valuable data for attackers for immediate monetization. Can be captured when on-site PoS or billing systems communicate with external payment processor gateways or when patients enter financial information in patient portals and other systems.

Recommendations

Healthcare organizations and patients alike should not treat quantum risk and PQC migration as distant theoretical issues. The ingredients for quantum exposure already exist today: large volumes of long-lived, high-value data; widespread dependence on protocol implementations that are not yet PQC-capable; and thousands of internet-exposed healthcare systems that store or transport some of the sector's most sensitive information. In practice, the greatest near-term concern is not that quantum attacks are already happening – since cryptographically relevant quantum computers are not yet available – but that adversaries can harvest encrypted healthcare traffic now and retain it until quantum decryption becomes feasible.

This report elucidates how this risk is unevenly distributed. Traditional IT systems still hold the bulk of patient and business data and remain the most likely targets for ransomware, data theft, and future attacks. However, network infrastructure, internet-facing medical information systems, and specialized devices are also critical because they move, expose, or mediate access to sensitive data and are slower to migrate to PQC. The data most at risk today is that which is both easy to intercept and valuable for years: EHR and EMR records, medical imaging, laboratory results, medication data, and financial information. These are precisely the datasets that cross organizational boundaries, traverse public networks, and often depend on cryptographic stacks that will be slow to migrate.

To be able to migrate their assets before quantum attacks become feasible, HDOs need to first inventory their systems, identify choke points such as partner interconnections and internet edge devices, understand which support PQC or not, assess the risks they are exposed to and what can be done to mitigate these risks.

The main operational constraint for the migration is crypto-agility. Where organizations control the TLS or VPN termination points and software stacks, migration can move relatively quickly. In other cases, it's a much bigger challenge. High-agility environments include IT systems under direct administrative control. Medium-agility environments involve shared ownership, such as partner-managed endpoints and vendor appliances. Low-agility environments include legacy proprietary systems, regulated medical devices, and gateways where cryptographic changes depend on vendor release cycles, recertification, or even hardware replacement.

This is why healthcare PQC planning cannot be reduced to a device or protocol checklist. It requires understanding which assets can be easily upgraded, which cannot, and what sensitive data each one protects. Below is a list of actions that HDOs can take in the upcoming months to prepare for this migration and ensure they will be well-positioned once either this becomes mandated or quantum attacks become practical:

Next 6-12 Months

- Use this report as an example to map your own terrain, identify common assets, data types, internet exposure and risk in your networks.
- Prioritize internet-exposed connections, such as patient portals, external-facing APIs, VPN gateways, and inter-organization data exchange.
- Enforce TLSv1.3 wherever possible.
- Update internal governance and risk frameworks by integrating PQC into threat models and aligning with transition guidance (<https://csrc.nist.gov/pubs/ir/8547/ipd>).
- Define PQC KPIs, such as percentage of assets that are PQC-capable or number of flows with sensitive data that are quantum-safe.
- Identify which assets can or cannot be updated to support PQC and plan their updates.

2-24 Months

- Update crypto libraries/applications, such as OpenSSL or OpenSSH, and device firmware where possible to support PQC.
- Segment and isolate legacy systems that cannot be updated.
- Plan for PQC gateways and secure remote access (SRA) solutions in front of legacy systems and network segments that cannot be updated.
- Engage vendors to understand PQC roadmaps for those that have not yet offered alternatives.
- Consider including PQC requirements or clear roadmaps into procurement decisions and contract renewals.
- Start measuring the PQC KPIs defined previously.

24+ Months

- Continuously measure the PQC KPIs against objectives in each identified network segment.
 - Consider replacing those assets that have no clear roadmap for the migration.
 - Identify further risk mitigation measures for those network segments considered risky containing assets without vendor-provided migration roadmaps and that cannot be replaced.
-

Stay on top of the latest threats. Sign up for the Vedere Labs Threat Feed (<https://forescout.vederelabs.com/register>) and get the full context in our monthly newsletter (<https://www.forescout.com/research-labs/#newslettersignup>) .
