BRINGING ORDR TO CHAOS

HIPAA/HITECH New Rules: More Than Just a Checklist

Use the latest rules as an opportunity to enhance security.

March 5, 2025

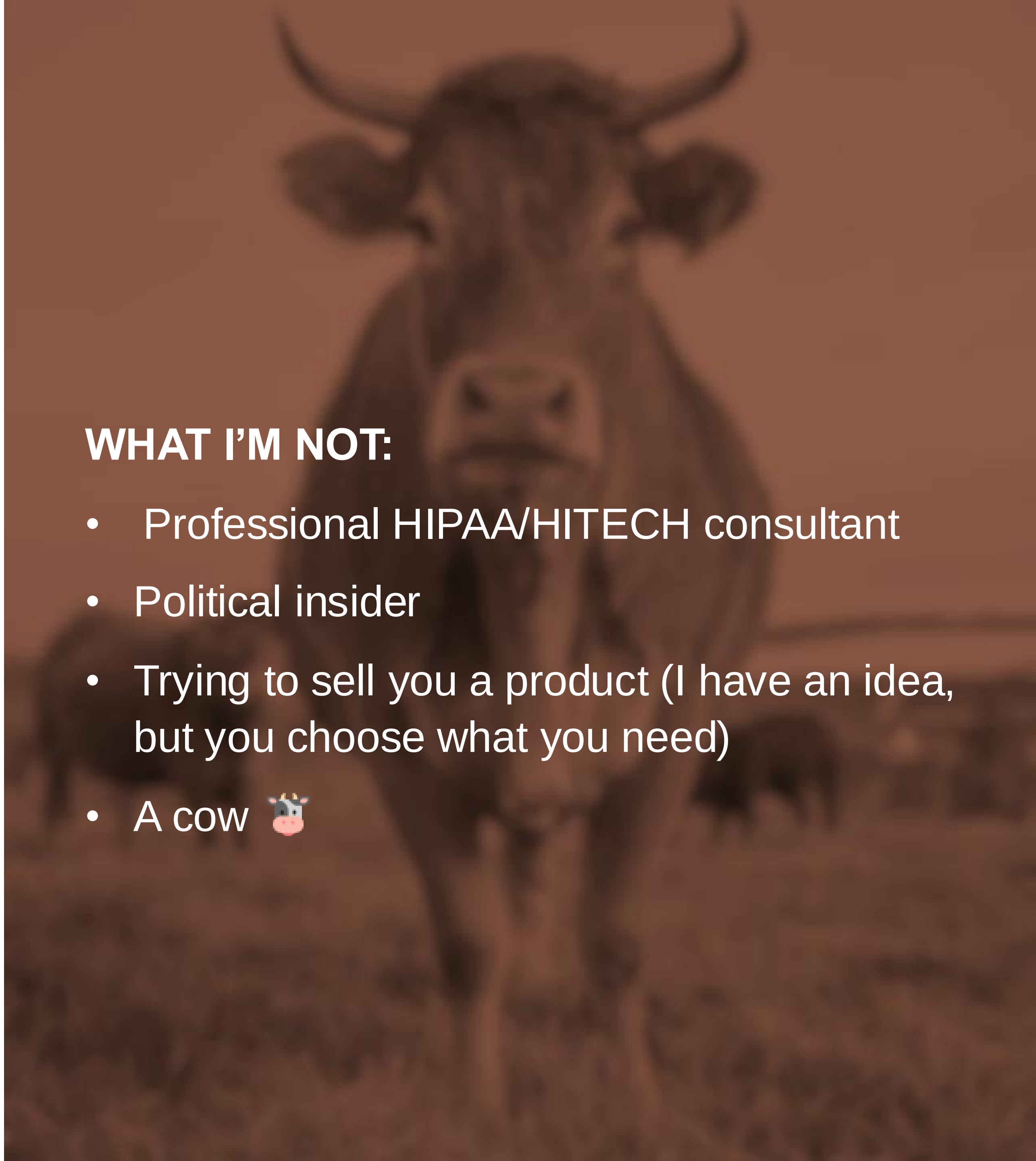
ORDR.NET

CHIEF HEALTHCARE OFFICER, ORDR

Wes Wright

WHO I AM:

- 20-year Air Force veteran: Korean linguist then CIO
- Scripps, Seattle Children’s, Sutter
- Imprivata and now ORDR!
- CHIME/HIMSS member since 1993



WHAT I’M NOT:

- Professional HIPAA/HITECH consultant
- Political insider
- Trying to sell you a product (I have an idea, but you choose what you need)
- A cow 🐮

What’s the Latest

- Released for comment (Jan 6) → Paused by Trump administration
- Once unpaused, compliance required in 180 days
- Industry opposition: CHIME, AHA, AMA, and others
- Reality check: Rules would improve healthcare security, but organizations are delaying action

Why Do They Matter

- **Similar to existing rules, but with enforcement teeth**
- “Addressable” controls now required (OCR enforceable)
- “You shall” replaces “You should”

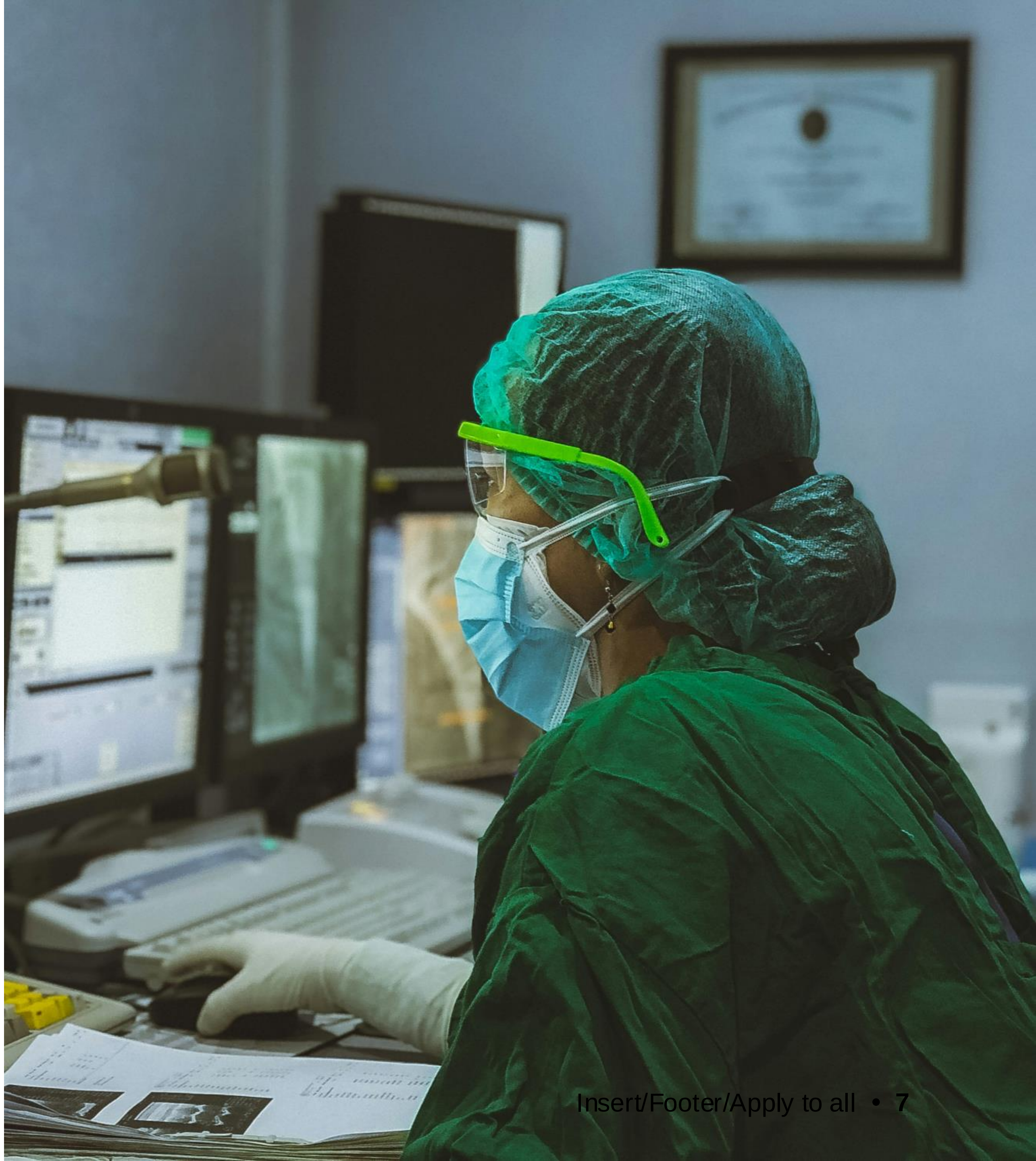
- **Clear rationale behind each rule**
- Explains "why" behind each rule with real-world examples

- **Preemptively addresses common objections**
- Includes **cost-benefit analysis** for internal buy-in (verify figures)

HIPAA/HITECH NEW RULES

Quick Impressions

- **It’s long – 450+ pages**, covering:
  - Administrative safeguards
  - Technical controls
  - Failure examples (justifying changes)
  - Cost-benefit analysis (shows immediate ROI)
- **Bottom line:** It’s all about **protecting ePHI**!



Top “Must-Do’s” for CTOs/CISOs

Map real-time ePHI flow

with full asset inventory (IT, IoMT, IoT, OT)

- **Monitor** vulnerabilities, installed software, users, & locations
- **Align with new rules**: Anything affecting ePHI must be mapped

Segment systems

clinical (ePHI) from non-clinical & other clinical systems

- **Isolate** critical systems to **reduce attack blast zones**
- **Example**: EHR & CV systems **must not share** network zones

Real-time vuln/patch status

Of every connected device within your organization

- **Ensure** compliance with CVE patching requirements
- **Prioritize remediation** based on asset risk & exposure

HIPAA/HITECH NEW RULES

Start with Inventory

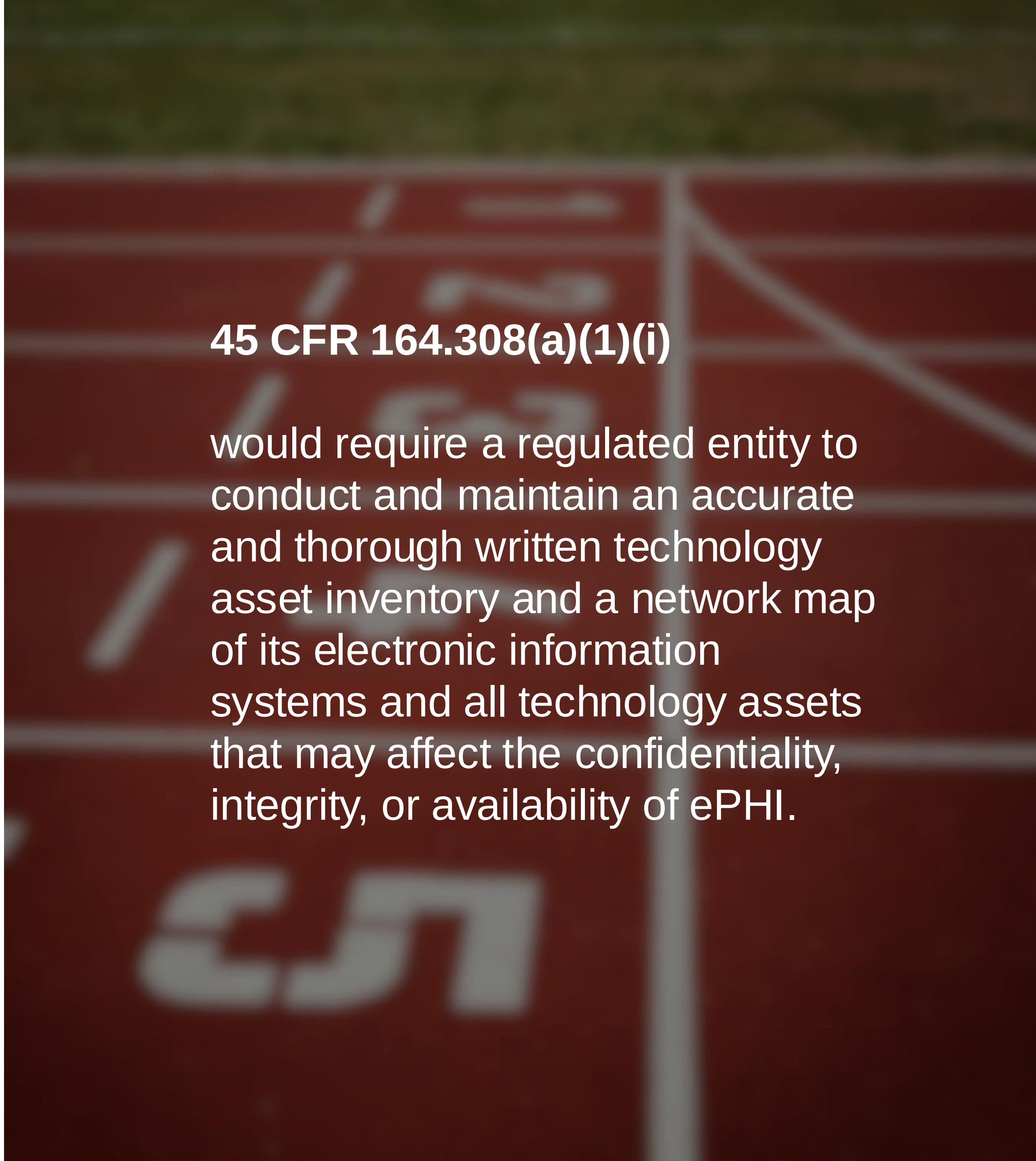
“While maintaining an accurate and thorough inventory of technology assets is not currently an explicit requirement of the Security Rule, it is clearly a fundamental component….”

ALL things in real time

Devices

- What they are
- Vuln/patch level
- Who owns it

People: Unique identifiers for both people and devices



45 CFR 164.308(a)(1)(i)

would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI.

HIPAA/HITECH NEW RULES

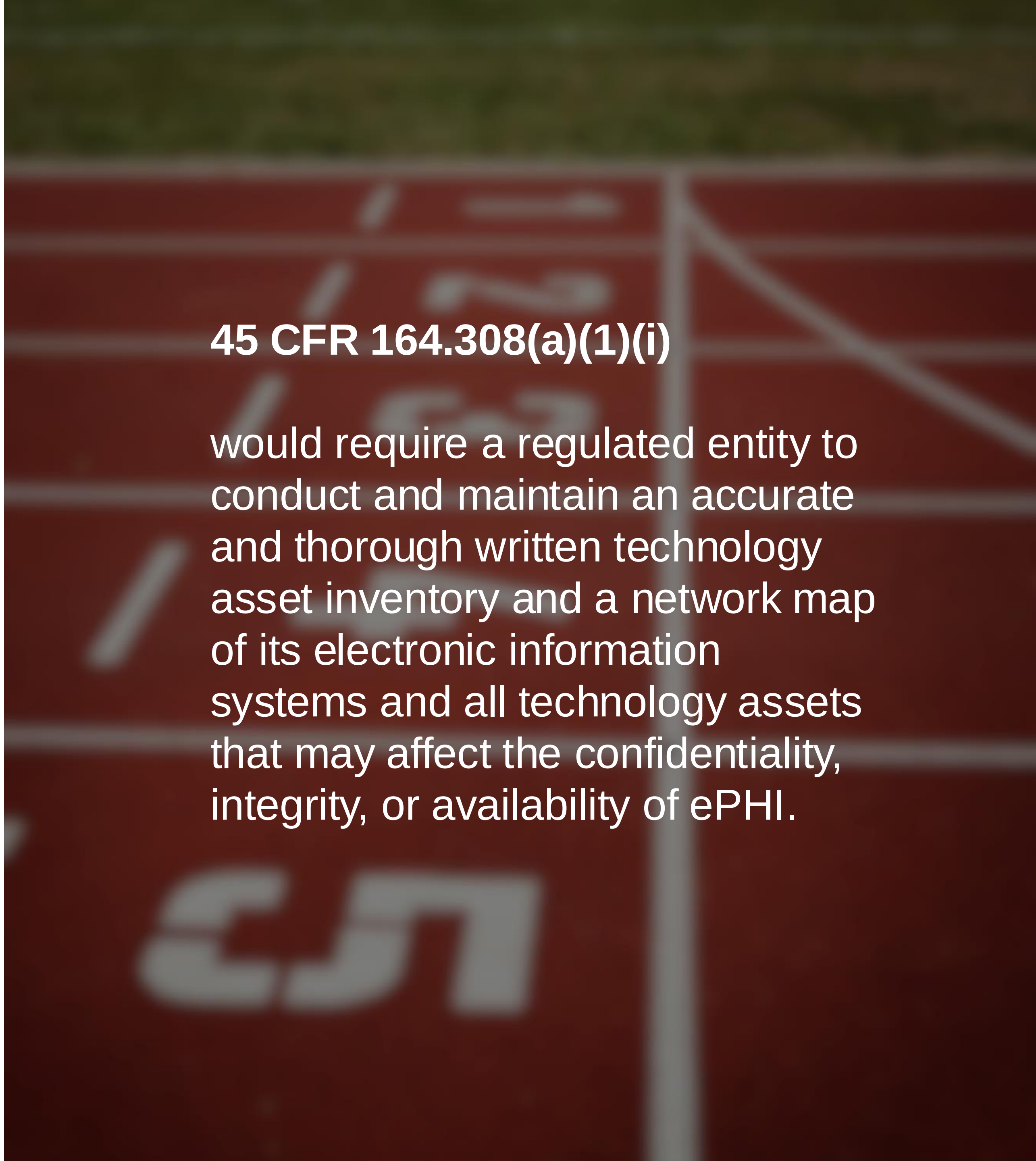
Start with Inventory

ePHI

Where is it?

How does it move within your organization?

- Where are the start/end points
- Which network gear does it go through
- Is it encrypted at all points in the journey



45 CFR 164.308(a)(1)(i)

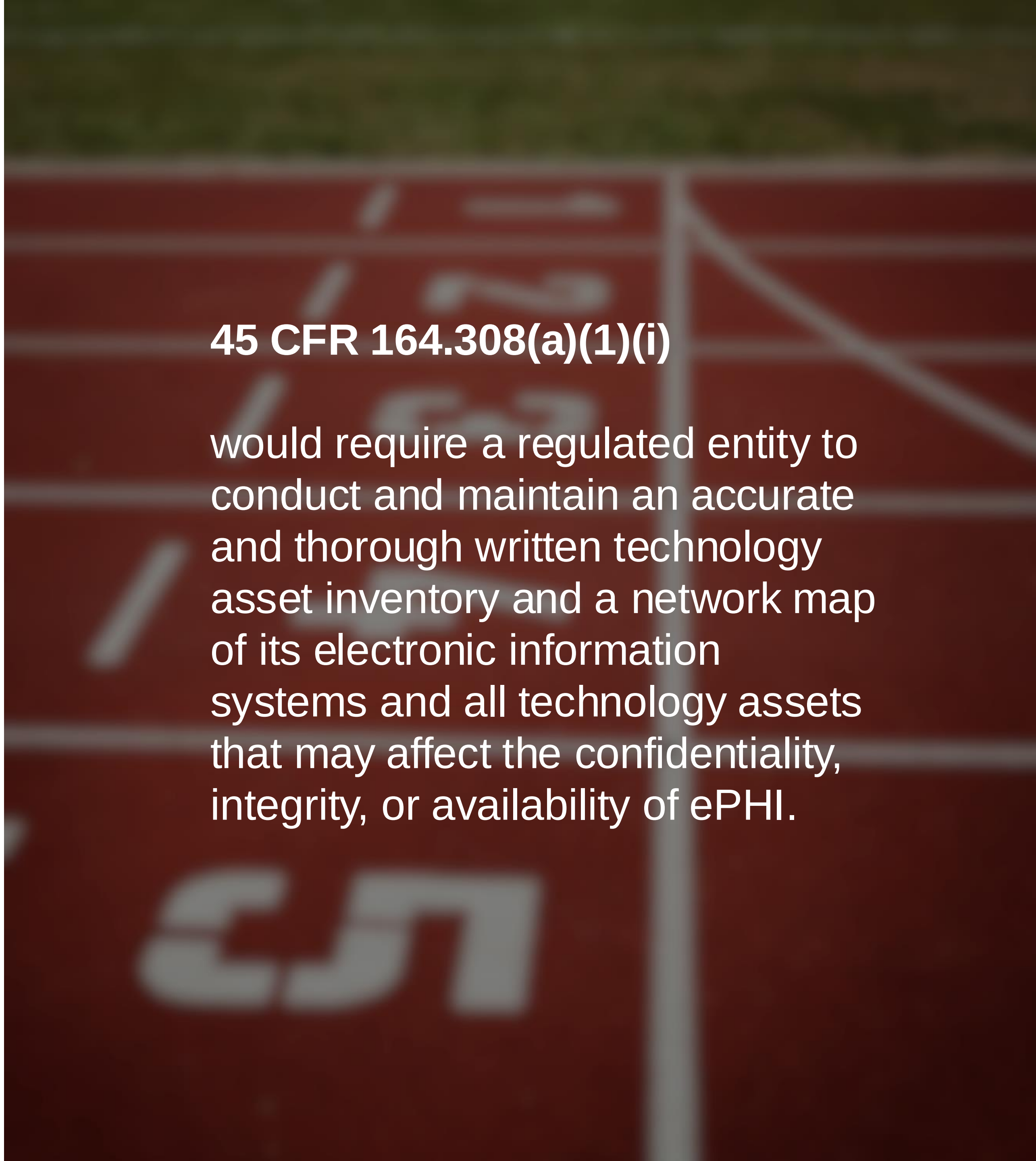
would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI.

HIPAA/HITECH NEW RULES

Start with Inventory

Vulnerabilities/Patches

- Inventory must include vulnerability data for compliance
- Traditional scanners miss OT, IoT, IoMT — know your gaps
- HHS mandates remediation for Critical (15 days) & High (30 days) CVEs



45 CFR 164.308(a)(1)(i)

would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI.

HIPAA/HITECH NEW RULES

Final Thoughts

- The New Rules are a win for healthcare IT and the customers we serve.
- Inventory is your keystone — if it’s only 70% accurate… well, good luck. (CMDB?)
- With real-time, accurate inventory, the New Rules aren’t onerous—they’re necessary.

WHAT I’M NOT:

- Professional HIPAA/HITECH consultant
- Political insider
- Trying to sell you a product (I have an idea, but you choose what you need)
- Still not a cow 🐮