

A GUIDE BY PATIENTS, FOR PATIENTS

Cyber Safety Is Patient Safety

Protect your care, your accounts and your community, with practical steps patients can take today.

- | | | | |
|---|---|--------------------------------------|---------------------------------------|
| 01
Prepare for hospital
downtime | 02
Lock down your accounts | 03
Use AI with care | 04
Speak up together |
|---|---|--------------------------------------|---------------------------------------|



This guide is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). Share and adapt it freely with credit to The Light Collective and the Health Sector Coordinating Council Cybersecurity Working Group. creativecommons.org/licenses/by/4.0



Shining a light on actions you can take

Headlines about hospital hacks and AI scams can feel like a storm with no shelter. This guide gives you the facts and the habits that have evidence behind them.



When a hospital loses its computers, care slows down and patients are harmed.¹ When a patient group loses its page, years of support can vanish. When a chatbot confidently gives a wrong answer, decisions get made on it, and the consequences can be serious.

Each of these is a place where cyber risk meets patient safety. Patients wrote this guide to map those places: how digital harm reaches people, what we can do today to prepare, and what we can ask of the hospitals, platforms and companies we rely on.



Start wherever is most useful to you. If you have ten minutes, page 6 is a good first stop.

Before you begin

Resilience starts with understanding. Cyber risk and patient safety now meet in the same places: the portal, the pharmacy app, the support group, the chatbot. Understanding how digital harm happens opens up solutions to prevent it, catch it early and recover faster. Hospitals, platforms and technology companies carry their share of that work; this guide covers ours.

What this guide covers



ACTION 1 | PAGE 6

Prepare for hospital downtime

Keep your own copy of records, medicines and key phone numbers, so care keeps moving when a hospital's computers go down.



ACTION 2 | PAGE 7

Lock down your accounts

Add a second lock (two-factor authentication) to your email and social media, so one stolen password cannot take over your account or your group.



ACTION 3 | PAGE 9

Use AI with care

Remove what identifies you (your name, your hospital, a rare biomarker) before you upload, check what comes back, and use AI to prepare questions rather than to make the final call.



ACTION 4 | PAGE 10

Speak up together

Report scams and harm, ask hospitals and apps hard questions, and expect them to do their part.

Also in this guide

- 3** Why cyber self-care matters
- 4** Cybersecurity, patient safety and health privacy
- 5** How cyberattacks harm patients
- 6 to 10** The four actions, one page each

- 8** Case study: a stolen cancer support page
- 11** Your cyber safety checklist
- 12** Learn more: the research behind this guide
- 13 to 14** Glossary, acknowledgments and sources

Why cyber self-care matters

Our health now lives online. This guide helps patients and caregivers protect it, without fear and without going it alone.



Patients already practice self-care. We track medications, prepare questions for appointments, learn our conditions and lean on each other in support groups.

More and more of that care now runs through technology: patient portals, pharmacy apps, online communities and AI chatbots. When those systems are attacked, misused or simply get things wrong, patients feel it first. Hospitals go offline, support groups get hijacked, and chatbots give confident answers that may not be right.

Headlines about these events often spread fear and misinformation. We wrote this guide to shine a light on good information instead: what the evidence shows, what patients can do, and what we should expect from the institutions that hold our data.



What is cyber self-care?

Cyber self-care means the everyday habits patients use to protect their health information, accounts and care when technology fails or is misused. In plain terms, it is a backup plan for your digital health life. It sits alongside the self-care many of us already practice, and it works best when we do it together.

Who this guide is for

Patients, caregivers, patient organizations, and the leaders and moderators of patient communities online.

How to use it

Read it in any order. Each action page stands on its own. Page 11 is a checklist of the steps outlined in the guide; page 13 has a glossary of terms.

How we wrote it

We drew on published research, government guidance and lived experience. Every claim was vetted, and every fact links to a public source you can check.



Written by patients, for patients. This guide was a collaboration between patient organizations, patient advocates, and experts in cybersecurity. Patients set the questions, reviewed every page and tested it with people in their communities. Experts helped us get the facts right.

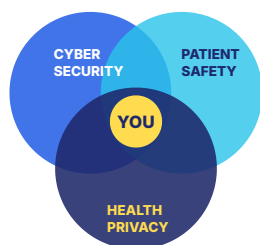
Cybersecurity, patient safety and health privacy: how they differ

Each can fail on its own. Knowing which one failed tells you what to do and who to call.



Patient safety means the absence of preventable harm to a patient, in the World Health Organization's words. About 1 in 10 patients is harmed while receiving care, and more than half of that harm is preventable.² Cybersecurity and health privacy are separate problems that can each lead to that harm, so this guide covers all three.³

	Patient safety	Cybersecurity	Health privacy
What it covers	Keeping care from hurting you: wrong medicines, missed diagnoses, surgical errors, infections	Protecting computers and data from people who break in, steal, lock or disrupt them on purpose	Your right to decide who sees, uses and shares health data that identifies you
Key question	<i>Could this care harm me, or put me in harm's way?</i>	<i>Is someone breaking in, tampering or shutting systems down?</i>	<i>What legal rights do I have if my data are shared without my consent?</i>
Example	A misdiagnosis or wrong test result caused by a medical error in an online system	Hackers lock a hospital's systems, cutting off access to patient care and causing downtime	A hospital website sends appointment details to an advertising tracker ⁴
Your action	Keep your own copy of your medication list, and look up your hospital's safety record at leapfroggroup.org ⁵	Add a second lock to your accounts and pause before you click	Ask who sees your data, keep identifiers out of chatbots, and use your HIPAA rights (page 10)



Patient safety, cybersecurity, health privacy: examples of where they meet

Each word names its own failure, with its own place to report it (page 11). In real life they arrive together, and one failure sets off the next: a locked computer becomes a missed dose. Six examples from reported cases.

CYBERSECURITY MEETS PATIENT SAFETY

Ransomware locks a hospital's lab system. Nothing is stolen, but a heart attack blood test that should take an hour takes four, and treatment has to be delayed.¹

CYBERSECURITY MEETS SAFETY AT HOME

An attack takes down a clinic's prescribing system and refills stall. One patient with asthma wrote online that "breathing burns" as the medicine ran out.¹

CYBERSECURITY MEETS HEALTH PRIVACY

Attackers steal a health system's records and post them on the dark web, including intimate images of patients with breast cancer.¹

HEALTH PRIVACY MEETS PATIENT SAFETY

A data broker sells a list of people with depression or PTSD, names and addresses included. That list can cost someone coverage, a job or their safety.⁶

PRIVACY FAILS WITH NO HACK AT ALL

Every password holds, yet a hospital website sends your appointment details to an advertiser.⁴ Some patients skip the clinic rather than risk a leak.¹

ALL THREE AT ONCE

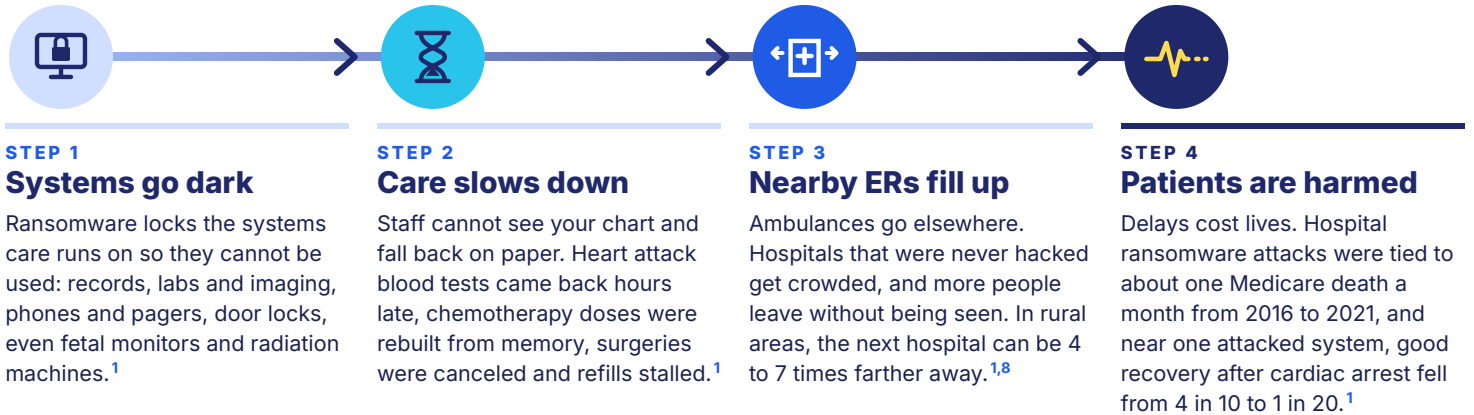
A hacker takes over a rare brain cancer support page. Thirteen years of parents' posts sit in a stranger's hands, and 19,000 people lose their meeting place (page 8).⁷

How cyberattacks harm patients

Attacks on hospitals have shifted from stealing data to shutting down care on purpose. Researchers now call them threat-to-life crimes, and the harm reaches patients' bodies.

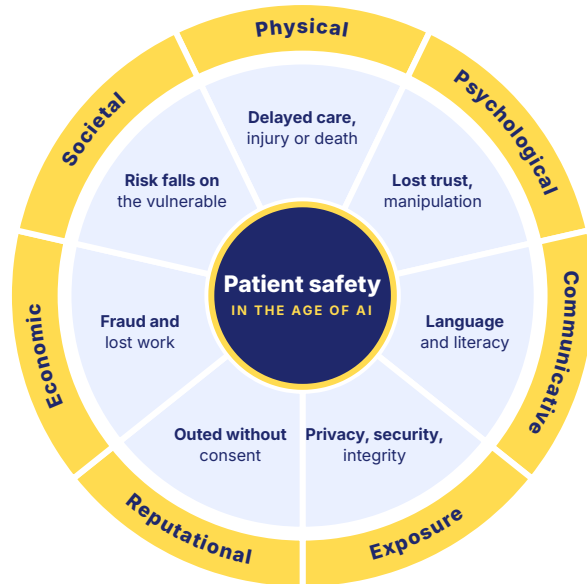


A 2026 review of 59 studies from 13 countries, plus posts by patients and staff in 3,408 online health communities, documented **316 harms to patients** from hospital cyberattacks.¹ Here is how an attack travels from a locked computer to the bedside.



Examples of cyber harm

Patient safety is more than medical error. A breach, a data sale or a misleading chatbot can hurt patients even when no clinician makes a mistake.^{9,10}



Physical	Injury or death from delayed care, misdiagnosis, or loss of access to critical care in an acute or emergency situation.
Psychological	Loss of trust after a breach; being targeted, manipulated or influenced based on leaked data.
Communicative	Consent forms written above a patient's reading level; AI summaries that distort clinical meaning.
Exposure	Health data shared with trackers and brokers outside HIPAA; records altered so care rests on false information.
Reputational	Being outed without consent in a way that causes discrimination, lost opportunities or worse.
Economic	Medical identity theft puts someone else's care on your bill; recovery costs time off and legal help.
Societal	Fake patient bots and scams hijack support communities; lost trust keeps people from care and trials.

A breach is a **security** failure. A lawful sale of your data is a **privacy** failure. To a patient, both are **safety** failures.

Page 6 shows the steps you can take. Studies and examples: page 12.

Build your downtime kit now

Downtime means a hospital's computers are offline. Staff work from paper and phones and may not be able to see your chart. Your own copies help keep your care moving.



Actions you can take for hospital downtime

1 Download your records now

Every MyChart portal has a share or download option: request a formal copy (a PDF) or a computer-readable copy that other apps can read.¹¹ Do the same for older portals and records from past doctors. HIPAA gives you the right to a copy of your own data, in the form you ask for, usually within 30 days.^{12,13}

2 Keep your own medication list

List each medicine, dose and how often you take it, plus diagnoses, allergies and medical devices, in a notes app or your portal app.¹⁴ During downtime, staff may not be able to see your chart, and researchers found allergies and medication histories in particular were missing. If this happens to you, show your list.¹

3 Save the records that guide your care

Recent lab results, imaging reports, care plans and visit summaries. Save them in a password-protected, encrypted file on a device you control, with a second copy in a backup you trust, so one lost phone does not mean losing everything.¹⁵

4 Save your key phone numbers

Care team, pharmacy, a backup pharmacy and your insurer, in your contacts. Patients in attacked systems reported stalled refills and no way to reach their clinic.¹ When portals go dark, phone calls usually still work.¹⁵

5 Ask your care team one question

"If your computer systems go down, how do I reach you, get refills and get test results?" Save the answer with your list.

6 Lock your copies

A passcode protects your phone, not a file copied onto a laptop. Turn on your computer's built-in encryption (FileVault on a Mac, Device encryption or BitLocker on Windows), and keep records in a password-protected, encrypted file or folder.

Get your records with FHIR

FHIR (say "fire") is the common format U.S. patient portals offer, by federal rule, so an app you choose can pull your records. You sign in and pick what to share.¹⁶

Once data leaves your portal, HIPAA generally no longer covers it, so the app you choose matters. We recommend open-source tools that run on your own computer.

One example: **MyChart Takeout**, a free, secure, open-source tool that exports your full MyChart record in your browser, so your data never leaves your machine. Its author, Josh Mandel, MD, is a physician and developer who led the SMART on FHIR standard.¹⁷

After a breach letter arrives

Keep the letter. It is evidence if you report harm (page 11). Stolen data often fuels scams later, so three habits help.

Hang up and call back. If someone calls about a bill or your records, end the call and dial the number you already know.¹⁸

Read every benefits statement. Look for care you never received or medical bills you do not recognize.¹⁹

Freeze your credit. A freeze is free to place and lift; contact all three credit bureaus.²⁰

Three layers of backup

Your device, a second copy and a person. One will still work when the others do not.

On your device

Your medication list and records in a password-protected, encrypted file on a phone or computer locked with a passcode.

A second copy

An encrypted cloud backup or a second device, so one lost phone does not mean losing everything.

A person who knows

A caregiver or family member who knows where your copies live and can speak for you.

Keep your online accounts in your own hands

Social media, email and other online accounts hold our stories, contacts and health details. Learn how attacks unfold and how to keep control.



Online harm to patients often starts far from any hospital and ends with **money, medical identities and communities stolen**.



Privacy can be lost without a hack

A secure company can still share your health information in ways you did not choose. Top hospital websites once sent appointment details to Facebook through a tracking tool.⁴ Strong passwords only protect your logins and cannot stop tracking tools that send data. If you learn this has happened, speaking up (page 10) matters.

Actions you can take for your accounts

- 1 Lock down your email first**
Your email resets every other password, so it works like a master key. Give it the strongest protection.²⁴
- 2 Use a password manager**
Give every account its own strong password and let a password manager remember them. Your phone's built-in one, such as Apple Passwords or Google Password Manager, works well.²⁵
- 3 Add a second lock**
Turn on two-factor authentication. An authenticator app is good; a physical security key is the strongest option. Save your backup codes and bookmark each platform's recovery page.^{25,26}
- 4 Check who has access**
Review where you are logged in and which apps connect to your accounts. Log out of anything you do not recognize and turn on login alerts.
- 5 Pause before you click**
Urgent warnings that your account will be deleted are a common trick. Open the app or type the address yourself instead of clicking a link in a text message or email.^{18,27}
- 6 Use TLC's Online Safety Toolkit**
Step-by-step guides for social media accounts and patient groups, plus more on two-factor tools and options, at lightcollective.org/safety-toolkit.²⁴

Run a patient group?

Keep one stolen login from ending a community. A real case is on the next page.

Make your group resilient: add a second trusted admin.

Each admin has their own login, so one hack cannot end the group.

Require a second lock. Every admin turns on two-factor authentication.

Review the admin list often. TLC's moderation resources can help.²⁸

Case study: How a cancer support page was stolen

A real account takeover, step by step, and what to do in the first hour if it happens to you.



KENTWOOD, MICHIGAN | OCTOBER 2023

13 years of support, gone in a weekend

A mother had run a Facebook page about her daughter's rare brain cancer since 2011. More than 19,000 people followed it, and she used it to talk with parents around the world about treatment.

One weekend a hacker took over her personal Facebook account and, with it, the support page. She could no longer log in.⁷

"I was crying because... literally it was like 13 years, gone."

Page founder, October 2023⁷

Meta did not respond to her requests or to reporters' questions.⁷

19,000+

followers cut off

13 yrs

of posts and connections

How online accounts get hacked

Reports did not say how this page was taken. Many takeovers follow these steps.

- 1 An urgent warning or request arrives.** It may be an email, text or direct message claiming to be from a platform, a bank or someone you know. It often comes from an address or account that is not official, and it pushes you to act fast, such as appealing within 24 hours before your page is deleted.^{18,27}
- 2 A link asks you to sign in.** It opens a page that looks real and asks for your password and login code. Some fake pages also ask for photos of your ID.²⁹
- 3 Scammers sign in and change the locks.** With your password and code, they log in and change your password, email and two-factor settings so you cannot get back in.
- 4 Friends and group members become targets.** Scammers use the account to send scams to everyone who trusts it, or they sell it. In one Canadian case, friends of a hacked user lost about \$2,500 to fake listings.³⁰ Guardio Labs, a security research team, tied one 2026 campaign to about 30,000 stolen Facebook accounts.²⁹
- 5 Getting your account back can take days, or never happen.** Recovery often means rounds of identity checks with the platform, and the founder in this case was still locked out when her story was reported.^{7,30}

Reduce the risk before it happens

Second lock on. Two-factor authentication with an authenticator app on email and every social account.

Open the app yourself. Check any warning inside the app itself rather than through the link in a message.

Make your group resilient: add a second trusted admin. Each with their own login and a second lock, so one stolen account does not end the group.

If it happens to you: act in the first hour



Secure your email first. Change its password and turn on two-factor authentication, because email controls every reset.

Warn your members. Use a co-admin, another group or a text to say: do not click links or send money from the hacked account.

Start official recovery. Go to your platform's recovery page, such as facebook.com/hacked, from your own browser.²⁶

Report it. Report phishing at ReportFraud.ftc.gov; if anyone lost money, file at ic3.gov.^{18,31}

Patients and physicians using AI

Weighing benefits and risks. AI can help you prepare questions and understand your care, and your doctor may be using it too. Here is how to make it work for you.



More and more, patients use AI to ask for health advice, especially when we cannot get the care we need.

Your doctor may be using AI too. Ambient scribes record the visit and draft the visit notes. You should be told before a visit is recorded, asked for consent, and able to decline with no effect on your care. Ask who stores the recording and when it is deleted.^{32,33}

1 in 3

U.S. adults used an AI chatbot for health advice in the past year.³⁴

77%

are concerned about the privacy of medical information shared with AI tools.³⁴

41%

of those who used AI to ask a health question uploaded their own medical records to do it.³⁴

2 in 3

U.S. hospitals on the largest records system had adopted an AI scribe by mid-2025.³⁵

Where the risks come in



RISK 1

Uploading sensitive health information

Consumer chatbots are not covered by HIPAA, the federal law that protects records held by your doctor; it covers only tools your doctor, hospital or insurer provides. A company can keep and reuse what you share.³⁶



RISK 2

Not all chatbots are equal

Stanford's MedHELM project tests AI models on 121 medical tasks; they did best at writing notes and explaining care, worse at clinical decisions.³⁷ AI can sound sure while wrong, and tend to agree with you.³⁸



RISK 3

Who else uses AI

Scammers use the same tools to make fraud cheaper and more convincing. In 2025 the FBI logged more than 22,000 AI-related complaints and about \$893 million lost.²³ Fake AI apps steal login codes.^{39,40}

COMPARED WITH WHAT?

Weigh AI against the care we can reach

Isaac Kohane, a physician and clinical AI scientist at Harvard, argues AI should be measured against the care patients actually get, rather than an ideal system.⁴¹

The health care we have

795,000 Americans die or are permanently disabled each year because a dangerous disease was misdiagnosed.⁴²

24+ hours waiting in the ER for a bed, reported by 97% of 140+ emergency physicians surveyed by their national college.⁴³

The AI we have

#1 health technology hazard of 2026, says ECRI, an independent patient safety nonprofit: chatbots have "suggested incorrect diagnoses."⁴⁴

7 in 10 health chats happen outside clinic hours, one AI company reports.⁴⁵

Experts do not yet agree on which uses of AI are safe and protect our privacy and security. Patients deserve AI that is tested, honest about its limits and accountable for harm. More reading on page 12.⁴⁶

Actions you can take for AI safety

1

Remove what identifies you before you upload

Before you load a record into a chatbot or type a question, take out your full name, birth date, address, medical record or insurance numbers, and ultra-rare disease details that are not needed.⁴⁷

3

Go in prepared

Use AI to prepare questions and understand terms. For an answer that could change a health decision, check a second source or ask your health care provider.⁴⁷

5

Get AI apps from the official source

Fake AI apps copy real ones and steal login codes. Download only from the developer's site or the official app store.⁴⁰

2

Check your settings and read the fine print

Turn off training on your chats and keep them out of shared links. Then read the privacy policy: can the company keep, train on, share or sell your health information?¹⁶

4

Ask the tool to show its uncertainty

Describe what you have noticed, then ask it to weigh other explanations and say how sure it is.

6

Ask your doctor about their AI tools

Which AI tools touch your care, and can you see what they produced if there is an error? You can decline a scribe with no effect on your care.^{32,33}

Advocate for our digital selves

Our records, chats, posts and support groups make up a digital self that deserves protection too.



Much of the harm from cyberattacks is hard to see because it goes unreported. Harm is usually logged through the same hospital systems an attack shuts down.¹ Patients hold the other half of the picture.

The fallout often lands outside the hospital: a refill that stalls at the pharmacy, a breach letter followed by scam calls, a support group that disappears overnight. Those harms reach the medical community only when patients report them. Your reports help hospitals, regulators and researchers see what an attack costs and prevent the next one.

Actions you can take together

1 Use your rights

Ask for copies of your records and fix mistakes in them.¹² If a hospital or insurer fails to protect your health information, you can file a complaint with HHS's Office for Civil Rights.⁴⁸

2 Report what you see

Report scams at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov) and forward scam texts to 7726.^{18,49} Reports become the evidence regulators and researchers use.

3 Ask questions that hold institutions accountable

Who is accountable when a digital tool causes harm? How can patients challenge a decision or report a concern? Will you tell us what changed because we spoke up?

4 Protect your community

Share this guide, help your group's admins turn on two-factor authentication, and set clear rules for posting links.²⁸

5 Act together

Ask for patient representatives with meaningful decision-making authority, compensation for their expertise, and a clear process for showing how patient concerns change policies and products.⁵⁰ AI tools reflect the choices of the people who build them, so patients belong in the room when those choices get made.⁵¹

What you should expect from institutions

Cyber self-care does not shift the job of safety onto patients. Hospitals, platforms and technology companies still have to do their part.

Social platforms

Strong account security by default and fast, human help when a patient group is hijacked.

Apps and AI companies

Clear limits on what a tool can do, no ads or AI training on health data without consent, and a way to report harm.

All of them

Accountability when a digital tool causes harm, and a report back on what changed because patients spoke up.



PROOF IT WORKS

Patients turned a download button into evidence

Advocates downloaded their own Facebook data to see which health companies tracked them, and published a peer-reviewed study.⁵² The Markup, a nonprofit newsroom, then found a third of top U.S. hospitals sending patient information to Facebook,⁴ and hospitals began removing those trackers.

Your cyber safety checklist

Check off one step a week. You do not have to do them all at once.



This week I will

1 Prepare for hospital downtime

Do this before an attack, not after

- ☐ Download my records from each patient portal
- ☐ Keep a current list of my medicines, doses, allergies and conditions on my phone
- ☐ Save recent labs, imaging and care plans to a device I control, with a backup
- ☐ Save numbers for my care team, pharmacy, a backup pharmacy and insurer
- ☐ Ask my care team how to reach them if their systems go down
- ☐ Tell someone I trust where my kit lives

2 Lock down your accounts

Read more in [TLC's Online Safety Toolkit](#)

- ☐ Strong, unique password and two-factor authentication on my email
- ☐ Two-factor authentication on my social media accounts, backup codes saved
- ☐ A password manager (built-in ones like Apple Passwords or Google Password Manager work well; see [TLC's toolkit](#))
- ☐ Log out of unknown devices and turn on login alerts
- ☐ Bookmark each platform's official account-recovery page
- ☐ If I run a group: two or more admins, all using two-factor authentication

3 Use AI with care

Make AI work for you

- ☐ Remove my name, birth date, address and ID numbers before I upload
- ☐ Turn off model training, keep chats out of shared links, read the privacy policy
- ☐ Ask the tool to weigh other explanations and say how sure it is
- ☐ Check answers that could change a decision with a second source or clinician
- ☐ Get AI apps only from the official developer
- ☐ Ask my doctor which AI tools touch my care and whether I can see their output

4 Speak up together

Report fraud and harm. Every report adds to the evidence regulators use to act.

- ☐ **Scam call, text or email:** report at [ReportFraud.ftc.gov](#) and forward scam texts to 7726^{18,49}
- ☐ **Lost money or data to a cybercrime:** file a complaint with the FBI at [ic3.gov](#)³¹
- ☐ **Someone used my identity or insurance:** get a recovery plan at [IdentityTheft.gov](#)¹⁹
- ☐ **A bill or Medicare charge for care I never got:** tell my insurer and report to HHS OIG at [oig.hhs.gov](#) or 1-800-HHS-TIPS⁵³
- ☐ **My provider or insurer failed to protect my health data:** file a complaint with the [HHS Office for Civil Rights](#)⁴⁸
- ☐ **A medical device, app or software problem, including a cybersecurity issue:** report to [FDA MedWatch](#) using Form 3500B for patients^{54,55}

CYBER SAFETY IS PATIENT SAFETY

Together, we can shine a light on cyber patient safety

No one should face a hacked hospital, a stolen support group or a confidently wrong chatbot alone. Every step in this guide protects you and the people in your community, and every question you ask pushes hospitals, platforms and AI companies to build safer systems.

The Light Collective is a nonprofit that advances the rights, interests and voices of patient communities in health technology. Patients founded us after finding their private support groups exposed online.

The Health Sector Coordinating Council Cybersecurity Working Group, our partner on this guide, is a government-recognized council of more than 400 health care providers, medical technology and pharmaceutical companies, payers and health IT organizations that works with government to reduce cyber threats to patient care.⁵⁶



The research behind this guide

For readers who want the studies and the stories. You do not need this page to act on the four actions.



Examples of real attacks and breaches

ASCENSION | MAY 2024

Records and the MyChart portal went offline across 140 hospitals; some diverted ambulances.⁵⁷ Nurses described catching medication errors.⁵⁸

[Read more: AP](#) [NPR](#)

CHANGE HEALTHCARE | FEBRUARY 2024

Pharmacies could not bill insurance, and some patients were quoted full retail prices for their medicines while workarounds took days.⁵⁹

[Read more: Axios](#)

SYNNOVIS, LONDON | JUNE 2024

Blood testing broke down: 10,146 appointments and 1,705 procedures postponed.⁶⁰ A long wait for blood test results contributed to one patient's death.⁶¹

[Read more: NHS England](#) [The Register](#)

KETTERING HEALTH, OHIO | MAY 2025

While the hospital's systems were down, scammers called patients pretending to be hospital staff and asked for credit card payments.²²

[Read more: WCPO](#)

IRHYTHM | JUNE 2026

Hackers stole data on at least 360,000 wearers of the company's heart monitors, including insurance and device numbers, then demanded a ransom not to leak it.⁶²

[Read more: SecurityWeek](#)

What the studies show

ATTACKS IN 13 COUNTRIES

316 documented harms to patients

A 2026 UC San Diego review of 59 studies, plus posts by patients and staff online.¹

[Read the study: Straw et al., JMIR 2026](#)

NEARBY EMERGENCY ROOMS

Ambulance arrivals rose from 1,741 to 2,354

At ERs near a hacked San Diego health system in 2021. Stroke codes rose from 59 to 103, and 360 people left without being seen, up from 158.⁸

[Read the study: JAMA Network Open 2023](#)

CARDIAC ARREST NEAR AN ATTACKED HOSPITAL

Good recovery fell from 4 in 10 to 1 in 20

Survival with good brain function at hospitals near one attacked hospital system.¹

[Read the study: Straw et al., JMIR 2026](#)

DATA BROKERS

11 brokers willing to sell mental health data

One offered names and home addresses of people with depression, cancer or PTSD.⁶

[Read the study: Duke Sanford 2023](#)

CHATBOTS AND DIAGNOSIS

Right conditions found under 35% of the time

In an Oxford trial of 1,298 adults using chatbots. A man who swapped table salt for sodium bromide based on a chatbot's advice spent about three weeks in the hospital.^{63,64}

[Read the study: Nature Medicine 2026](#)

Go further

Online Safety Toolkit

The Light Collective's step-by-step guides for patients and group leaders.²⁴

Critical AI Health Literacy

Campos and Salmi, National Academy of Medicine, on AI as a skill patients can own.⁴⁶

MedHELM leaderboard

Stanford's running scorecard of how AI models perform on 121 medical tasks.³⁷

Secure by Design

CISA's call for technology makers to build products that are safe out of the box, so the burden does not fall on patients.⁶⁵

HSCC publications

Free cybersecurity guidance for hospitals, clinics and health technology makers from our partner on this guide.⁶⁶

Straw et al., JMIR 2026

The review of patient harms during hospital cyberattacks behind page 5, with its open CIPHER dataset.¹

Glossary of terms

Plain-language definitions for words used in this guide, followed by the people who helped shape it.



Account takeover. Someone else gets into your online account and locks you out.

Ambient AI scribe. Software that listens to a medical visit and drafts the clinical note. You should be told before it is used and be able to decline.

Authenticator app. A phone app that makes a fresh login code every 30 seconds, used as a second lock on your accounts. Safer than codes sent by text.

Breach. Health or personal information seen, taken or shared by someone who should not have it.

Chatbot or large language model (LLM). An AI system trained on huge amounts of text to write answers. It sounds fluent whether or not it is correct.

Credit freeze. A free block that stops anyone from opening new credit in your name.

Cybersecurity. Defending computer systems and data against people who attack on purpose.

Device encryption. A built-in setting (FileVault on a Mac, BitLocker or Device encryption on Windows) that scrambles everything on a computer so a thief cannot read it without your password.

Downtime. A period when a hospital's computer systems are offline and staff fall back on paper, phones and faxes. Researchers have linked downtime to delayed tests, canceled surgeries and medication errors.

Electronic health record (EHR). Your care team's digital chart of your health information.

Explanation of benefits. A statement from your insurer listing care billed under your name.

FHIR. Fast Healthcare Interoperability Resources, pronounced "fire": the common format U.S. patient portals must use so an app you choose can pull your records.

Hallucination. AI output that sounds plausible but is incorrect or made up, such as an invented study or lab value.

Health privacy. Your control over who uses and shares your identifiable health data.

HIPAA. A federal law protecting health information held by doctors, hospitals, insurers and their business partners. Consumer apps and chatbots fall outside it unless your doctor, hospital or insurer provides them.

Medical identity theft. Someone uses your name or insurance to get care, drugs or payments.

Password manager. An app that creates and stores a strong, unique password for every account.

Patient portal. A website or app from your provider for records, results and messages. MyChart is one example.

Patient safety. The absence of preventable harm to a patient, in the World Health Organization's words, such as medication or diagnostic errors.

Phishing. A fake email, text or call designed to trick you into clicking a link, sharing a password or sending money.

Ransomware. Malicious software criminals use to lock a network's files and demand payment. Many also steal data.

Right of access. Your right under HIPAA to get a copy of your health records, usually within 30 days.

Security key. A small physical device, often shaped like a USB stick, that you plug in or tap to prove it is you. The strongest form of second lock.

Sycophancy. An AI's tendency to agree with you, even when you are wrong.

Two-factor authentication (2FA). A second check after your password, such as an app code, so a stolen password alone cannot open your account.

Acknowledgments

Thank you to the patient leaders and experts who helped us learn together and shape our findings. Your lived experience, questions and expertise made this guide stronger.

Andrea Downing

The Light Collective

Christine Von Raesfeld

The Light Collective

Michael Mittelman

American Living Organ Donor Fund

Erica Olenski

Monarch Futures

Donna Cryer

Cryer Health

David White

Patient Advocate

Erin Moore

Patient Advocate

Valencia Robinson

Women of Color Wellness Alliance

Lacey Harbour

VP Quality and Regulatory Advancement, Pathway for Patient Health

Bellinda King-Kallimanis, PhD

VP of Patient-Focused Research, LUNGevity

Jeff Tully, MD

UC San Diego Center for Healthcare Cybersecurity

Christian Dameff, MD

UC San Diego Center for Healthcare Cybersecurity

Isabel Straw, BMBS, PhD

University College London and UC San Diego Center for Healthcare Cybersecurity

Greg Garcia

Health Sector Coordinating Council

Sources and how to cite this guide

Every numbered source in this guide, with a link you can check. Facts current as of October 2026.



Sources

1. Straw I, Kumar D, Kweon S, Selzer J, Dameff C, Tully J. Unveiling patient-level harms and at-risk clinical groups during hospital cyberattacks: systematic review of global case studies and social media data. *Journal of Medical Internet Research* 28:e88257 (2026). doi:10.2196/88257
2. World Health Organization. Patient safety fact sheet. Sept 11, 2023.
3. Clusmann J, Freyer O, ... Downing A, ... Kather JN. Safety and security of large language models in healthcare. *Nature* 656, 577-589 (2026).
4. The Markup. Facebook is receiving sensitive medical information from hospital websites. June 16, 2022.
5. The Leapfrog Group. Choosing the right hospital, including the Hospital Safety Grade.
6. Kim J. Data brokers and the sale of Americans' mental health data. Duke University Sanford School of Public Policy, Tech Policy Lab. Feb 2023.
7. FOX 17 West Michigan. Kentwood family frustrated after cancer support page hacked. Oct 30, 2023.
8. Dameff C, Tully J, et al. Ransomware attack associated with disruptions at adjacent emergency departments. *JAMA Network Open*, 2023.
9. Perakslis ED, Ranney ML, Goldsack JC. Characterizing cyber harms from digital health. *Nature Medicine* 29, 528-531 (2023).
10. Cryer DR. Patients in the Loop. The Light Collective, October 2026. The seven-harm wheel on page 5 is adapted from this work and from Perakslis, Ranney and Goldsack (2023).
11. MyChart (Epic). Share your record: request a formal copy or a computer-readable copy of your health record.
12. HHS. Your rights under HIPAA to access your health information.
13. ASTP/ONC. Get it: how to access your health records.
14. Ready.gov. Tips for medications in an emergency.
15. CDC. Emergency medical kit for children with special healthcare needs.
16. Posnack S. Power to the patient: our record, our right, our choice. HealthIT.gov, Office of the National Coordinator (ONC), March 12, 2020.
17. Mandel J. MyChart Takeout: export your own health data. Open-source tool that runs entirely in your browser; your data never leaves your machine.
18. FTC. How to recognize and avoid phishing scams.
19. FTC. What to know about medical identity theft.
20. FTC. What to know about credit freezes and fraud alerts.
21. Gizmodo. Facebook nixes worrying loophole that put vulnerable closed groups at risk (BRCA Sisterhood group). July 12, 2018.
22. WCPO. Cyberattack forces outage at Kettering Health; scam callers try to get patients' card information. May 2025.
23. FBI Internet Crime Complaint Center. 2025 Internet Crime Report: 1,008,597 complaints and \$20.9 billion in losses; \$7.7 billion in losses reported by people 60 and older; 22,364 AI-related complaints with \$893 million in losses.
24. The Light Collective. Online Safety Toolkit for Patients.
25. CISA. Secure Our World.
26. Meta. Facebook and Instagram hacked-account recovery: facebook.com/hacked and instagram.com/hacked.
27. WTOP. Why the BBB is warning Facebook page owners about a new scam. May 2024.
28. The Light Collective. Moderation practices for peer support group leaders.
29. The Hacker News. 30,000 Facebook accounts hacked via fake Meta Support emails (Guardio Labs, AccountDumping). May 2026.
30. CBC News, Go Public. Report on a New Brunswick Facebook account takeover and Marketplace scam. March 2024.
31. FBI Internet Crime Complaint Center. Report a cybercrime at ic3.gov.
32. NEJM AI. Perspective on ambient AI scribes in clinical consultations, policy, consent and patient safety. doi:10.1056/Alpc2501401
33. Ohde JW, et al. Barriers and opportunities of scaling ambient AI scribes for clinical documentation across diverse healthcare settings. *npj Digital Medicine* 9:369 (2026).
34. KFF. Tracking poll on health information and trust: use of AI for health information and advice. March 25, 2026.
35. Yang F, Graetz I. Ambient AI tool adoption in US hospitals and associated factors. *American Journal of Managed Care* 32(1):e25-e30 (2026). 1,744 of 2,784 Epic hospitals (62.6%) had adopted an ambient AI tool as of June 2025.
36. PC Gamer. ChatGPT removes search-engine sharing after nearly 4,500 conversations were indexed by Google. Aug 4, 2025.
37. Bedi S, Cui H, Fuentes M, et al. MedHELM: holistic evaluation of large language models for medical tasks. Stanford Center for Research on Foundation Models, 2025. Leaderboard at crfm.stanford.edu/helm/medhelm.
38. Chen S, et al. When helpfulness backfires: LLMs and the risk of false medical information due to sycophantic behavior. *npj Digital Medicine*, Oct 2025.
39. Stokel-Walker C. Deepfakes and doctors: how people are being fooled by social media scams. *BMJ* 2024;386:q1319.
40. Malwarebytes. Attack of the clones: fake ChatGPT apps are everywhere. Nov 3, 2025.
41. Kohane IS. Compared with what? Measuring AI against the health care we have. *NEJM* 391(17), Oct 2024.
42. Newman-Toker DE, et al. Burden of serious harms from diagnostic error in the USA. *BMJ Quality & Safety* 33(2):109-120 (2024).
43. American College of Emergency Physicians. Emergency department boarding: a public health crisis (physician stories, n=140+).
44. ECRI. Misuse of AI chatbots tops annual list of health technology hazards (2026).
45. Axios. OpenAI report: 40 million people a day use ChatGPT for health; 7 in 10 health conversations happen outside normal clinic hours. Jan 5, 2026.
46. Campos H, Salmi L. Critical AI health literacy as liberation technology: a new skill for patient empowerment. *National Academy of Medicine Perspectives*, Dec 8, 2025.
47. Mayo Clinic. Can you trust AI for health advice?
48. HHS Office for Civil Rights. Filing a HIPAA complaint.
49. FTC. ReportFraud.ftc.gov.
50. The Light Collective and Digital Public. Collective Digital Rights for Patients, v1.1 (2022). Resources at lightcollective.org/trust.
51. Yu KH, Healey E, Leong TY, Kohane IS, Manrai AK. Medical artificial intelligence and human values. *NEJM* 390:1895-1904 (2024).
52. Downing A, Perakslis E. Health advertising on Facebook: privacy and policy considerations. *Patterns* 3(9), 2022.
53. HHS Office of Inspector General. Report fraud (1-800-HHS-TIPS).
54. FDA. MedWatch: safety information and adverse event reporting program.
55. FDA. Cybersecurity of medical devices (patients report device cybersecurity issues with MedWatch Form 3500B).
56. Health Sector Coordinating Council Cybersecurity Working Group. About the HSCC.
57. AP via PBS Wisconsin. Cyberattack forces Ascension to divert ambulances and take records offline. May 13, 2024.
58. NPR. Nurses describe care lapses after Ascension ransomware attack. June 19, 2024.
59. Axios. Prescription outage after ransomware attack on UnitedHealth unit. March 1, 2024.
60. NHS England (London). Update on cyber incident: clinical impact in South East London. Sept 19, 2024.
61. The Register. Patient death linked to Synnovis ransomware attack; 170 patients harmed. June 26, 2025.
62. SecurityWeek. iRhythm data breach impacts at least 360,000 people. Oct 12, 2026.
63. Bean AM, et al. Reliability of LLMs as medical assistants for the general public: a randomized preregistered study. *Nature Medicine*, Feb 2026.
64. *Annals of Internal Medicine: Clinical Cases*. A case of bromism influenced by use of artificial intelligence. Aug 2025.
65. CISA. Secure by Design.
66. Health Sector Coordinating Council Cybersecurity Working Group. Publications.



How to cite this guide

The Light Collective and the Health Sector Coordinating Council Cybersecurity Working Group. *Cyber Safety Is Patient Safety: A patient guide to protecting your care, your accounts and your community*. October 2026. lightcollective.org

Licensed under **CC BY 4.0**: share and adapt freely with credit. Questions or feedback: contact@lightcollective.org