

The Healthcare RiskOps Manifesto

"Committees are, by nature, timid. They are based on the premise of safety in numbers; content to survive inconspicuously, rather than take risks and move independently ahead. Without independence, without the freedom for new ideas to be tried, to fail, and to ultimately succeed, the world will not move ahead, but rather live in fear of its own potential"

Ferdinand Porsche

And you may ask yourself, "How do I work this?"
And you may ask yourself, "Where is that large automobile?"
And you may tell yourself, "This is not my beautiful house."
And you may tell yourself, "This is not my beautiful wife."

David Byrne

The End is Near

"People of Earth, hear this!"

A specter is haunting healthcare.

And we've got work to do.

It's about challenging the old assumptions of managing risk because nothing has changed. Yet, everything has changed.

It's about heralding a new vision because the old one doesn't work.

Change creates opportunities.

Change drives outcomes.

And healthcare needs secure outcomes. Healthcare risk needs change.

We must challenge assumptions: identity, role, purpose, place, power.

Change built on strong beliefs that will upset the status quo.

We don't care. We are focused on moving the industry forward.

Le risque est avant-gardiste.

Futurism. Vorticism. Dada. Surrealism. Situationism. Neoism.

Risk the Elephant. Uncaged.

Risk is Nazaré. It's a red balloon.

Risk is sunflower fields. And fire on the mountain.

Risk guides the first decision. It's as old as Eden.

Fight.

Or flight.

Risk is nucleotide. To ego. It's DNA, linked to personality. Purpose.

Risk is an Indian Chief heading from Indio to the Joshua Tree Inn. In 40 mph wind gusts. It's AMZN at \$1,200 per share. Bitcoin at \$26,000. It's going all in on number 23. It's calculated. It's intuitive. Most of all, risk requires action.

This is the end, beautiful friend. THE END.

One - Overthrow the Status Quo

Throw it all away and start over.

Risk without action is mental hijinx.

Risk in this society being, at best, an utter bore and no aspect of society being at all relevant. But, let's not start shooting at soup cans.

Let's be booed.

Loudly. BAMN!! (By Any Means Necessary).

The opposite of love is not hate. It is indifference.

Of risk? (hint: It's not safe.)

The opposite of risk is impossibility.

Without risk, there is no possibility.

Chance is a coin flipping in a casino.

Let's stop leaving outcomes to chance.

Let us end with our ASSUMPTIONS:

- Only some applications and services are a risk to our organization.
- We can only afford to assess critical and high risk vendors and products.
- Assessing risk at a point in time is sufficient to protect us.

These will not do.

Two - The Business of Risk is Business

Risk is not a technical issue.
Risk is not a process issue.
Risk is not a resource issue.

Risk is a business issue. The business of risk is business.

A business runs on vision, mission, values, strategy, execution.

The lifeblood of business is culture. Transparent. Thriving on trust.

Culture eats strategy. All. Day. Long.

Care operates in a culture of risk. Triage code. Risk code.
Risk the side effect for the cure.
Every second saves more heart muscle.

Information is the "heart muscle" of healthcare.

Every second counts.

- When protecting patient privacy;
- When treating a virus;
- When diagnosing cancer;
- When saving a sister; when saving a brother.

Cyber risks threaten the heart muscle of care.
Cyber risks threaten patient data.
Cyber risks threaten care operations.
Cyber risks threaten patient lives.

Continuously. Day & Night.

Risk never sleeps. It hides patiently in infusion pumps, quietly lurks on hospital networks and in the cloud, and says good morning at the end of every shift. Risk doesn't take vacation. Or call in sick.

But we can't protect what we can't see. To fight risks, we need transparency. Transparency is the enemy of risk.

These beliefs define who we are and drive why we are. They drive us to create a better way for reducing risks - one that is transparent, immediate, and always on.

Three - The Death of Questionnaires

"To admire an old picture is to pour our sensibility into a funeral urn instead of casting it forward with violent spurts of creation and action. Do you want to waste the best part of your strength in a useless admiration of the past, from which you will emerge exhausted, diminished, trampled on?"

- F. T. Marinetti, [The Futurist Manifesto](#)

Power users corrupt. Influence of teams incites.

We are all just prisoners here, of our own (medical) device.

Let us break free of the virtual bars that constrain us -

row row

| | |
|--------|--------|
| column | column |

row row

Spreadsheets, documents! Truly identical in their unstructured juxtaposition of data without relationship. Boardrooms or zoom sessions where we present side by side with colleagues and agendas we do not know. Reciprocal ferocity of compliance, finance, IT, and the business; challenging one another using the same spreadsheet with formulas and color. To assess risk once a year, critical and high, as one does using email and phone calls, that time could allow! We can even imagine remediations tracked to a conclusion! But to assess risk, with fragile tools and anxiety every day, that we cannot admit!

Do you want to lose data?
Do you want to lose patients?
Do you want to lose reputation?

Four - Risk Management is People is Process is Automation

People process risks every day. (Say that three times fast).

We risk our lives when getting dressed, crossing the street, driving in cars, shopping, climbing, running, sitting, flying, eating, etc.

Risk is as human as breathing.

(When's the last time you thought about breathing?)

Say it again: the BUSINESS of RISK is BUSINESS.

The complexities of business demand people, processes and technology.

The complexities of risk require people, automation, and actionable insight.

Spreadsheets are not working. Legacy risk technologies are not working. Slow and costly certifications alone are not working.

Risk programs:

- without automated remediation, validation & accountability provide an illusion of safety;
- without mapping an inventory of vendors to PHI & BAAs result in critical gaps to coverage;
- without metadata struggle to find actionable insights;
- without vulnerability alerts are frozen in time with old data;
- without early risk data put legal & purchasing at a disadvantage;
- without a risk operations command center perpetuate the siloed approach to risk in healthcare today.

Imagine a world in which we trust one another. Completely.

Come on providers now, smile on your vendors, everybody get together, and reduce healthcare risks right now.

Five - Innovation, Move Me Brightly

We calculate risk using likelihood, impact, costs.

We collect evidence. Trust but verify. We document risks in registers.

We rationalize risk- vs. control-based frameworks.

We plot and report risks in quadrants. Colors flashing.

Sometimes we get it right. Oftentimes we get it wrong by:

- a little: "The incident cost 2.5% more than we predicted."
- a lot: "We captured the risk of a pandemic occurring in 2020; however, likelihood was very low."

And every year, we apply the same old assumptions.

And every year, breaches of patient data continue to rise.

And every year, we buy more security. And (try to) hire more people.

And every year, silos of managed risk develop with tall & thick walls.

And every year, the attack surface grows larger from new technology.

And every year, the attackers get smarter. More sophisticated. Brutal.

It's no longer just about protecting data. Lives are at stake.

It's about the impact on business operations.

It's about ransomware closing down clinics and practices.

It's about patient safety. It's about protecting lives. But we resist innovating in the one area that may actually move the needle on risk avoidance.

Innovation alone is not enough.

It won't get us to where we need to be.

We need to change the way we manage risk. We need to eliminate silos.

We need to move risk from a report to a command center.

We need to pull pages out of the DevOps and SecOps playbooks.

We need to transform risk in a way that combines compliance, security, and operations integrated across the enterprise.

Let's move the needle together.

Six - Let's See Action

Connecting risk with operations is the only way out of the theoretical - this technical quagmire - and into the practical.

We must move away from managing risk to controlling risks.

- No business but in risk
- No management but in operations
- No protections but in controls

A foolish prediction is the hobgoblin of unprepared minds, adored by statesmen and executives and divines.

Exchange likelihood for control-based vigilance!

Reimagine risk from how it could be to why it will be!

If the doors of transparency were opened, risk would appear to the business as it really is, avoidable. Or something like this.

We are pretty bad at assessing probabilities. We're overconfident in our estimates and don't know how to calibrate probabilities.

And yet, calculating and plotting risk drive most risk programs.

Risk considerations at the earliest, and ideally every, stage of planning and development. Today, risk is siloed throughout the health system. It needs to move away from tactical silos of data collection where clinicians, biomed, IT risk analysts, architects, and operations teams work independently.

We need to bring everyone together, working as a single, cohesive team that can respond better and faster to risks that face patient care delivery and the business.

We need to streamline workflows; consolidate and integrate processes; turn data into actionable insight; leverage standardization and best practices; implement effective tooling and automation at the heart of the process.

Seven - Hello Risk, Meet Operations

There is a new risk movement underway in healthcare.

It's called RiskOps.

RiskOps integrates risk, including cyber risk, with the enterprise.

RiskOps is a thriving network: it covers clinical, strategic sourcing, research, IT, security operations, and secure system development.

RiskOps takes a vendor and product lifecycle view, providing accountability, visibility, and action at every stage: contracting, purchase, configuration, implementation, usage, reassessment, renewal, updates (patch, minor or major), and termination.

RiskOps is a natural complement of and extension to SecOps and DevOps.

RiskOps reduces risks to care and overall business by identifying risks and controls as early as possible:

- Risks found early in the contracting process enable protective language in agreements;
- Risks found early in the assessment process map to remediation obligations.

RiskOps delivers better ROI as automation, shared responsibility and coordinated actions reduce the need for more staff while increasing the quality and output of all teams.

RiskOps makes everyone a "risk champion" of the business. It defines clear roles and responsibilities, enhancing collaboration and building confidence with better reporting and overall accountability.

RiskOps is a viral network of peers, connecting with a common vision: take risk out of healthcare.

With a RiskOps network, health systems can reduce risks of an incident occurring or the impact of an incident (e.g. data breach, ransomware attack, clinical disruption, patient harm, etc.).

Eight - Where Do We Go From Here: Alone or Together?

We are convinced that the simplest approach will prove to be the most effective – the solution to healthcare risk is to reduce it directly by a now widely discussed measure: the network.

This may be difficult to understand, but there are others struggling just like you.

We want to help.

We stand with you on the border
of innovation and risk.

We stand with you on the edge
of evolution and revolution.

(The stakes are too high to play it safe.)

No matter, we keep having these crazy dreams: what if we could take risk out of healthcare? In these dreams anything is possible. Ideas freely flow. Patients and their data are protected. Always. And innovation is available to everyone. Risk free.

In this world, everyone is connected & all risk is transparent. Which means the silos, the walls have to come down by any means necessary. Which means bridges must be built. By every means necessary. We need to bring the walls down! We've had enough of walls. Let's bring on the bridges of viral connectivity. The power of the network is absolute. It leverages collective wisdom so you don't have to learn

every lesson yourself.

Together, we identify and remediate risks based on real-time data. We extend the perimeter, pushing the risk horizon out further than we thought possible. Together, we serve as a beacon, an early warning to all vulnerabilities. All risks.

You don't have to go it alone: Together is how it should work. Together is how it does work.

Are you ready to join us?

After the Flood

A vision for the future of risk in healthcare in 4,000 A.D.,

NO ATTACKS

NO INCIDENTS

NO VULNERABILITIES

NO BUGS

NO

THERE WILL BE HARMONY

PLACE

PURPOSE

HEALTH

LIFE

Destroy the past, embrace the future.

Welcome to RiskOps.

- THE BEGINNING -

Footnote: This was written by someone who deeply cares about healthcare and strongly believes we can eliminate risks if we (courageously) work together. References obscure or otherwise are "borrowed" with thanks and deference: The Youngbloods, R. Creely, W.C. Williams, F.T. Marinetti, The Eagles, W. Blake, V. Solanas, C. Olson, Dylan, MLK, Garcia, and other literary and music references that fight for attention. To learn more: www.censinet.com/riskops

