CYBERSECURITY READINESS PODCAST SERIES

# Episode 112

## When the EHR Goes Dark: Patient Safety Meets Cybersecurity Governance

*with Dr. Mark Yoffe, MD, Board-Certified Internist and Cybersecurity Professional*

| | |
|---|---|
| **Host** | Dr. Dave Chatterjee, Duke University |
| **Guest** | Dr. Mark Yoffe, MD, Board-Certified Internal Medicine Physician and Cybersecurity Professional |
| **Topic Focus** | Patient Safety During Cybersecurity Incidents — Clinical Resilience, Professional Ownership, and AI Governance in Healthcare |
| **Podcast Portal** | https://www.cybersecurityreadinesspodcast.com/ |

## Summary

In Episode 112 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Dr. Mark Yoffe, a board-certified internal medicine physician who has also built deep expertise in cybersecurity, to examine a question most healthcare organizations have not fully reckoned with: what actually happens to patient care when the electronic health record goes dark. Dr. Chatterjee opens with a sobering scenario — a nurse unable to confirm whether a cardiac patient's anticoagulant was administered overnight because the EHR is degraded, resulting in a double dose — and notes that variations of this scenario have occurred during real ransomware attacks and extended downtime events, even though most healthcare organizations have not mapped which clinical dependencies fail first or pre-assigned who decides what when systems cannot be trusted.

Dr. Yoffe, who bridges internal medicine and information security, explains how the same words — confidentiality, integrity, availability — carry weight in both professions, and walks through what actually happens on the floor when digital systems go down: clinicians shift from an "information push" environment, where alerts and updates come to them, to an "information pull" environment, where they must actively seek out information, usually from other humans, because the chart itself can no longer be trusted. The conversation moves through the compensatory mechanisms hospitals fall back on — written charts, physical examination, and the judgment clinicians rely on when information is incomplete — and into how security professionals can translate technical metrics like uptime into the language leadership and clinicians actually understand: patient care and mission impact.

Analyzed throughout the episode through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) Framework, the discussion also tackles the distinct governance challenge posed by AI in healthcare — a tool that, unlike a scalpel or a hammer, is never quite the same tool twice — and closes with a shared conviction that preparation is not a once-a-year tabletop exercise but a daily discipline that determines how clinicians and organizations perform when systems, and stakes, are at their worst.

## Discussion Highlights

### The Double-Dose Scenario: When the EHR Goes Dark and Patient Safety Hangs in the Balance

Dr. Chatterjee opens the episode with an illustrative scenario: a cardiac patient's overnight anticoagulant dose cannot be confirmed because the electronic health record is degraded and there is no paper backup, so both the overnight and the incoming nurse administer the dose, resulting in a double dose. He stresses this is not hypothetical — variants of this exact failure mode have occurred during actual ransomware attacks and extended downtime events — yet most healthcare organizations have not practiced for it, mapped which clinical dependencies fail first, or pre-assigned who makes what decisions when systems cannot be trusted.

> *A nurse cannot confirm whether a cardiac patient's anticoagulant was administered overnight. The patient receives a double dose, and this is not hypothetical. Variants have occurred during actual ransomware attacks and extended downtime events.*
>
> **— Dr. Dave Chatterjee**

## From Push to Pull: How Clinicians Adapt When the Network Goes Quiet

Dr. Yoffe describes what actually happens on the floor when digital systems fail: the first thing clinicians notice is quiet — the EHR stops making noise, phones ring less, and the steady stream of alerts and updates disappears. That quiet is initially reassuring, he explains, but it marks a shift from an "information push" environment, where information comes to the physician because of the many people and systems working behind the scenes, to an "information pull" environment, where clinicians must go find information themselves. Because digging through a degraded chart is unreliable, clinicians learn quickly to rely more heavily on direct communication with other humans.

> *So clinicians learn very quickly to transition from an information push environment to an information pull environment... and when we do that, we tend to rely more on humans.*
>
> **— Dr. Mark Yoffe**

## Bridging Two Languages: Translating Security Metrics Into the Language of Patient Care

Dr. Yoffe argues that cybersecurity professionals working behind a screen can lose sight of the real-world, highly leveraged consequences of their work, and that communicating with leadership requires translating technical criteria into language leadership understands. Using uptime as an example — a cybersecurity professional citing a 98.5% uptime against a 99% industry standard is making an IT argument, not a mission argument — he explains that leaders understand patient care and access to treatment, so framing the same gap in terms of its impact on care delivery is far more likely to get their attention and support.

## Commitment, Preparedness, Discipline: Why Healthcare Makes the Case for Itself

Dr. Chatterjee connects the discussion directly to his Commitment–Preparedness–Discipline (CPD) Framework, noting that the healthcare context makes the case for commitment far less of a hard sell than in other industries: when cybersecurity governance is neglected, patient care suffers and, in the worst cases, patients can die. He walks through how each pillar applies — commitment as leadership's resolve to treat cybersecurity as a strategic priority rather than a compliance checkbox, preparedness as the depth of people, process, and technology marshaled to detect, respond, and recover, and discipline as the consistent, day-to-day execution of practices like patch management, access controls, and continuous monitoring.

> *If you are not actively committed to cybersecurity governance, cybersecurity best practices, patient care will be affected. Patients could die, so the consequences are drastic.*
>
> **— Dr. Dave Chatterjee**

## Falling to the Level of Instinct: Why Daily Cyber Hygiene Beats the Annual Tabletop

Dr. Yoffe draws an analogy to martial arts: in a real fight, a practitioner does not recall the formalized kata, they fall back on instinct — whatever they have rehearsed repeatedly. The same is true of cybersecurity discipline, he argues; someone who reuses a bank password for a streaming account signals a personal security posture, just as an organization's daily habits, not just its annual tabletop exercises, determine how it performs under real stress. He also reframes the communication gap between frontline staff and leadership as a bridge to be built through two-way communication, rather than a one-directional handing down of decisions.

> *In stress situations, we fall to the level of our instincts.*
>
> **— Dr. Mark Yoffe**

## Governing a Tool Smarter Than Us: The Unique Challenge of AI Governance in Healthcare

Turning to AI-assisted clinical decision support, Dr. Yoffe explains why AI governance is conceptually unlike any governance challenge that has come before it. A scalpel or a hammer, once approved, remains the same tool indefinitely; AI is constantly learning and changing, so the tool being governed today is not the tool that existed yesterday. He also raises a second, more provocative challenge: AI, in some respects, is smarter than the humans meant to oversee it — a dynamic with no real historical precedent in governance and controls.

> *Is it even possible for a nine-year-old to govern a forty-three-year-old? Those are, I think, conceptually, two of the main challenges of even speaking about AI governance.*
>
> **— Dr. Mark Yoffe**

### Bidirectional Oversight, Unidirectional Ownership: Why AI Will Never Own the Decision

Dr. Chatterjee and Dr. Yoffe explore AI-enabled diagnostic tools, such as X-ray reading, and AI-assisted, less invasive surgical procedures, and the governance tension these create: even as AI systems become more capable, human oversight of AI output remains essential, and Dr. Yoffe suggests the relationship may increasingly run in both directions, with AI in some sense also overseeing human decision-making. What does not change, he stresses, is professional ownership — a licensed professional cannot delegate accountability for a decision to a technology or to anyone outside their license, no matter how capable the tool. Dr. Chatterjee ties this back to the CPD Framework's commitment pillar, which calls for clear assignment of ownership and responsibility alongside the resources needed to carry it out.

> *AI is not going to own the decision. It's always going to be the professional who owns the decision.*
>
> **— Dr. Mark Yoffe**

### Closing Reflections: Preparation as a Daily Discipline, Not an Annual Event

Dr. Yoffe closes by reiterating that preparation is not a matter of what happens during a periodic tabletop exercise, but of the habits formed in day-to-day clinical and organizational life — the same commitment, preparedness, and discipline that carry an organization through the moments when systems are degraded or compromised. Dr. Chatterjee reinforces that commitment, preparedness, and discipline are intrinsically connected, and that cybersecurity and AI governance must be integrated with an organization's broader strategic goals rather than siloed off or fully outsourced to a security team, since when quality of care suffers, the entire organization is affected.

> *Preparation is key, and the discipline, the habits that we form in our daily lives, but also in a company life... are what prepares us to act in situations where systems are degraded or things are compromised.*
>
> **— Dr. Mark Yoffe**

### The CPD Framework Applied to Healthcare Cybersecurity Governance

Dr. Chatterjee maps his Commitment–Preparedness–Discipline (CPD) Framework directly onto the healthcare cybersecurity and patient-safety themes discussed throughout the episode.

| CPD PILLAR | APPLICATION TO HEALTHCARE CYBERSECURITY GOVERNANCE |
|---|---|
| **COMMITMENT** | Leadership must treat cybersecurity as a strategic priority tied directly to patient safety, not a compliance checkbox — assigning clear ownership and responsibility, and empowering people with the resources and decision-making authority needed to carry it out. |
| **PREPAREDNESS** | Organizations need the people, processes, and technology to detect, respond to, and recover from degraded or compromised systems, including mapped clinical dependencies, rehearsed downtime playbooks, and pre-assigned decision authority for when systems cannot be trusted. |
| **DISCIPLINE** | Consistent, day-to-day execution — patch management, access controls, security awareness training, penetration testing, and continuous monitoring — determines how clinicians and organizations actually perform under stress, since people fall back on practiced habits, not formal training, in a real crisis. |

## Actionable Recommendations

| RECOMMENDATION | DETAIL |
|---|---|

| | |
|---|---|
| **Map Clinical Dependencies Before the Crisis Hits** | Identify which clinical workflows and decisions fail first when systems degrade, and pre-assign who is authorized to make which calls when the EHR cannot be trusted — rather than discovering this in the moment. |
| **Rehearse the Shift From Information-Push to Information-Pull** | Train staff for the moment systems go quiet: alerts and updates stop flowing automatically, and clinicians must actively seek reliable information from colleagues rather than assume no news is good news. |
| **Translate Security Metrics Into the Language of Patient Care** | When making the case to leadership, reframe technical metrics like uptime in terms of their impact on patient access to care and treatment, rather than presenting them as IT or compliance criteria alone. |
| **Build Daily Cyber Hygiene as an Organizational Habit, Not Just a Tabletop Exercise** | Recognize that people fall back on instinct under real stress; invest in everyday security practices and awareness so the default behavior in a crisis is the right one. |
| **Preserve Human Professional Ownership Over AI-Assisted Decisions** | Even as AI oversight of human decisions becomes more plausible, keep accountability for clinical and security decisions with licensed, responsible professionals who cannot delegate that ownership to a tool. |
| **Treat AI Governance as a Continuously Moving Target** | Unlike a one-time-approved device, an AI system keeps learning and changing after approval — build governance policies that assume the tool in use today will not be the same tool tomorrow. |
| **Extend Cybersecurity Awareness Beyond the Security Team** | Encourage clinicians and other non-security staff to build baseline security awareness relevant to their roles, so the entire organization — not just the security function — contributes to a stronger security posture. |
| **Apply the CPD Framework to Integrate Cybersecurity, AI Governance, and Organizational Strategy** | Use Commitment to assign clear ownership, Preparedness to build response capacity and rehearsed playbooks, and Discipline to sustain daily execution — aligned with the organization's broader mission rather than siloed off to a single team. |

## Time Stamps

| TIME | CONTENT |
|---|---|
| **0:02** | Introduction — Dr. Chatterjee's background and credentials |
| **0:49** | Host framing: the double-dose EHR scenario and episode stakes |
| **2:56** | Dr. Mark Yoffe's professional journey — bridging internal medicine and cybersecurity |
| **4:00** | COVID-19 as a driving force behind Dr. Yoffe's interest in information security |
| **5:14** | A further example of how degraded systems can affect patient safety |
| **6:47** | What happens inside a hospital during a ransomware attack |
| **9:40** | A patient's perspective: the stakes of information availability in critical care |
| **11:22** | Do hospitals rehearse downtime playbooks? Tabletop exercises in healthcare |
| **12:55** | Compensatory mechanisms — is a hospital paralyzed when systems go down? |
| **14:55** | What Dr. Yoffe wants healthcare and security listeners to take away |
| **17:11** | The CPD Framework introduced and applied to healthcare cybersecurity |
| **22:34** | The martial-arts analogy: falling to the level of instinct under stress |
| **24:43** | Communication effectiveness and the shift to AI governance in healthcare |

| | |
|---|---|
| **27:46** | Why AI governance is conceptually different from governing any prior tool |
| **29:55** | AI-enabled diagnostics and less invasive, AI-assisted surgery |
| **32:34** | Bidirectional oversight and the concept of professional ownership |
| **35:10** | Tying ownership and accountability back to the CPD Framework |
| **39:01** | Governance as the foundation for controls and mission execution |
| **39:49** | Strategic alignment — integrating cybersecurity and AI governance |
| **41:35** | Closing thoughts from Dr. Yoffe: preparation as a daily discipline |
| **42:33** | Special thanks and episode wrap-up |

## Memorable Quotes

> *A nurse cannot confirm whether a cardiac patient's anticoagulant was administered overnight... This is not hypothetical. Variants have occurred during actual ransomware attacks and extended downtime events.*
> **— Dr. Dave Chatterjee**

> *In stress situations, we fall to the level of our instincts.*
> **— Dr. Mark Yoffe**

> *AI is not going to own the decision. It's always going to be the professional who owns the decision.*
> **— Dr. Mark Yoffe**

> *Preparation is key, and the discipline, the habits that we form in our daily lives... are what prepares us to act in situations where systems are degraded or things are compromised.*
> **— Dr. Mark Yoffe**

## Disclaimer

The information contained in this summary is for general guidance only. The discussants assume no responsibility or liability for any errors or omissions in the content of this podcast. The information is provided on an as-is basis with no guarantee of completeness, accuracy, usefulness, or timeliness. The opinions and recommendations expressed are those of the discussants and not of any organization.

Dr. Yoffe's statements in the podcast remain his own. This written summary was prepared by the host and does not represent Dr. Yoffe's own words. Both are provided for general educational discussion only and are not intended to define, establish, or constitute an opinion on any standard of care.

Dr. Dave Chatterjee | dchatte.com | dchatte@gmail.com | linkedin.com/in/dchatte