Position Paper: Computer-Related Healthcare Risks

Peter G. Neumann
Chief Scientist
SRI Computer Science Lab, Menlo Park CA 94025 USA
neumann@CSL.SRI.COM https://www.csl.sri.com/users/neumann

Abstract

This is a summary of recent risks related to healthcare from the ACM Forum on Risks to the Public on Computers and Related Subjects, which I created in August 1985 and have moderated since then. The complete set of RISKS archives is at http://www.risks.org, and specific issues referred to as (R vol no) can be obtained directly in the searchable site in Newcastle UK: http://catless.ncl.ac.uk/Risks/i.j.html and ftp://www.sri.com/risks).

CCS Concepts: Security and Privacy; Applied Computing → Life and Medical Sciences

Keywords: Healthcare Risks and Damages, System and Subsystem Trustworthiness, Safety, Security, Integrity, Reliability, Survivability, Usability, Real-time Behavior, Assurance

ACM Reference Format:
Peter G. Neumann. 2024. Position Paper: Computer-Related Healthcare Risks. *In Proceedings of the 2024 Workshop on Cybersecurity in Healthcare (HealthSec '24), October 14-18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3689942.3694749

Introduction

I have assembled a collection of computer-relevant items, categorized thematically – mostly from the past five years of RISKS. Included are human safety and security issues (e.g., hospitals and health-care providers hit by ransomware and other attacks), a wide variety of privacy issues, COVID-related problems, and other miscellaneous risks, along with some of my own interspersed comments about the risks in each category – generally italicized.

Almost everything today seems to have dual-use applicability, in the sense of having both up-sides and down-sides, with many different risks emerging in both cases. However, awareness of the risks by both system developers and the general public is typically very poor, and would benefit from reaching more widely. Not only are the risks widely ignored overall, the notion of ground truth seems to have disappeared when it comes to conspiracy theories and rampant disinformation.

HealthSec '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-1238-8/24/10. https://doi.org/10.1145/3689942.3694749

The risks of misinformation and willful disinformation are not a new challenge, but recently have been seriously exacerbated. This is also becoming especially difficult as it relevant to artificial intelligence and chatbots.

Risks seem to be getting wildly out of control, particularly with respect to computers involved in healthcare, hospital and clinical uses of artificial intelligence, self-driving vehicles, and other life-critical or mission-critical automated and semi-automated systems: From a computer perspective, **we desperately need evidence-based assurance rather than over-hyped assertions that we should simply trust the developers and operating managers. Otherwise, the integrity and credibility of our rampantly increasing overdependence on untrustworthy technology may cause a collapse of trust in our technology.** Undoubtedly, avoiding systemic failures may require radical changes in how computer science and system engineering should be taught and practiced, along with corresponding oversight, and consequentially much heavier penalties for failures.

My own research has been inspired by the Albert Einstein Principle – that *Everything should be made as simple as possible, **but no simpler***. It is just one of many important principles that are needed to make our computer-related healthcare into a more robust, safe, and secure discipline; however, it has been one of my most fundamental principles ever since my long discussion on complexity with Albert Einstein at home in November 1952. In numerous cases, it is the violation of the "no simpler" part, ignoring obscure corner-cases whose triggering can result in disasters. In healthcare, the *no-simpler* might be related to the stark difference between allopathic medicine (western) and holistic/functional medicine (which treats causes rather symptoms). It is often the source of systemic failures in embedded devices such as the Therac 25 (noted below), and rampant system security and safety flaws.

Holistic thinking in healthcare is not just thinking *out of the box* – it is realizing that there never was a box in the first place, as diagnosing and treating problems are often open-ended. However, that is my own apparently counter-cultural view, and not the primary thrust of this position paper.

In the near future, global warming and environmental hazards are likely to have a terrible impact on healthcare in countries where there is little electricity, and in developed countries where power failures will require massive cogeneration plants to ensure power system survivability in crises. I have tried here to minimize examples of secondary and tertiary risks, although in some cases they can escalate into critical factors.

Overall, we must also beware of human foibles – e.g., being blinded or legally bound by so-called best practices, which in reality are lowest-common-denominator guides and nowhere near what should be best practice. We must also avoid over-endowing uses of technology to solve non-technological problems, simplistic legislation, charlatans, frauds, and other recurring risks, some of which related to healthcare are noted here.

Systemic Trustworthiness Requirements:

Risks Regarding Human Safety, Integrity, Security, Privacy, Reliability, Real-time Response, and more

Everything in our lives seems to be increasingly interconnected with other problems: healthcare is influenced by climate change, locust swarms, melting icebergs, failing bird flocks, bird flu, and previously unseen migration patterns, the dolphin and whale groundings, pollution, Tonga-Hunga Ha'apai eruption, underground explosions, and so on. Air pollution is linked to irreversible sight loss (R 32 49). Forever chemicals are widespread in U.S. drinking water (R 32 46). Glyphosate was found in samples from a French infertility clinic raising questions about controversial chemical's impact on fertility. (More than 55% of sperm samples from a French infertility clinic contained high levels of glyphosate, the world's most common weedkiller, raising further questions about the chemical's impact on reproductive health and overall safety, noted on 24 May 2024.) Rainwater everywhere on Earth unsafe to drink due to forever-chemicals (R 33 38-39). A weekend-long Iowa fertilizer spill killed 750K fish in Iowa and Missouri over a 60-mile stretch of rivers (R 34 12). As Tom Lehrer wrote in the song Pollution, "Don't drink the water, and don't breath the air." Brain-altering bioweapons snd DNA surveillance: Experts are already preparing for the next biological threat (R 32 49). Scientists propose lithium to cope with high-risk condition in future fusion facilities (R 32 49). A hole in the International Space Station made by a meteorite the size of a grain of sand (R 33 27). Nuclear waste. Toxic dumps. Computer fabrication effluents. GPS spoofing. Cyber-attacks could jeopardize global food supplies (R 33 23) – they are already affecting shipping through the Suez Canal. The lack of trustworthiness in artificial intelligence is outrageous. And so on, ad infinitum. Thus, we need more holistic thinking, where so many factors are involved in healthcare and human wellbeing. Nevertheless, although we focus mostly on first-order risks to healthcare – we also note some of the collateral risks.

Medical Device Failures

The Therac-25 was an early example of a radiation therapy device that alternated as a high-intensity research machine. The Therac-20 had a physical interlock that prevented the switchover from research mode to therapy mode from causing any damage. The programmer of the Therac-25 software forgot the hardware interlock in the Therac 20, and some people were killed or maimed. Professor Nancy Leveson at MIT and the University of Washington was very influential in the aftermath of this case. Her works on human safety are noted in the reference section. Some more recent examples follow.

- Medical and IoT Devices Vulnerable to Attack: Researchers at Forescout's Vedere Labs cybersecurity intelligence team and CyberMDX cybersecurity service provider discovered seven vulnerabilities, known collectively as *Access:7*, in more than 150 Internet of Things (IoT) devices made by over 100 companies. Three of the critical bugs allowed attackers to gain full control of devices by remotely executing malicious code. The remainder, rated moderate to high in severity, allow attackers to steal data or execute denial-of-service attacks. The flaws were found in multiple versions of PTC Axeda agent and PTC Desktop Server, which are used in many IoT devices to enable remote access and management. All versions of the Axeda technology below 6.9.3 are affected. PTC has released patches for the vulnerabilities. [Jai Vijayan, 8 Mar 2022, Dark Reading, R 33 09)
- FDA Warning Links Heart Pump to 49 Deaths: A troubled Impella heart pump that has now been linked to 49 deaths and dozens of injuries worldwide will be allowed to remain in use, despite the FDA's decision to issue an alert about the risk that it could puncture a wall of the heart. The FDA said Abiomed (the manufacturer of the device, acquired by Johnson & Johnson in 2022) should have notified the agency more than two years before that, when the company first posted an update on its website about the perforation risk. "To say that you're addressing 49 deaths by saying 'be careful' is not addressing the problem at all." Rita Redberg, UCSF cardiologist and professor. (R 34 12)
- Bluetooth-related flaws threaten dozens of medical devices, including pacemakers (R 31 59); Oximeters used to be designed for equity. What happened? (R 32 70) Blood oxygen monitors face scrutiny from FDA panel (33 51); 'Painless' glucose monitors are popular, but with little evidence that they help most diabetes patients (R 32 55); More than 200 people with diabetes injured after software issue drained insulin pump batteries, shut down unexpectedly due to a problem with a connected mobile app; Class 1 Recall (R 34 24); Cell phones and cancer: New UC Berkeley study suggests cell phones sharply increase tumor risk (R 32 76-77); Study finds variations in quantitative MRI scanners' measurements (R 32 75); Get This Thing Out of My Chest: A life-sustaining heart pump was taken off the market after years of problems and FDA inaction. Thousands of people are now stuck with it embedded in their hearts. Those who already have the heart pump, also known as the HVAD, can't simply get it removed or replaced. The required surgery is typically considered more dangerous than leaving it in. (R 33 01); Vulnerability of insulin pumps (R 33 46); Surprisingly many risky infusion pumps? Are you part of the IoT? (33 08); Four vulnerabilities discovered in popular infusion pumps, WiFi batteries (R 33 44)
- Government says polluters can dump raw sewage into rivers as Brexit disrupts water treatment (R 32 87)
- AI comes to the operating room: Images made by lasers and read by computers can help speed up the diagnosis of brain tumors during surgery. "The study involved brain tissue from 278 patients, analyzed while the surgery was still going on. Each sample was split, with half going to AI and half to a neuropathologist. The diagnoses were later judged right or

wrong based on whether they agreed with the findings of lengthier and more extensive tests performed after the surgery. The result was a draw: humans, 93.9% correct; AI, 94.6%." 'Correct'? No false-positive or false-negative AUC ROC measures! (R 31 54)

- A High-Risk Medical Device Didn't Meet Federal Standards. The Government Paid Millions for More. (R 33 02); More than half of medical devices have critical vulnerabilities (R 33 03)
- Their Bionic Eyes Are Now Obsolete and Unsupported: Patient had to find out second-hand that the company had abandoned the technology and was on the verge of going bankrupt. While his two-implant system is still working, he doesn't know how long that will be the case. (R 33 06)
- Top Philips executive approved sale of defective breathing machines by distributors, with tests showing health risks (R 33 92)
- Wearable fitness trackers could interfere with cardiac devices, study finds (R 33 63)
- Your Medical Devices Are Getting Smarter: Can the FDA Keep Them Safe? Unfortunately, the historical record is spotty. (R 33 89); Medical and IoT devices are almost all vulnerable to attack (R 33 09)
- Crushed to death by robot in South Korea (R 33 93-94)

Ransomware and Other Cyber-Attacks

Ransomware is the latest form of disruption of entire sets of networked computer-communication systems. Here are a few recent outages and the concomitant risks. However, there are many other forms of attacks.

- Ransomware Attack Against UnitedHealth Shows Flaws in Cybersecurity Persist: The recent cyberattack on the billing and payment colossus Change Healthcare (Making Change as well as Changing Healthcare?) revealed just how serious the vulnerabilities are throughout the U.S. healthcare system, and alerted industry leaders and policymakers in the urgent need for better digital security. (R 34 12) [They clearly have not been reading RISKS for any of the past 38 years! PGN]; Alarms over healthcare cyberattacks are getting louder (R 33 45); Corporate Greed Made the Change Healthcare Cyberattack Worse (R 34 17); UnitedHealth Top Executive Slammed Over Cyberattack (R 34 24); London Hospitals FaceMajor Disruptions After Cyberattack: ransomware cyberattack on Synnovis significantly disruptive (R 34 29)
- Patients of a Vermont hospital are left in the dark after a cyberattack (R 32 39)
- Irish Health Service hit by ransomware (Patrick O'Beirne); Steamship Authority targeted in ransomware attack, unable to make reservations for several weeks to/from Martha's Vineyard and Nantucket – serious implications on ambulances, hospitals, etc. (R 32 70); What if doctors are always watching, but never there? (R 32 72)
- U.S. Publishes Draft Federal Rules for Cyber Incident Reporting*: Companies would need to report substantial attacks within 72 hours and ransom payments within 24 hours. (James Rundle, *Wall Street Journal*, R 34 13); Ransomware attacks on hospitals take toll on patients (33 51); Ransomware attacks have entered a heinous new phase (R 33 66); Cybercriminal group claims responsibility for ransomware attack as hospital CEO says recovery will take weeks (R 33 92); Paying ransom for data stolen in cyberattack bankrolls further crime, experts caution (R 33 94); Ransomware forces 3 hospitals to turn away all but the most critical patients (R 31 45) Ransomware and cyber-insurance (R 32 71); Company shuts down because of ransomware, leaves 300 without jobs just before holidays (R 31 53); Cybersecurity insurance, if you can get it (R 32 70); We Have Met the Ransomware Enemy, and It Is (Partly) Us! (R 32 71); Cybersecurity Framework Profile for Ransomware Risk Management – Preliminary Draft (R 32 71); Secret chats show how Cybergang became a ransomware powerhouse (R 32 69); How to Negotiate with Ransomware Hackers (R 32 70) Hackers are using the Coronavirus panic to spread malware (R 31 59); (R 31 60); Live Coronavirus Map Used to Spread Malware (R 31 62); Coronavirus Reactions Creating Major Internet Security Risks (R 31 64); Keeping the DNS Secure During the Coronavirus Pandemic (R 31 68); Clinical trials hit by ransomware attack on health tech firm (R 32 31); How coronavirus turned the dystopian joke of FaceID masks into a reality A computer virus expert looks at CoVID-19 (R 31 64-67); Nearly 50% of Twitter Accounts Talking about Coronavirus Might Be Bots (R 31 72); Thousands of cases went unreported in California when a computer server failed (R 32 19); Devices Used In COVID-19 Treatment Can Give Errors For Patients With Dark Skin (R 32 42); Ransomware and new virus strains (R 32 43); How California's new Digital Vaccine Records can be easily abused (R 32 76); Healthcare giant comes clean about recent hack and paid ransomware (R 34 22)
- Water supply control system breached and adjusted to dangerous PH level; Poor password security led to water treatment facility hack; AA21-042A: Compromise of U.S. Water Treatment Facility (R 32 49) (Multiple items, R 32 49)
- Health-care hack spreads pain across hospitals and doctors nationwide (R 34 09); Cyberattack Paralyzes the Largest U.S. Healthcare Payment System (R 34 09); Costa Rica declares emergency in ongoing cyberattack (R 33 20)
- Cut submarine cables cause web outages across Africa; 6 countries still affected (R 34 10)
- FBI blocked planned children's hospital cyberattack (R 33 25)
- Chernobyl and other nuclear power disasters caused huge healthcare problems. The most recent risk was the Russian mishandling of Chernobyl Redux in the war in Ukraine. (R 33 09)
- The nuclear mistakes that could have ended civilization (R 32 19,20); Nuclear waste and nuclear waste management at the Hanford site (R 32 31); India's inadvertent missile launch underscores the risk of accidental nuclear warfare news and research (R 33 14); The dangerous business of dismantling America's aging nuclear plants (R 33 21); Fighting Around Zaporizhzhia Nuclear Power Plant Is 'Out of Control: Nuclear power plants were designed to defend against certain foreseeable risks, but not wars! (R 33 37); Nuclear Fusion Is Already Facing a Fuel Crisis: It doesn't even work yet, but nuclear fusion has encountered a shortage of tritium, the key

fuel source for the most prominent experimental reactors. (R 33 37); Nuclear War Simulator Creator Says Public Must Know Potential Destruction (R 33 49)
- Hospital IT melts in heatwave, leaving doctors without patient records (R 33 35); Google, Oracle cloud servers wilt in UK heatwave, take down websites (R 33 35)
- Even a security expert can get phished (R 34 10)

Utility Outages

Beginning with the massive east-coast power outage in 1965 (when I was in the ninth floor of the MIT Project Mac computer room, and the disk units all made a slurping noises shutting down simultaneously), power outages have periodically been a massive problem. Hospitals have learned that they need standby backup power to continue life-critical operations. We have also learned that entire power grids can be easily brought down by hacking attacks.

- Cosmic rays causing 30,000 network malfunctions in Japan each year (R 32 60); There are doubts about evidence that 5G harms humans (R 32 57,58); Energy-harvesting card treats 5G networks as wireless power grids (R 32 58,59); Yet another 5G attack vector (R 32 58); U.S. and Japan to invest $4.5bn in next-gen 6G race with China (R 32 61); U.S. Intelligence Agencies warn about 5G network weaknesses (R 32 66); Major Internet outage affecting users from Washington DC to Boston; Verizon fiber cut reported (R 32 47); Hospital network/computer outage in Pacific Northwest (R 33 48); Veteran Affairs big software upgrade is plagued by hidden costs and flawed training (R 32 77); Israeli Health Ministry website faces cyberattack, oversea access blocked (R 33 44)
- Risks of CPAP machines: CPAP murder mystery regarding the advent of remotely controllable ones with minimal security? (R 33 12)
- Death or Utopia in the Next Three Decades (R 31 93); Mental health, stress, and moral injury (R 32 09); The problem with mental health bots (R 33 48); Can AI help fill the therapist shortage? Mental health apps show promise and pitfalls (R 34 16); We Need to Change the System That Keeps Pilots from Seeking Mental Health Care (R 33 55)

Global Implications

Uncontaminated food supplies are dwindling, GMO is taking over; water, air, and ground contamination are burgeoning. Ecosystems are failing. Species extinction is rampant. All of these problems have effects on healthcare.; One-fifth of countries at risk of ecosystem collapse, analysis finds (R 32 32,33) Global methane emissions soar to record high (R 32 17); Why climate change is about to make your bad commute worse (R 32 19); Greenland's ice sheet has melted to a point of no return, according to new study (R 32 200; rebuttal (R 32 24,25); MRI study reveals all mammals, including humans, share equal brain connectivity (R 32 17)

- Groundbreaking new material 'could allow artificial intelligence to merge with the human brain' (R 32 21,22); The Brain Implants That Could Change Humanity (R 32 25); Neuralink: Elon Musk unveils pig he claims has computer implant in brain (R 32 25); Elon Musk Defends Neuralink Against Neuroscientist's Concerns of Chips Overheating (R 32 37) The future is cyborg: Kaspersky study finds support for human augmentation (R 32 27,28)
- Doctors 'bribed to use infected blood products' (R 34 26)

HIPAA and Privacy/Social Problems

HIPAA is causing considerable disruption to medical practitioners. Privacy is also a huge problem, in part because computer systems are inadequately trustworthy, and handling of data is often sloppy.

- HIPAA Electronic health records and doctor burnout (R 31 22,23)
- Babylon Health app error allowed UK users to watch videos of other patients' private doctor visits (R 31 98)
- Researchers examine burden of electronic health record on primary-care clinicians (R 32 76)
- Dartmouth Medical School drops online cheating cases against students (R 32 71)
- From a small town in North Carolina to big-city hospitals, how software infuses racism into U.S. healthcare (R 32 32); Fixing medical devices that are biased against race or gender (R 32 71)
- Facebook Is Receiving Sensitive Medical Information from Hospital Websites (R 33 29); Facebook plans to show content mainly from strangers (R 33 29); Facebook to hijack Facebook accounts when Gmail credentials are used to sign in to the service. (R 33 30); Facebook encrypting links to avoid URL-stripping (R 33 33); Facebook, privacy and abortion (R 33 33); Danger: Metaverse Ahead! (R 33 38)
- Thoughts about Google's new blog post regarding health-related data privacy (R 33 32); FEC approves Google's horrible political spam filter bypass plan (R 33 38)
- Anonymity no more? Age checks come to the Web. (R 32 91)
- Banning anonymous social media accounts would only stifle free speech and democracy (R 32 91)
- Navy doctors and dentists were [accidentally] told they owe 3 more years of service; military admits to another record-keeping error (R 33 70)
- Medicare forced to expand forms to fit 10-digit bill a penny shy of $100M (R 34 13)

Data Breaches and Privacy Problems

Privacy leaks are frequent, especially with respect to personal medical records. Surprisingly there is also unexpected sharing.

- Hospitals give tech giants access to detailed medical records. Deals with Microsoft, IBM and Google reveal the power medical providers have in deciding how patients' sensitive health data is shared. (R 31 55)
- 96% of U.S. hospital websites share visitor info with Meta, Google, data brokers: Hospitals despite being places where people implicitly expect to have their personal details kept private frequently use tracking technologies on their websites to share user information with Google, Meta, data brokers, and other third parties, according to research. (R 34 17); Phishing attack hits Los Angeles County public health agency, jeopardizing 200,000-plus residents' personal info (R 34 31)

- Independent security researcher discovers information trove of 1.2B users' personal information (mostly from by People Data Labs); server shut down after FBI contacted (R 31 49)
- How to prevent a data breach, lessons learned from the infosec vendors themselves (R 31 48)
- Hackers steal data for 15 million patients, then sell it back to lab that lost it (R 31 52)
- Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, hospitals, hospitals, etc. (R 32 54)
- Albertans' personal information exposed after national healthcare provider hacked, data put up for sale (R 32 79)
- GoDaddy says data breach exposed over a million user accounts (R 32 94)
- Amazon's Dark Secret: It Has Failed to Protect Your Data (R 32 94)
- Artist finds private medical record photos in popular AI training data set (R 33 46)
- Data breach of Ontario's vaccine booking system affects hundreds of thousands, province says (R 33 57)
- Biometric devices sold on eBay reportedly contained sensitive U.S. military data (R 33 59)
- Data breach of Michigan healthcare giant exposes millions of records (R 33 94)
- Data on 267,000 Sarnia patients going back 3 decades among cyberattack thefts at 5 Ontario hospitals (R 33 93-94)

Risks of Artificial Intelligence

Artificial Intelligence generally has no assurance that it will be correct, safe, reliable, secure, or anything else. We note the need for evidence-based assurance in the introduction to this paper. It is particularly relevant to healthcare, not just with respect to large language models, chatbots, and machine learning, but also to their being embedded in untrustworthy hardware and operating systems, with inadequate oversight. See my CACM article on total-system trustworthiness, http:\\www.csl.sri.com/~neumann/cacm252.

Considering the risks before you leap seems like a useful mantra. Sadly, it seems to be ignored by people who develop automated vehicles, ChatGPT, sensitive uses of artificial intelligence, cryptocurrencies, and many other systems that frequently appear in this section. This is particularly critical in healthcare, to which computer systems and the Internet are being widely used – and widely misused or exploited. However, rampant misuse of artificial intelligence has seriously exacerbated trustworthiness.

- The state of AI right now is absolutely ridiculous. This is terrifying (R 33 34) [This item from July 2022 was true then, but is even more relevant now.]
- Assigning liability when medical AI is used (R 31 62); Most medical imaging devices run outdated operating systems (R 31 62); Come on, Microsoft! Is it really that hard to update Windows 10 correctly? [Yes!] (R 31 62)
- To Understand the Medical Supply Shortage, It Helps to Know How the U.S. lost the lithium battery (R 31 72)
- Mayo Clinic AI engineers face an acid test: Will their algorithms help real patients? (R 31 56)
- AI algorithms detect diabetic eye disease inconsistently (R 32 44)
- Flawed Algorithm Used to Determine UK Welfare Payments Is 'Pushing People Into Poverty' (R 32 31)
- Digital stethoscope uses artificial intelligence for diagnosing lung abnormalities (R 32 40)
- Artificial intelligence-created medicine to be used on humans for first time (R 31 56,57); AI in medicine (R 32 70); Implantable AI system developed for early detection and treatment of illnesses (R 32 84); Insufficient evidence that AI breast cancer screening is accurate enough to replace human scrutiny (R 32 86); AI matches cardiologists' expertise, while explaining its decisions (R 32 86) AI Can Help Patients – but Only If Doctors Understand It: Algorithms can help diagnose a growing range of health problems, but humans need to be trained to listen. (R 32 87); Artificial Intelligence: Stephen Colbert: "Are you afraid of artificial intelligence taking over?" Ricky Gervais: "I'd love for any intelligence to take over." (R 33 22)
- Sloppy Use of Machine Learning Is Causing a Reproducibility Crisis in Science (R 33 38)
- This $5 billion insurance company likes to talk up its AI. Now it's in a mess over it. (R 32 70);
- Artificial intelligence predicts patients' race from their medical images (R 33 23-24)
- Health apps share your concerns with advertisers. HIPAA can't stop it. (R 33 46)
- FBI warns individuals employed in the healthcare industry of the ongoing scam involving the impersonation of law enforcement and government officials (R 33 43)
- AI has arrived in your doctor's office. Washington doesn't know what to do about it. (R 33 92)
- California halts operations of Cruise self-driving robotaxis (R 33 92)
- The FDA should better regulate medical algorithms (R 32 90)
- More on The Titan's Submersible Disaster Was Years in the Making (R 33 83)
- Mushroom pickers urged to avoid foraging books on Amazon that appear to be written by AI. [The risks of erroneous Chat-Bots are enormous, and it may be difficult to sue anyone for false representations. PGN] (R 33 82)
- Risks of self-driving cars: California Gov. Gavin Newsom vetoed a bill Friday that would have required a human safety operator to be present any time a self-driving truck operated on public roads in the state. (R 33 87-88
- Colorado ski town emergency dispatch centers fielding dozens of automated 911 calls from skier iPhones (R 33 60); Robot Cars Are Causing 911 False Alarms in San Francisco (R 33 61); How Smart Are the Robots Getting? (R 33 61,62)
- Today's Robotic Surgery Turns Surgical Trainees Into Spectators: "Medical training in the robotics age leaves tomorrow's surgeons short on skills.; (R 33 36-37); Who is at fault when something goes wrong? (R 33 38)
- Autonomous Vehicles Are Driving Blind (R 33 89-90)
- Do-It-Yourself artificial pancreas given approval by team of experts (R 32 93)
- Lab tests delayed by *Twilight Zone* births (R 32 16)

- Trans man says confusion caused cervical screening delay (R 32 90-91)
- CoolSculpting: fat-freezing procedure left supermodel Linda Evangelista 'disfigured' (R 32 89)
- An AI app claims it can detect sexually transmitted infections. (R 34 15)
- Hospital bosses love AI. Doctors and nurses are worried. (R 33 78)
- Microsoft lays off an ethical AI team as it doubles down on OpenAI (R 33 66); AI is now indistinguishable from reality (R 33 69-70); Doctors warn about AI's *existential threat to humanity* (R 33 70)
- AI to act as doctor's second pair of eyes to spot nearly invisible colon cancer growths (R 33 66)

Disinformation, Lies, Fakes, Biases, etc.

The notion of ground truth seems to be vanishing, in many contexts, but particularly with respect to bad uses of AI and educational practices that seem to be dumbing down what is taught in many schools, together with a proclivity for acceptance of patently obvious "truthiness", which is offered instead (early 19th century term revived by Stephen Colbert: The appearance of trust in something that is not trustworthy). Sloppy or even dishonest research practices are also an occasional problem. Once again, we need greater emphasis on evidence-based research.

- Texas Surgeon Is Accused of Secretly Denying Liver Transplants (R 34 17)
- Hospital's false death announcement leads to a wife's suicide; husband later found alive (R 34 02)
- The makers of EyeDetect promise a new era of truth-detection, but many experts are skeptical (R 32 94)
- True Story? Lie-Detection Systems Go High-Tech: Electrodes affixed to the face may determine whether someone is lying, e.g., moving eyebrows involuntarily, or slight movement of lips, and eye-tracking; claims it detects 73% of lies. More than 65 U.S. law enforcement agencies and close to 100 agencies worldwide use EyeDetect, which claims to be 86% to 88% accurate. (R 33 06)

Legislation and Law Enforcement

Governments have become sharply polarized, and some law enforcement institutions have become seriously biased.

- Who Is Liable when AI Kills? (R 33 31)
- Tesla is settling with the family of the Apple engineer who died in an Autopilot crash (R 34 16)
- UK proposes new rule for AI: AI systems will have to identify a legal person to be held responsible for any problems under proposals for regulating AI unveiled by the UK government: Ensure that AI is used safely; Ensure that AI is technically secure and functions as designed; Make sure that AI is appropriately transparent and explainable; Consider fairness; Identify a legal person to be responsible for AI; Clarify routes to redress or contestability. (R 33 34-35);
- True Story? Lie-Detection Systems Go High-Tech (noted above, but also relevant to law enforcement). (R 33 06)
- Electronic Health Record Legal Settlements (R 33 53)

Miscellaneous Other Risks

- Hospital prices for the same emergency care vary up to 16X; Hospitals' *trauma activation fees* are unregulated and extremely variable. A 2023 KFF analysis on compliance found that the pricing information hospitals provided is "messy, inconsistent, and confusing, making it challenging, if not impossible, for patients or researchers to use them for their intended purpose." A February 2024 report from the nonprofit organization Patient Rights Advocate found that only 35 percent of 2,000 US hospitals surveyed were in full compliance with the 2021 rule. (R 34 19)
- Some hospitals still use pneumatic tubes – and they can be hacked (R 32 81) hospital equipment (R 32 83)
- Woman died trapped in burning 2009 Dodge Journey SUV after a vehicle malfunction-caused fire, and she could not unlock the doors (R 33 62)
- Pedestrian dies after Cruise cars block ambulance: alleged that would have survived had two Cruise cars and an unoccupied police car not prevented the ambulance from leaving promptly. (R 33 83); see for reinterpretation (R 33 84) and much more (R 33 85-86)
- 3+ Years Later and Millions of U.S. Patient X-Rays are Still Exposed to the Internet by Insecure PACS Servers (R 33 23)
- WashDC Metrorail Safety Commission says Metrorail routinely skipped steps in restoring lethal electrical power to tracks in work zones. putting workers at risk. (R 33 37)
- 'Our world is in peril', United Nations Secretary General Warns General Assembly (R 33 46)
- Long-term planning and optimization, includes PGN quoting Paul Krugman: "... if we can't save the Great Salt Lake, what chance do we have of saving the planet?" (R 33 28-29,31)
- Unusual computer errors from outer space (R 33 49)
- Ethiopian Air plane fails to descend as pilots reportedly fell asleep during flight (R 33 40); oxygen starvation? stress?
- Major psychologists' group warns of social media's potential harm to kids (R 33 70); The risks of machine learning psychotherapy with voice interfaces (R 33 87)
- Illumina Cybersecurity Vulnerability May Present Risks for Patient Results and Customer Networks: Letter to Healthcare Providers (R 33 25)
- It's time to ask patients to quit social media, especially regarding mental health (R 33 34)
- Cyberprofessionals say industry urgently needs to confront mental health crisis (R 33 83)
- Algorithmic Tracking 'Damaging Mental Health' of UKWorkers (R 32 93)
- The major healthcare and cybersecurity risks in Right-to-Repair laws (R 33 32); A New Jailbreak for John Deere Tractors Rides the Right-to-Repair Wave (R 33 39)
- How a Lucrative Surgery Took Off Online and Disfigured Patients (R 33 92)
- Dangerous prescription drug ads on TV (R 33 82)
- Hackers are stealing encrypted data today so quantum computers can crack it in a decade (R 32 92)
- U.S. Gender Care Is Ignoring Science (R 34 36: Pamela Paul, *The New York Times*, Sunday Opinion, 14 Jul 2024); rebuttal (R 34 37); counter-rebuttal (R 34 38)

- New findings shed light on risks and benefits of integrating AI into medical decision-making (R 34 37)

COVID-19, Vaccines, and Politics

COVID and other respiratory diseases seem to have become pervasive, in part as a result of changes in our ecological environment, which in turn created huge changes in almost everyone's life over the past years. The coverage in the ACM Risks Forum was rather overwhelming, and too much to include here on a per-item basis – as it covered a very wide range of risks. Thus, we merely summarize some of the main risks that arose. The full list can be found in the RISKS archives.

- Causality and Casualty: Covid Vaccine Side Effects: 4 Takeaways From Our Investigation (R 34 22); Could the Covid-19 Vaccines Have Caused Some People Harm? Thousands think that their cases have been ignored.
  - "I'm not real." Patients who they experienced bad side effects say they have received little support or acknowledgment.
  - Listening for Signals. There are gaps in the official reporting, e.g., individual shots were not recorded in mass vacc Other countries have sought out reports of bad side effects and reached conclusions the U.S. has not.
  - Pervasive Misinformation. The rise in the anti-vax movement has made it difficult ... to candidly address potential side effects.
  - Several fascinating individual cases are noted in some detail. (R 34 23); two follow-ons (R 34 24)
- Could the Covid-19 Vaccines Have Caused Some People Harm? (R 34 25); Ex-CDC Director Dr. Robert Redfield Says It's High Time To Admit Significant Side Effects of COVID-19 Vaccines (R 34 25); An Object Lesson From Covid on How to Destroy Public Trust: Officials should have told us what they knew, or at least leveled with us about what they didn't know. (Zeynep Tufekci) https://www.nytimes.com/2024/06/08/opinion/covidfaucihearings-health.html [split] (R 34 30)
- We Are Blowing the Fight to Contain Bird Flu (R 34 22)
- Bird Flu Shows That the U.S. Learned All the Wrong Lessons about Covid: Two years after H5N1 jumped to mammals, health officials don't seem to have a plan. (R 34 40)
- Earlier items: New CDC Study Shows Coronavirus Can Survive For Hours On Floors, Walls, Shoes (R 31 68,69); Coronavirus detected on particles of air pollution (R 31 74); 'No evidence' that recovering from Covid-19 gives people immunity, WHO says (R 31 74,76); 'Rule of 48' redux concerning airborne spread of pathogens, a reminder with wide applicability to all research (R 32 69)
- Regulation: Masking the CoVID-19 problem (R 31 65,67,68); CDC loosened mask guidance to encourage vaccination – it failed spectacularly (R 32 70); California virus-fighting efforts hampered by data delays (R 32 18); Expired certificate contributed to undercounting of Calif. COVID cases (R 32 20); As U.S. Prepares to Ban Ivermectin for Covid-19, More Countries in Asia Begin Using It (R 32 87) The CDC Isn't Publishing Large Portions of the Covid Data It Collects (R 33 07); Dr. Birx ADMITS She 'Knew' COVID-19 Vaccines 'Were Not Going to Protect Against Infection' (R 33 35-39)
- Integrity relating to vaccines and care: Criminals have stolen nearly $100 billion in Covid relief funds, Secret Service says (R 33 01) A magnet for rip-off artists: Fraud siphoned billions from pandemic unemployment benefits (R 33 21); Estimated $163-billion from pandemic unemployment benefits were misspent or stolen (R 33 21); ID.me made baseless pandemic fraud claims to win contracts, Congress says (R 33 54); The more you submit, the more we get paid: How Fintech fueled COVID aid fraud (R 33 56) Florida surgeon general fudged data for dubious COVID analysis, tipster says (R 33 63); How a Big Pharma Company Stalled a Potentially Lifesaving Vaccine in Pursuit of Bigger Profits (R 33 92); Dana-Farber Cancer Institute has retracted 7 studies amid controversy over errors (R 34 16)
- Remediation: Coronavirus: Robots use light beams to zap hospital viruses (R 31 64); MIT Will Post Free Plans Online for an Emergency Ventilator That Can Be Built for $100 (R 31 64); MIT-based Team Works on Rapid Deployment of Open-source Low-cost Ventilator (R 31 64,65); Measurement units risk in those Open Source ventilators? (R 31 65); Error rates and CoVID-19 antibody tests (R 31 68); Getting Back To Normal: Big Tech's Solution Depends On Public Trust (R 31 68) [Is it even possible for what was once 'normal' ??]; The world after coronavirus (R 31 69,70)
- Logistics and the Supply Chain: To Understand the Medical Supply Shortage, It Helps to Know How the U.S. lost the lithium battery (R 31 72); Risks of supply-chain threat sharing (R 32 24)
- Disinformation and hoaxes: FTC, FCC crack down on coronavirus robocall scams, 132M calls/day (R 31 66); Tokyo firm urges caution against surge in coronavirus-related disinformation on April Fools' Day (R 31 64); Coronavirus Rumor Control (R 31 68); Commissioner of FDA admits he provided false information about COVID-19 treatment (R 32 23); Just 12 people are behind most vaccine hoaxes on social media (R 32 69); Reddit CEO rejects call for a crackdown on coronavirus misinformation (R 32 85); FOX News' Tucker Carlson defends making and selling fake covid vaccine cards (R 32 87); Surgeon General Demands Data on COVID-19 Misinformation From Major Tech Firms (33 08)
- Reactions, Protests, and Retaliations: Broadband engineers threatened due to 5G coronavirus conspiracies (R 31 65); A viral email about Coronavirus had people smashing buses and blocking hospitals. (R 31 60); Man who breached coronavirus stay-home notice stripped of Singapore PR status, barred from re-entry (R 31 60); Breast cancer patient attacked by violent anti-mask protest outside Los Angeles clinic (R 32 78)
- Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers (R 34 21)
- Computer Modeling: Mathematics of life and death: How disease models shape national shutdowns and other pandemic policies (R 31 64,65); Risks of extrapolation (R 31 64); David Reed comment on models (R 31 65); *Pandemic drone* test flights are monitoring social distancing (R 31 72); The Untold Story of

the Birth of Social Distancing (R 31 73); The illusion of certainty (R 31 73); Schools Adopt Face Recognition in the Name of Fighting Covid (R 32 36); Artificial intelligence model detects asymptomatic Covid-19 infections through cellphone-recorded coughs (R 32 37); AI flunks COVID test (R 32 80); CoVID and security awareness training (R 32 36); Why experts urge caution in using covid risk and tracking tools (R 32 38);; Traffic Analysis and Herd Immunity (R 32 77-78); The COVID testing company that missed 96% of cases: Northshore Clinical Labs in Nevada (R 33 21) [Numerous politically motivated items not included in RISKS, and thus not included here. PGN]

- Economic and Social Issues: The Economic Ramifications of COVID-19 (R 31 62); Covid-19 is nature's wake-up call to complacent civilization (R 31 63); Covid-19: *Nature is sending us a message*, says UN environment chief (R 31 63); Risks of Ostracizing (ostrichizing with your head in the sand?) Yourself: Many things are interdependent with others (R 31 64); Russia's Planned Coronavirus App is a State-Run Security Nightmare
  (R 31 65); Why human brains are bad at assessing the risks of pandemics (R 32 26); 463 people's COVID benefits accidentally sent to one of them (R 33 22); Children's rights violations by governments that endorsed online learning during the Covid-19 Pandemic (R 33 24)
- Privacy: Privacy Cannot Be a Casualty of the Coronavirus; **should have been textitmust be.** (R 31 66); UK government using confidential patient data in coronavirus response (R 31 68); How Coronavirus Is Eroding Privacy (R 31 68,69); Israel stops using phone tracking to enforce COVID-19 quarantines (R 31 72); Apple, Google announce new privacy protection rules for contact tracing apps (R 31 79); Microsoft says the pandemic argues for a federal privacy law (R 31 70); The iOS Covid app ecosystem has become a privacy minefield (R 32 38); CDC call for data on vaccine recipients raises alarm over privacy (R 32 40).

Conclusions

This collection of riskful items related to health-care is quite long, and yet is only a sampling of the RISKS archives. Many the total archival risks cases are indirectly also relevant here. However, subsets that are considered here suggest some conclusions and recommendations of what needs to be changed, fixed, or controlled in the future:

- We need greater emphasis on developing manageable and easily used systems and subsystems that are significantly more trustworthy than what we have today.
- We need more emphasis on evidence-based research that identifies and removes flaws, or demonstrates their absence.
- We need more sensible procedures with pervasive oversight and stringent enforcement where the risks are greatest.
- We need to systematically eschew false claims, unsupported beliefs, bogus conspiracy theories, and public-relations hype that suggests AI is the answer to all problems – and that technology is the solution to inherently nontechnological problems.
- We need to protest against simple-minded political and legislative measures that are iatrogenic (i.e., worse than the malady), unnecessarily costly, and in reality over-complicating or overly simplistic, in the sense of the Einstein Principle noted in my introduction.
- Last but not least, any attempt to pursue holistically motivated healthcare must face a variety of nontechnological issues – e.g., socio-economic, geo-political, religious, and even age-old customs maltreating women – that are contrary to the principles in which many of us believe, such as equality, liberty, and justice for all, especially as this relates to healthcare.

References

[1] Nancy Leveson has a series of books on human safety, each in succession wrapping the readers' arms more closely to the enormous complications that must be dealt with. She is a close colleague, and her work is a hugely important resource for the technological aspects of safety. Her most recent books and research papers are enumerated on her website, and speak for themselves. http://sunnyday.mit.edu/.

[2] My own book reflects a desire to look at past and recurring problems holistically: *Computer-Related Risks*, Addison-Wesley and ACM Press, 1995. It considers trustworthiness as an overarching requirement that encompasses security, reliability, safety, survivability, and other -ilities in a total-system integrative way. The tragedy is that almost everything negative described in the book is still happening today, and that most of the desired remediations have basically been ignored by system developers and nations – they are not paying attention to reality. However, we must remember that technology alone is not the answer – although today's technology is pitifully inadequate, especially in supporting systems with critical requirements for trustworthiness.

[3] A 1989 report by my colleagues JohnM. Rushby and R. Alan Whitehurst was prescient: Formal verification of AI software. It considered using formal analysis of AI1q systems to increase their assurance. (See Final report for NASA, SRI Computer Science Laboratory, February 1989: https://www.csl.sri.com/papers/csl-88-7/.) In retrospect, that report has become extremely relevant today – in light of the enormous lack of assurance in today's AI feeding frenzy of low-assurance commercial AI systems (e.g., see Bruce Schneier, AI and Trust, 2023: https://www.belfercenter.org/ publication/ai-and-trust). Fortunately, intelligent AI researchers have been getting that message more readily than commercial AI providers.

[4] Our SRI Computer Science Lab has for several decades been exploring the application of formal mathematical logic to the biosciences. I firmly believe that their approach holds enormous progress for the linkages (e.g., integrating the immune and neurological systems) that are needed for a truly holistic approach to healthcare. Carolyn Talcott has been leading that effort with our Division President Patrick Lincoln cheering her on. Sylvan Pinsky is also contributing remotely as a still-active alumnus. In collaboration with biologists, this ongoing project develops evidence-based formal models of cellular response to external signals (drugs, stress, messages from other cells). Formal analysis tools support using these models for in-silico experiments, explaining and predicting side-effects of drugs, understanding host-pathogen interactions, among other things. The project has made available online a database of experimental findings curated from published works that provides supporting evidence for the models: http://www.datum.csl.sri.com There is also a growing literature of work by others in this direction as well.

[5] For those readers who need more hope for the future, I would suggest visiting our CHERI website in Cambridge UK:

https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/ CHERI has the potential to be the most trustworthy hardware-software clean-slate general-purpose system architecture ever, and it is beginning to be recognized as a unique breakthrough. CHERI is a joint effort between SRI and the University of Cambridge, under development and evaluation since 2010. It has commercial manifestations (e.g., experimental CHERI-Arm-Morello boards, whose specifications have been formally proven to satisfy critical security properties), and open-sourced CHERI-RISC-V, and CHERI-FreeBSD with two real-time operating systems, plus recent support from Codasip. The White House has recently reported that CHERI is the only current system providing extensive memory safety. On the other hand, the devil is always in the details and even the most secure hardware does not imply the most secure software.

[6] This contribution ends with a very personal note. My daughter Helen has a practice of Oriental Medicine, and is currently undergoing some intense detox programs attempting to remove several forever chemicals and other immune-system detractors left over from 30-plus years of chronic Lyme Disease. I have come to the conclusion that the missing links today are the holistic ones – for example, between the immune system and the nervous system, both of which are together impaired in Helen. For example, as a result of functional medicine, her glyphosate level was cut dramatically, as were her mercury, lead, palladium, malathion, Round-Up components, and lots more. The list of toxicities before the detox program was considerable. (The Palladium toxicities are still much too high.) However, her knowledge, discipline, and determination – and commitment to as full a recovery as possible – have been daunting, and are a great source of encouragement. Unfortunately, this treatment is well outside of standard-care practices.

[7] A relevant book Helen shared with me is by Sara Szal Gottfried, *The Autoimmune Cure*: https://www.saragottfriedmd.com. This is a holistic book (her fifth) – heavily annotated, with an outstanding bibliography. It seems to be close to where I think integrative healthcare needs to go in the future, despite the economic arguments for not going outside of an AMA box that does not actually exist. The possibilities of everything related to healthcare still seem to be open-ended with respect to diagnosis, treatment, and the end-game – also open-ended relating to new risks from both new and old approaches. Many of them may be related to our immune systems and our overly toxic environments.

[8] Holistically, the possibilities of everything related to healthcare still seem to be open-ended with respect to diagnosis, treatment, and the end-game -- also open-ended relating to new risks from both new and old approaches. Many of them may be related to our immune systems and our overly toxic environments. In retrospect, our holistic approach discovers that many of the pieces are interwoven. Thus, we come again to the observation that I noted in the introduction: there never was a box, and that trying to enforce it was a gigantic mistake that is hindering efforts to reform the healthcare systems.