Healthcare Sector Cybersecurity Psychology Framework (HS-CPF v1.0):

Patient Safety e Resilienza Clinica negli Ambienti Critici

Technical Report — Companion Settoriale al CPF v1.0

Giuseppe Canale, CISSP
Ricercatore Indipendente
g.canale@cpf3.org
URL: cpf3.org
ORCID: 0009-0007-3263-6897

25 Novembre 2025

Abstract

Il settore sanitario rappresenta il punto di massima tensione tra cybersecurity e operatività: dove in altri domini un blocco di sicurezza produce perdite economiche o ritardi operativi, in ambiente clinico può produrre morte. Questa realtà—il ransomware come minaccia cinetica, il denial-of-service come denial-of-care—richiede un approccio alla sicurezza psicologica radicalmente diverso. L'Healthcare Sector Cybersecurity Psychology Framework (HS-CPF) affronta questa sfida mappando le dieci categorie fondamentali del CPF sulla specificità dell'ambiente ospedaliero: la "Clinical Urgency" che rende i controlli di sicurezza incompatibili con l'imperativo ippocratico, la gerarchia medica che produce deferenza assoluta verso i "camici bianchi", l'altruismo professionale che viene sistematicamente sfruttato dagli attaccanti, e i "shadow workflow" che i reparti sviluppano per sopravvivere alla complessità tecnologica. Il framework preserva l'architettura matematica dell'Implementation Companion, consentendo il monitoraggio del rischio psicologico senza interrompere le cure. L'obiettivo non è imporre sicurezza *contro* il personale clinico, ma progettare sicurezza *per* il personale clinico, riconoscendo che proteggere gli operatori dallo stress digitale significa proteggere i pazienti.

Parole chiave: cybersecurity, sanità, patient safety, ransomware, EMR, stress clinico, resilienza, workflow clinici, break-glass

1 Introduzione: Il Panorama delle Minacce Cliniche

Il 28 settembre 2020, una donna è morta a Düsseldorf. Non per complicazioni mediche, non per errore chirurgico, ma perché un attacco ransomware aveva paralizzato i sistemi dell'Universitätsklinikum Düsseldorf, costringendo il reindirizzamento dell'ambulanza verso un ospedale più lontano[1]. I trenta minuti aggiuntivi di trasporto sono risultati fatali. Questo incidente ha segnato un punto di svolta: il ransomware non è più solo una minaccia informatica—è una minaccia cinetica, capace di uccidere.

Il settore sanitario è divenuto il bersaglio primario degli attacchi cyber. Il rapporto IBM Cost of a Data Breach 2024[2] documenta che la sanità mantiene il costo medio per breach più elevato di qualsiasi settore: $10.93 milioni, quasi il triplo della media intersettoriale. Gli attacchi ransomware agli ospedali sono aumentati del 94% nel biennio 2022-2024[3]. Queste statistiche, tuttavia, non catturano la dimensione più grave: l'impatto sulla cura del paziente.

1.1 Il Conflitto Ippocratico

"Primum non nocere"—prima di tutto, non nuocere. Questo principio, fondamento dell'etica medica da oltre due millenni, crea un conflitto strutturale con i requisiti della cybersecurity moderna.

Per un medico al Pronto Soccorso, il timeout della sessione che lo disconnette dalla cartella clinica elettronica (EMR) mentre sta consultando le allergie di un paziente in shock anafilattico non è un "controllo di sicurezza"—è un danno al paziente. L'autenticazione multi-fattore che richiede 30 secondi durante un arresto cardiaco non è "best practice"—è un ostacolo potenzialmente letale. La policy che vieta la condivisione delle password non considera che in sala operatoria il chirurgo con le mani sterili non può digitare credenziali.

Questa non è resistenza irrazionale alla sicurezza. È l'applicazione rigorosa del principio ippocratico: quando il controllo di sicurezza può danneggiare il paziente, il personale medico è eticamente obbligato a bypassarlo. Il problema non è convincere i medici che la sicurezza è importante—lo sanno. Il problema è che i sistemi di sicurezza progettati per ambienti "office-based" sono strutturalmente incompatibili con la realtà clinica.

1.2 L'Ambiente Fisico: Caos Controllato

L'ambiente ospedaliero differisce radicalmente da qualsiasi altro contesto lavorativo per caratteristiche che rendono impraticabili le policy di sicurezza standard.

Device Condivisi. Le Workstation on Wheels (WoW), i terminali di reparto, i sistemi nelle sale operatorie sono utilizzati da decine di operatori diversi ogni giorno. Il concetto di "postazione personale" non esiste. Ogni accesso richiede autenticazione, e ogni autenticazione sottrae tempo alla cura.

Rumore e Interruzioni. Il Pronto Soccorso opera a livelli di rumore che raggiungono 70-80 dB[4]—equivalenti a un'autostrada. Gli operatori sono interrotti in media ogni 6-8 minuti[5]. In questo contesto, la concentrazione necessaria per riconoscere un tentativo di phishing semplicemente non esiste.

Turni e Fatica. Il personale sanitario opera su turni di 12 ore, spesso con straordinari. La ricerca documenta che dopo 17 ore di veglia, le performance cognitive equivalgono a un tasso alcolemico di 0.05%[6]. Dopo 24 ore, a 0.10%—legalmente ubriachi in ogni giurisdizione.

Pressione Emotiva. Il personale sanitario affronta quotidianamente la morte, la sofferenza, le famiglie disperate. Il burnout nel settore supera il 50%[7]. In questo contesto di esaurimento emotivo, le risorse cognitive per la vigilanza di sicurezza sono cronicamente depleted.

1.3 Ransomware come Denial-of-Care

L'impatto psicologico di un attacco ransomware in ambiente ospedaliero trascende la perdita di dati o il costo del riscatto. È un trauma organizzativo.

Quando i sistemi EMR si bloccano, il personale deve tornare a carta e penna—procedure che molti giovani medici non hanno mai praticato. Le prescrizioni devono essere verificate manualmente. I risultati di laboratorio devono essere comunicati telefonicamente. Le immagini diagnostiche diventano inaccessibili. Ogni decisione clinica rallenta, e ogni rallentamento può costare vite.

Interviste con personale che ha vissuto attacchi ransomware documentano sintomi di stress post-traumatico[8]: ansia persistente, incubi, senso di colpa per le decisioni prese sotto pressione. L'attacco non colpisce solo i sistemi—colpisce le persone che li usano per salvare vite.

Il HS-CPF riconosce questa realtà. Non propone di "convincere" i medici ad accettare controlli che percepiscono come dannosi. Propone di riprogettare la sicurezza per l'ambiente clinico, riconoscendo che la protezione del personale dallo stress digitale è protezione del paziente.

2 Fondamenti Teorici: La Psicologia dell'Ambiente Clinico

2.1 La Gerarchia Medica come Sistema di Autorità

L'ospedale opera con una gerarchia che ricorda le strutture militari. Al vertice, i Primari e i Direttori di Dipartimento esercitano autorità quasi assoluta. Gli specializzandi, gli infermieri, i tecnici operano in una catena di comando dove contestare un superiore comporta rischi professionali significativi.

Questa struttura ha ragioni storiche e funzionali: in situazioni di emergenza, la decisione rapida di un'autorità riconosciuta può salvare vite. Tuttavia, crea vulnerabilità psicologiche sistematiche che il CPF categoria 1 (Authority-Based Vulnerabilities) cattura con precisione.

Gli studi di Milgram[9] sull'obbedienza all'autorità trovano nel contesto ospedaliero un'amplificazione estrema. L'esperimento Hofling del 1966[10] dimostrò che il 95% degli infermieri era disposto a somministrare un dosaggio potenzialmente letale di un farmaco sconosciuto su ordine telefonico di un medico mai incontrato. Cinquant'anni dopo, la dinamica fondamentale persiste.

2.2 L'Altruismo come Vulnerabilità

Il personale sanitario è selezionato—attraverso anni di formazione, tirocinio e pratica—per l'orientamento verso l'altro. La motivazione intrinseca che spinge a scegliere una carriera in medicina è, fondamentalmente, il desiderio di aiutare.

Questa caratteristica, essenziale per la funzione curativa, crea una vulnerabilità strutturale che la CPF categoria 4 (Affective Vulnerabilities) cattura. Gli attaccanti che comprendono questa dinamica costruiscono campagne di phishing che sfruttano direttamente l'impulso di aiutare: "Risultati esami urgenti", "Dati donatore organi", "Paziente critico richiede consultazione immediata".

La ricerca di Batson[11] sull'ipotesi empatia-altruismo dimostra che l'empatia genera motivazione altruistica che può override considerazioni di self-interest. Nel contesto sanitario, dove l'empatia è competenza professionale core, questo override è la norma, non l'eccezione.

2.3 Il Tribalismo di Reparto

I reparti ospedalieri funzionano come micro-culture semi-autonome. Il team di Terapia Intensiva sviluppa norme, linguaggio, procedure informali che lo distinguono dalla Chirurgia, che a sua volta differisce dal Pronto Soccorso.

Questo tribalismo ha funzioni adattive: crea coesione, supporto reciproco, efficienza attraverso comprensione condivisa. Tuttavia, produce anche "shadow workflow"—procedure informali che aggirano i sistemi ufficiali per necessità operativa.

La password scritta sul monitor, il badge condiviso tra colleghi di turno, l'account generico "infermiere-reparto" che tutti usano—questi non sono atti di negligenza individuale. Sono adattamenti collettivi a sistemi progettati senza comprendere la realtà operativa. La CPF categoria 6 (Group Dynamic Vulnerabilities) cattura queste dinamiche.

3 Manifestazioni Settoriali della Tassonomia Core 10×10

3.1 Categoria 1: Authority-Based Vulnerabilities

3.1.1 Manifestazione: "White Coat Supremacy (The God Complex)"

In ambiente ospedaliero, l'autorità non è semplicemente gerarchica—è quasi sacrale. Il "camice bianco" conferisce un'aura di autorità che trascende la specifica competenza dell'individuo che lo indossa.

Meccanismo Psicologico. La White Coat Supremacy opera attraverso dinamiche profondamente radicate:

1. I pazienti e il personale junior attribuiscono ai medici senior conoscenza quasi-onnisciente
2. Questa attribuzione si estende oltre il dominio clinico a qualsiasi richiesta il medico formuli
3. Contestare un Primario—anche su questioni IT—è percepito come insubordinazione professionale
4. Il personale IT, esterno alla gerarchia clinica, ha autorità limitata nell'imporre regole ai medici

Scenario Tipico. Un Primario chiede la password a uno specializzando "per verificare rapidamente un esame" mentre lo specializzando è impegnato. Lo specializzando fornisce la password immediatamente. Non considera che il Primario potrebbe usare le sue credenziali per accedere a dati non autorizzati, o che le credenziali potrebbero essere compromesse. Contesta il Primario non è un'opzione psicologicamente disponibile.

Indicatori CPF Coinvolti.

- 1.1 (Unquestioning compliance): Compliance assoluta a qualsiasi richiesta del "camice bianco"

- 1.6 (Authority gradient inhibiting security reporting): Il personale junior non segnala violazioni dei senior
- 1.3 (Authority figure impersonation susceptibility): Un attaccante che impersona un medico senior ottiene compliance immediata
- 1.7 (Deference to technical authority claims): "Sono il Dr. X della Radiologia, ho bisogno di accesso urgente"

Calibrazione dei Parametri OFTLISRV.

L'Authority Gradient Index per il settore sanitario:

$$AGI = \frac{H_{requester} - H_{target}}{H_{max}} \cdot C_{clinical\_context}$$

dove $H_{requester}$ è il livello gerarchico del richiedente (1=studente, 5=Primario), H_{target} è il livello del target, H_{max} è la differenza massima possibile, e $C_{clinical\_context}$ è un moltiplicatore per contesto clinico (1.0 normale, 1.5 emergenza, 2.0 codice rosso).

Probabilità di compliance dato AGI:

$$P(Compliance|AGI) = \frac{1}{1 + e^{-\beta(AGI - 0.3)}}$$

con $\beta = 5.0$. Per $AGI > 0.5$, la compliance è praticamente certa.

Data Sources Specifici.

- HR/Credentialing: livelli gerarchici del personale
- EMR audit logs: pattern di accesso cross-account
- Badge system: presenza fisica vs login
- Incident reporting: segnalazioni di condivisione credenziali

3.2 Categoria 2: Temporal Vulnerabilities

3.2.1 Manifestazione: "Code Blue Urgency"

"Code Blue" è il codice universale per arresto cardiaco. Quando risuona, ogni secondo conta. In questi momenti, la tolleranza per qualsiasi ostacolo—inclusi i controlli di sicurezza—scende a zero.

Meccanismo Psicologico. Durante un'emergenza medica, il personale opera in modalità "tunnel vision" focalizzata esclusivamente sul paziente. I circuiti cognitivi dedicati a valutazioni secondarie (inclusa la sicurezza IT) sono soppressi a favore dell'azione immediata. Questo non è un fallimento—è un adattamento evolutivo che massimizza le probabilità di salvare la vita.

Il problema emerge quando questa modalità viene sfruttata: un attaccante che conosce i ritmi ospedalieri può timing un attacco durante i picchi di emergenze (notte, weekend) sapendo che la vigilanza sarà minima.

Scenario Tipico. Paziente in arresto. Il medico corre al terminale per verificare la storia di allergie. Il sistema chiede MFA. Il telefono è nella tasca del camice in sala medici. Il medico

chiede a un infermiere di "entrare con le sue credenziali". L'infermiere lo fa. L'allergia viene verificata, il paziente viene salvato. E le credenziali sono state condivise, il log non riflette chi ha realmente acceduto, la policy è stata violata—per necessità assoluta.

Indicatori CPF Coinvolti.

- 2.1 (Urgency-induced bypass): Bypass sistematico durante codici
- 2.2 (Time pressure cognitive degradation): Incapacità di valutare rischi secondari
- 2.3 (Deadline-driven risk acceptance): "Il paziente muore se non accedo ora"
- 2.9 (Shift change exploitation windows): Le emergenze durante handover sono particolarmente vulnerabili

Calibrazione dei Parametri OFTLISRV.

Il Clinical Urgency Index (CUI):

$$CUI(t) = \sum_i w_i \cdot E_i(t)$$

dove $E_i(t)$ è un indicatore binario per il tipo di emergenza i attivo al tempo t, con pesi:

Table 1: Pesi per il Clinical Urgency Index

Tipo Emergenza	Peso w_i
Code Blue (Arresto)	3.0
Code Red (Trauma)	2.5
Code Pink (Pediatrico)	2.5
Stroke Alert	2.0
STEMI Alert	2.0
Sepsis Alert	1.5
Rapid Response	1.0

La probabilità di bypass dato CUI:

$$P(Bypass|CUI) = 1 - e^{-\lambda \cdot CUI}$$

con $\lambda = 0.5$. Per $CUI > 2.0$, il bypass è quasi certo.

Soluzione: Break-Glass Policy.

Invece di tentare di prevenire il bypass (impossibile), implementare "Break-Glass Access":

1. Accesso immediato senza autenticazione completa
2. Log dettagliato automatico di ogni azione
3. Audit obbligatorio post-evento entro 24 ore
4. Giustificazione clinica richiesta per chiudere l'audit
5. Pattern di break-glass anomali triggherano investigation

Questa soluzione riconosce la realtà operativa mentre mantiene accountability.

3.3 Categoria 4: Affective Vulnerabilities

3.3.1 Manifestazione: "Compassion Exploitation"

L'altruismo che definisce la professione sanitaria diventa il vettore principale di attacco nel contesto clinico.

Meccanismo Psicologico. Il personale sanitario è condizionato a rispondere alla sofferenza. Quando un messaggio evoca urgenza clinica—un paziente in pericolo, un esame critico, un donatore di organi—la risposta emotiva precede e override la valutazione razionale.

Gli attaccanti sofisticati hanno imparato a costruire campagne che sfruttano specificamente il linguaggio clinico. "URGENTE: Risultato biopsia positivo - Dott. [Nome]" ha tassi di click che superano il 40% nel personale sanitario[13], contro una media del 3-5% per phishing generico.

Indicatori CPF Coinvolti.

- 4.3 (Trust transference): La fiducia nel "messaggio clinico" si trasferisce al link
- 4.6 (Guilt-driven overcompliance): "E se fosse vero e non apro?"
- 4.7 (Anxiety-triggered mistakes): L'ansia per il paziente produce click impulsivi
- 4.10 (Emotional contagion): L'urgenza percepita si propaga tra colleghi

Calibrazione dei Parametri OFTLISRV.

Lo score di Compassion Exploitation:

$$CE(m) = L_{clinical}(m) \cdot U_{perceived}(m) \cdot P_{patient\_harm}(m)$$

dove:

- $L_{clinical}(m)$: score di linguaggio clinico nel messaggio m (NLP)
- $U_{perceived}(m)$: urgenza percepita (keyword analysis: "urgente", "critico", "immediato")
- $P_{patient\_harm}(m)$: implicazione di danno al paziente ("paziente", "esame", "risultato")

Soglie di allarme:

- $CE > 0.7$ con sender esterno: block + alert immediato
- $CE > 0.5$ con sender esterno: warning banner potenziato
- $CE > 0.3$ con sender interno non riconosciuto: verifica MFA aggiuntiva

Data Sources Specifici.

- Email gateway: analisi contenuto con dizionario clinico
- EMR integration: verifica che pazienti citati esistano realmente
- Sender reputation: storico del mittente nel sistema sanitario
- Click tracking: correlazione tra CE score e tassi di click

3.4 Categoria 5: Cognitive Overload Vulnerabilities

3.4.1 Manifestazione: "Alert Fatigue Syndrome"

Il personale sanitario opera in un ambiente saturo di allarmi. Monitor cardiaci, pompe infusionali, ventilatori, sistemi di allerta clinica—tutti competono per l'attenzione. A questo si aggiungono gli alert di sicurezza IT.

Meccanismo Psicologico. La ricerca documenta che fino all'85-99% degli allarmi clinici sono falsi positivi o clinicamente non rilevanti[12]. Il personale sviluppa inevitabilmente "alarm fatigue": desensibilizzazione progressiva che porta a ignorare o disabilitare gli allarmi.

Quando gli alert di sicurezza IT si aggiungono a questo carico, vengono automaticamente categorizzati come "rumore" e ignorati. Un warning di sicurezza su un sito sospetto non può competere con il monitor che segnala aritmia.

Indicatori CPF Coinvolti.

- 5.1 (Alert fatigue desensitization): Gli alert IT sono rumore
- 5.4 (Multitasking degradation): Impossibile processare alert multipli simultanei
- 5.6 (Cognitive tunneling): Focus sul paziente esclude tutto il resto
- 5.7 (Working memory overflow): Troppi alert saturano la memoria di lavoro

Calibrazione. Alert Fatigue Index:

$$AFI = \frac{N_{alerts\_received}}{T_{shift}} \cdot (1 - R_{response\_rate})$$

dove N_{alerts} è il numero di alert (clinici + IT), T_{shift} è la durata del turno, e $R_{response\_rate}$ è il tasso di risposta appropriata agli alert.

Soglie:

- $AFI < 5$: normale
- $AFI \in [5, 15)$: elevato, ridurre alert non critici
- $AFI \geq 15$: critico, intervento immediato sulla cascata di alert

3.5 Categoria 6: Group Dynamic Vulnerabilities

3.5.1 Manifestazione: "Ward Tribalism & Shadow Workflows"

I reparti sviluppano culture locali che includono workaround sistematici ai controlli di sicurezza. Questi non sono atti di sabotaggio ma adattamenti collettivi per la sopravvivenza operativa.

Meccanismo Psicologico. Il team di reparto affronta sfide comuni: sistemi lenti, timeout frequenti, autenticazione ripetitiva. Nel tempo, il gruppo sviluppa "soluzioni" condivise: la password del turno scritta sulla bacheca, l'account generico che tutti usano, il badge che rimane inserito nella postazione.

Queste pratiche sono trasmesse ai nuovi membri come "come si fa qui". Contestarle significa contestare il gruppo, con conseguenze sociali significative. La pressione verso la conformità supera la compliance con policy esterne.

Scenario Tipico. Nuovo infermiere al primo turno in Terapia Intensiva. Nota la password scritta su un post-it. Esita. Il collega senior: "Qui facciamo così, altrimenti perdiamo tempo prezioso". L'infermiere si adegua. In due settimane, ha interiorizzato la pratica. Non la percepisce più come violazione.

Indicatori CPF Coinvolti.

- 6.1 (Groupthink security blind spots): Il reparto non "vede" il rischio delle proprie pratiche
- 6.3 (Diffusion of responsibility): "Tutti lo fanno, non è responsabilità mia"
- 6.4 (Social loafing): La sicurezza è "problema dell'IT, non nostro"
- 6.8 (Pairing hope fantasies): "Non succederà niente, abbiamo sempre fatto così"

Calibrazione dei Parametri OFTLISRV.

Detection di Shadow Workflow tramite correlazione badge-login:

Logica (L): Rilevare "Impossible Travel" intra-ospedaliero:

- Se $User_A$ fa login su EMR da $Ward_X$
- E il badge di $User_A$ risulta in $Ward_Y$ (diverso)
- E non esiste record di movimento badge tra Y e X
- $\Rightarrow$ Probabile utilizzo credenziali di $User_A$ da parte di altro operatore

Score di Credential Sharing:

$$CS_{ward} = \frac{N_{impossible\_travel}}{N_{logins}} \cdot 100$$

Soglie per reparto:

- $CS < 2\%$: normale (errori sporadici)
- $CS \in [2\%, 8\%)$: elevato, audit mirato
- $CS \geq 8\%$: shadow workflow sistematico, intervento CPIF

Correlazione con Shift Change:

$$\Delta CS_{shift} = CS_{t+1h} - CS_{t-1h}$$

dove t è l'orario di cambio turno. Un $\Delta CS > 5\%$ indica credential sharing concentrato negli handover.

Data Sources Specifici.

- Badge access system: posizione fisica in tempo reale

- EMR audit logs: workstation e timestamp di login
- Nurse scheduling system: turni e assegnazioni
- Network logs: MAC address delle workstation

3.6 Categoria 7: Stress Response Vulnerabilities

3.6.1 Manifestazione: "Chronic Burnout Degradation"

Il burnout nel personale sanitario ha raggiunto livelli epidemici post-COVID. Oltre il 50% dei medici e il 60% degli infermieri riportano sintomi di burnout[7]. Questo esaurimento cronico produce degradazione sistematica delle capacità cognitive, inclusa la vigilanza di sicurezza.

Meccanismo Psicologico. Il burnout produce:

- Esaurimento emotivo: incapacità di "preoccuparsi" di minacce astratte come la cybersecurity
- Depersonalizzazione: distacco che riduce l'engagement con qualsiasi procedura
- Ridotta efficacia personale: "tanto non cambia nulla"

Un operatore in burnout non ha le risorse cognitive per valutare criticamente un'email sospetta. La path of least resistance—click e vai avanti—diventa l'unica opzione praticabile.

Indicatori CPF Coinvolti.

- 7.2 (Chronic stress burnout): Esaurimento prolungato
- 7.4 (Flight response avoidance): Evitamento di qualsiasi complessità aggiuntiva
- 7.5 (Freeze response paralysis): Incapacità di decidere di fronte a warning
- 7.10 (Recovery period vulnerabilities): Post-turno intensivo, vulnerabilità massima

Calibrazione. Burnout Vulnerability Index:

$$BVI = \alpha \cdot Overtime_{30d} + \beta \cdot PatientLoad + \gamma \cdot IncidentExposure$$

dove:

- $Overtime_{30d}$: ore di straordinario negli ultimi 30 giorni
- $PatientLoad$: rapporto pazienti/operatore vs standard
- $IncidentExposure$: numero di decessi/eventi critici gestiti

Pesi suggeriti: $\alpha = 0.4$, $\beta = 0.35$, $\gamma = 0.25$.

3.7 Categoria 9: AI-Specific Bias Vulnerabilities

3.7.1 Manifestazione: "Diagnostic Automation Bias"

L'adozione di sistemi AI di supporto alla diagnosi (Clinical Decision Support Systems - CDSS) ha introdotto nuove vulnerabilità. I medici, specialmente quando affaticati, tendono ad accettare le raccomandazioni AI senza verifica critica.

Meccanismo Psicologico. Il CDSS è presentato come "basato su evidenze" e "più accurato dell'umano". Questa framing produce automation bias: il medico delega cognitivamente al sistema. Quando il sistema è corretto, l'efficienza aumenta. Quando il sistema è errato—o compromesso—l'errore viene propagato senza filtro umano.

Scenario Catastrofico. Un attaccante compromette il CDSS attraverso adversarial attack. Il sistema inizia a suggerire dosaggi di farmaci leggermente alterati. Un medico a fine turno, affaticato, accetta la raccomandazione senza verificare. Il paziente riceve un dosaggio letale.

Questo scenario, teorico ma tecnicamente plausibile, rappresenta il punto di convergenza più pericoloso tra cybersecurity e patient safety.

Indicatori CPF Coinvolti.

- 9.2 (Automation bias override): Accettazione acritica delle raccomandazioni AI
- 9.4 (AI authority transfer): Il CDSS diventa l'autorità invece dello strumento
- 9.7 (AI hallucination acceptance): Raccomandazioni "plausibili" ma errate
- 9.8 (Human-AI team dysfunction): Il medico non sa quando dubitare del sistema

Calibrazione dei Parametri OFTLISRV.

Override Rate per CDSS:

$$O_{rate} = \frac{N_{human\_override}}{N_{CDSS\_recommendations}}$$

Soglie calibrate per contesto clinico:

- Verde: $O_{rate} \in [0.10, 0.25]$ (healthy skepticism)
- Giallo: $O_{rate} < 0.10$ (over-trust) o $O_{rate} > 0.35$ (under-utilization)
- Rosso: $O_{rate} < 0.05$ (automation blindness critica)

Monitoraggio per Adversarial Detection:

- Baseline dei pattern di raccomandazione CDSS
- Anomaly detection su shift nelle distribuzioni di dosaggio
- Alert se outcome negativi correlano con accettazione CDSS
- Human-in-the-loop obbligatorio per farmaci ad alto rischio

3.8 Categoria 10: Critical Convergent States

3.8.1 Manifestazione: "Multi-Code Collapse"

Il settore sanitario è particolarmente vulnerabile a stati convergenti durante eventi che sovrappongono multiple emergenze—tipicamente, le Mass Casualty Incidents (MCI) o le ondate pandemiche.

Scenario Tipico. Incidente stradale con 15 feriti gravi. Il Pronto Soccorso si riempie (Cat 7: stress acuto). Codici rossi simultanei (Cat 2: urgenza massima). I sistemi rallentano per il carico (Cat 5: cognitive overload). Il personale usa credenziali condivise per velocizzare (Cat 6: shadow workflow). Arriva un'email "Lista aggiornata pazienti MCI" (Cat 4: compassion exploitation). Click. Ransomware.

Calcolo del Convergence Index Sanitario.

$$CI_{HS} = \prod_{i \in S} (1 + w_i \cdot v_i)$$

con pesi settoriali:

Table 2: Pesi Settoriali per il Convergence Index Sanitario

Categoria	Peso Standard	Peso HS-CPF
Cat 1 (Authority/White Coat)	1.0	1.4
Cat 2 (Temporal/Code Blue)	1.0	1.8
Cat 4 (Affective/Compassion)	1.0	1.6
Cat 5 (Cognitive/Alert Fatigue)	1.0	1.3
Cat 6 (Group/Ward Tribalism)	1.0	1.4
Cat 7 (Stress/Burnout)	1.0	1.5
Cat 9 (AI/Diagnostic Bias)	1.0	1.3
Cat 10 (Convergent)	1.0	1.9

Il threshold critico per il settore sanitario è $CI_{crit} = 4.0$ (inferiore al generale 5.0 per la criticità life-or-death delle conseguenze).

4 Strategia di Intervento CPIF negli Ospedali

4.1 Fase 1: Readiness Assessment

Gli ospedali sono organizzazioni complesse con stakeholder multipli e spesso in conflitto: amministrazione, corpo medico, nursing, IT, compliance, risk management. La readiness deve essere valutata separatamente per ciascun gruppo.

Principio Fondamentale: Parlare di Patient Safety, Non di IT Security.

La parola "cybersecurity" attiva resistenza nel personale clinico ("problema dell'IT, non mio"). La parola "patient safety" attiva engagement ("il mio lavoro").

Ogni comunicazione, ogni intervento, ogni policy deve essere framato in termini di protezione del paziente:

- Non "proteggi le tue credenziali" ma "proteggi l'accesso ai dati dei tuoi pazienti"

- Non "evita il phishing" ma "verifica prima di agire per non mettere a rischio le cure"
- Non "compliance con la policy IT" ma "sicurezza delle cartelle cliniche"

Dimensioni di Readiness Specifiche:

1. **Supporto della Leadership Clinica**: Senza i Primari, nessun intervento funziona
2. **Coinvolgimento del Nursing Leadership**: Gli infermieri sono il cuore operativo
3. **Allineamento IT-Clinica**: Storicamente conflittuale, richiede mediazione
4. **Risorse per Implementazione**: Tempo del personale è la risorsa più scarsa
5. **Storico di Iniziative Fallite**: Ogni fallimento passato aumenta il cinismo

4.2 Fase 2: Matching Vulnerabilità-Intervento

Il matching nel settore sanitario deve rispettare un vincolo assoluto: **nessun intervento può rallentare o ostacolare la cura del paziente**.

Questo vincolo elimina molte opzioni disponibili in altri settori. Ciò che rimane richiede creatività progettuale.

Interventi per White Coat Supremacy (Cat 1):

- Role-based access control rigoroso (il Primario non ha bisogno della password dello specializzando)
- Formazione specifica per la leadership clinica (i Primari come champion di sicurezza)
- Canali anonimi per segnalare pressioni inappropriate
- Policy esplicita che la condivisione credenziali è violazione anche su ordine superiore

Interventi per Code Blue Urgency (Cat 2):

- **Break-Glass Access**: Accesso immediato senza MFA, con logging completo e audit obbligatorio
- Autenticazione proximity-based (badge RFID) che non richiede azioni manuali
- Timeout estesi durante codici attivi (il sistema "sa" che c'è un'emergenza)
- Pre-autenticazione automatica quando si entra in aree critiche (ER, ICU, OR)

Interventi per Compassion Exploitation (Cat 4):

- Filtering email con dizionario clinico per sender esterni
- Delay obbligatorio (3 secondi) prima di click su link in email "urgenti"
- Verifica automatica: "Questo paziente esiste nel nostro sistema?"
- Simulazioni di phishing calibrate sul linguaggio clinico (non generico)

Interventi per Ward Tribalism (Cat 6):

- Coinvolgimento dei "informal leader" di reparto come security champion
- Redesign dei workflow che elimina la necessità dei workaround
- Single sign-on che riduce il numero di autenticazioni necessarie
- Badge di prossimità che sostituisce il login manuale

4.3 Fase 3: Design dell'Intervento

Principio: Sicurezza Passiva.

Il personale clinico non ha tempo né risorse cognitive per "fare sicurezza" attivamente. L'intervento deve essere progettato per funzionare *senza* richiedere azioni consapevoli.

Esempi di Sicurezza Passiva:

- Badge RFID che autentica automaticamente quando il clinico si avvicina al terminale
- Logout automatico quando il badge si allontana
- Filtering in background che blocca threat senza richiedere valutazione umana
- Default secure: i sistemi partono sicuri, le eccezioni richiedono azione consapevole

4.4 Fase 4: Navigazione della Resistenza

Resistenza Dominante: "Non ho tempo per l'IT."

Questa resistenza è legittima. Il personale sanitario non ha effettivamente tempo. La risposta non è convincerli che dovrebbero avere tempo—è progettare interventi che non richiedono tempo.

Strategia: Per ogni intervento proposto, calcolare il "time tax"—quanto tempo aggiunge al workflow clinico. Se il time tax è > 0, riprogettare fino a raggiungere time tax ≤ 0 (l'intervento fa risparmiare tempo o è neutro).

Resistenza dei Medici Senior: "Ho sempre fatto così."

I Primari hanno decenni di esperienza con workflow consolidati. Cambiare richiede effort cognitivo che percepiscono come non giustificato.

Strategia: Peer influence. Identificare un Primario "early adopter" rispettato e farlo diventare champion. Il cambiamento proposto da un pari ha probabilità di accettazione molto superiore al cambiamento imposto dall'IT.

Resistenza dell'IT: "I clinici non capiscono il rischio."

L'IT può sviluppare frustrazione verso il personale clinico che "non segue le regole". Questa frustrazione produce policy sempre più restrittive che vengono sempre più aggirate.

Strategia: Embedded IT. Assegnare personale IT a lavorare fisicamente nei reparti per periodi estesi. L'esperienza diretta della realtà clinica produce empatia e soluzioni più adeguate.

4.5 Fase 5: Implementazione

Sequenza di Implementazione Raccomandata:

1. **Settimane 1-4**: Assessment e stakeholder engagement
2. **Mesi 2-3**: Pilot in un reparto "friendly" (tipicamente un reparto con champion)
3. **Mesi 4-6**: Estensione ai reparti critici (ER, ICU) con adattamenti
4. **Mesi 7-9**: Roll-out progressivo ad altri reparti
5. **Mesi 10-12**: Consolidamento e ottimizzazione

Metriche di Successo.

- Riduzione del Credential Sharing Score
- Break-Glass utilization rate (deve esistere ma essere raro)
- Click rate su phishing simulation (calibrato su linguaggio clinico)
- **Nessun impatto negativo su metriche di patient outcome**

5 Implementazione Tecnica: Schema OFTLISRV

5.1 Architettura di Integrazione

L'ecosistema IT ospedaliero tipico comprende:

- **EMR** (Electronic Medical Records): Epic, Cerner, Meditech
- **PACS** (Picture Archiving): imaging diagnostico
- **LIS** (Laboratory Information System): esami di laboratorio
- **Pharmacy System**: prescrizioni e dispensazione
- **Badge/Access Control**: accesso fisico
- **Nurse Call System**: comunicazioni di reparto
- **Medical Device Network**: monitor, pompe, ventilatori

Il CPF engine per il settore sanitario deve integrarsi con tutti questi sistemi, con particolare attenzione alla latenza (non deve rallentare i sistemi clinici).

5.2 Detection Logic: Ward Tribalism (Esempio Dettagliato)

Obiettivo: Rilevare pattern di credential sharing sistematico a livello di reparto.

Data Sources (F):

- EMR audit logs: user ID, timestamp, workstation ID, azioni
- Badge system: user ID, timestamp, location (reader ID)
- HR system: assegnazione reparto, turni

Pre-processing:

1. Allineare i timestamp dei tre sistemi (possono avere drift)
2. Mappare workstation ID a location fisica
3. Mappare badge reader ID a location fisica
4. Creare finestre temporali di 5 minuti per il matching

Logic (L) - Impossible Travel Detection:

Algorithm 1 Impossible Travel Detection Intra-Ospedaliero

for each EMR login event e **do**
  $user \leftarrow e.user\_id$
  $login\_location \leftarrow location(e.workstation\_id)$
  $login\_time \leftarrow e.timestamp$
  $badge\_events \leftarrow get\_badge\_events(user, login\_time \pm 5min)$
  if $badge\_events$ is empty **then**
    flag as "No badge presence"
  else
    $badge\_location \leftarrow most\_recent(badge\_events).location$
    if $badge\_location \neq login\_location$ **then**
      $distance \leftarrow calculate\_distance(badge\_location, login\_location)$
      $time\_diff \leftarrow |login\_time - badge\_event.time|$
      if $distance/time\_diff > walking\_speed\_threshold$ **then**
        flag as "Impossible Travel"
      end if
    end if
  end if
end for

Thresholds (S):

- $walking\_speed\_threshold = 5$ km/h (normale camminata in ospedale)
- Tolerance per errori di timing: ± 2 minuti
- Minimum distance per flag: 50 metri (evita falsi positivi da reader adiacenti)

Aggregazione a Livello Reparto:

$$CS_{ward}(w,t) = \frac{\sum_{u \in w} ImpossibleTravel(u,t)}{\sum_{u \in w} Logins(u,t)} \cdot 100$$

Temporal Pattern - Shift Change Correlation:

$$\rho_{shift} = corr(CS_{ward}(t), ShiftChange(t))$$

dove $ShiftChange(t)$ è un indicatore binario per i 30 minuti intorno al cambio turno.

Un $\rho_{shift} > 0.5$ indica che la credential sharing è concentrata negli handover, suggerendo workaround per velocizzare il passaggio di consegne.

Response (R):

- $CS < 2\%$: log only, no action
- $CS \in [2\%, 5\%)$: alert settimanale al Nurse Manager
- $CS \in [5\%, 10\%)$: audit mirato, workshop con il team
- $CS \geq 10\%$: intervento CPIF completo, redesign workflow

Validation (V):

- Backtesting su 6 mesi di dati storici
- Verifica manuale di un campione di flag
- Interviste con personale per validare interpretazione
- Correlazione con incidenti di sicurezza noti

6 Case Study: The ER Ransomware Outbreak

6.1 Contesto dell'Incidente

Ottobre 2024. Un ospedale regionale italiano (anonimizzato) con 450 posti letto. Sabato sera, ore 22:30. Il Pronto Soccorso è in sovraccarico: 47 pazienti in attesa, 3 codici rossi simultanei, personale ridotto per il weekend.

6.2 Vettore di Attacco

Un'infermiera di triage, al terzo turno consecutivo di 12 ore (copertura per colleghi malati), riceve un'email apparentemente interna: "URGENTE: Lista aggiornata pazienti in attesa - Nuovo protocollo regionale". L'email contiene un allegato Excel.

L'infermiera, sovraccarica (Cat 7: Stress), ansiosa di gestire il flusso pazienti (Cat 4: Compassion/dovere di cura), clicca sull'allegato senza verificare il mittente.

L'Excel contiene una macro che esegue il payload ransomware.

6.3 Propagazione Laterale

Il ransomware si diffonde rapidamente per due ragioni:

1. Le workstation del PS utilizzano una password locale condivisa ("PSNurse2024") per "velocizzare" l'accesso durante le emergenze (Cat 6: Ward Tribalism)
2. Il segmento di rete del PS non è isolato dalla rete ospedaliera generale

In 23 minuti, il ransomware ha cifrato:

- 12 workstation del Pronto Soccorso
- Il server dipartimentale con i template di documentazione
- 3 workstation della Radiologia (connesse per visualizzazione immagini PS)

6.4 Impatto Clinico

L'EMR centrale (su server separati e meglio protetti) rimane funzionante, ma le workstation locali non possono accedervi. Il personale è costretto a:

- Tornare a documentazione cartacea improvvisata
- Chiamare telefonicamente per risultati laboratorio
- Trasportare fisicamente le immagini radiologiche

Un paziente con infarto (STEMI) subisce un ritardo di 18 minuti nell'accesso al cateterismo perché la documentazione per il consenso deve essere rifatta a mano. Fortunatamente sopravvive, ma il ritardo ha aumentato il danno miocardico.

6.5 Analisi CPF Retrospettiva

Fattori Convergenti:

- Cat 7 (Stress): $v_7 = 0.85$ (terzo turno consecutivo, weekend, sovraccarico)
- Cat 4 (Affective): $v_4 = 0.70$ (email sfruttava dovere di cura)
- Cat 6 (Group): $v_6 = 0.80$ (password condivisa sistematica)
- Cat 5 (Cognitive): $v_5 = 0.65$ (alert fatigue, rumore, interruzioni)
- Cat 2 (Temporal): $v_2 = 0.75$ (codici rossi attivi, urgenza percepita)

Convergence Index:

$$\begin{aligned} CI_{HS} &= (1 + 1.5 \times 0.85) \cdot (1 + 1.6 \times 0.70) \cdot (1 + 1.4 \times 0.80) \\ &\quad \cdot (1 + 1.3 \times 0.65) \cdot (1 + 1.8 \times 0.75) \\ &= 2.275 \cdot 2.12 \cdot 2.12 \cdot 1.845 \cdot 2.35 \\ &= 44.3 \end{aligned} \tag{1}$$

Il CI era oltre 11 volte superiore alla soglia critica settoriale di 4.0.

6.6 Detection Points Mancati

Con il HS-CPF implementato, l'incidente avrebbe generato alert a:

- **Pre-incidente**: Burnout Index elevato per l'infermiera (turni consecutivi)
- **Pre-incidente**: Credential Sharing Score del PS al 14% (ben sopra soglia)
- **Al momento del click**: Email con CE score > 0.8 da sender esterno
- **Post-click**: Lateral movement anomalo dalla workstation

6.7 Remediation Implementata

Post-incidente:

1. Segmentazione di rete: PS isolato con controlli inter-segmento
2. Eliminazione password locali condivise, implementazione badge RFID
3. Email filtering con dizionario clinico per allegati
4. Policy su turni consecutivi (massimo 2 senza approvazione)
5. Break-Glass formale con audit obbligatorio
6. Deployment pilota HS-CPF nel PS

7 Integrazione con l'Ecosistema CPF

7.1 Compatibilità Architetturale

L'HS-CPF mantiene piena compatibilità con l'architettura CPF:

- **Tassonomia**: Nessuna nuova categoria; manifestazioni settoriali
- **OFTLISRV**: Schema preservato; parametri calibrati
- **Reti Bayesiane**: Struttura invariata; probabilità condizionali aggiornate
- **Convergence Index**: Formula preservata; pesi settoriali (Tab. 2)
- **Response Protocols**: Struttura preservata; Break-Glass integrato

7.2 Interoperabilità con Standard Sanitari

L'HS-CPF è progettato per integrarsi con:

- **HIPAA** (USA): Privacy e sicurezza dei dati sanitari
- **GDPR** (EU): Con focus sui dati sanitari (Art. 9)
- **NIST Cybersecurity Framework**: Mapping diretto alle funzioni
- **HITRUST CSF**: Framework specifico per healthcare
- **Joint Commission Standards**: Accreditamento ospedaliero

7.3 Deployment Considerations

Prerequisiti:

- CPF base engine operativo (o deployment parallelo)
- Integrazione con EMR (Epic, Cerner, etc.) per audit logs

- Integrazione con Badge system per correlation
- Supporto della leadership clinica (non solo IT)

Fasi di Deployment:

1. Assessment della readiness clinica e IT
2. Pilot in un reparto con champion identificato
3. Calibrazione su dati reali (3-6 mesi)
4. Estensione progressiva con adattamenti per reparto
5. Full deployment con monitoring continuo

8 Conclusione: La Cyber-Resilienza come Parametro Vitale

Il settore sanitario opera all'intersezione più critica tra cybersecurity e outcome umani. Dove altri settori misurano l'impatto dei breach in dollari o in ore di downtime, la sanità lo misura in vite.

L'Healthcare Sector Cybersecurity Psychology Framework riconosce questa realtà unica. Non propone di forzare il personale clinico ad adottare pratiche di sicurezza progettate per uffici. Propone di riprogettare la sicurezza per l'ambiente clinico, riconoscendo che:

- L'imperativo ippocratico prevale su qualsiasi policy IT, e deve essere così
- I bypass di sicurezza non nascono da negligenza ma da necessità clinica
- La soluzione non è controlli più rigidi ma controlli più intelligenti
- Proteggere il personale dallo stress digitale significa proteggere i pazienti

Le manifestazioni settoriali identificate—White Coat Supremacy, Code Blue Urgency, Compassion Exploitation, Ward Tribalism, Diagnostic Automation Bias—non sono "problemi da risolvere" eliminando i comportamenti. Sono adattamenti razionali a un ambiente impossibile. La soluzione è modificare l'ambiente, non le persone.

Il Break-Glass Access, l'autenticazione proximity-based, il filtering intelligente delle email cliniche, la segmentazione che protegge senza isolare—questi sono gli strumenti di una sicurezza che lavora *per* il clinico, non *contro* il clinico.

Il case study del ransomware al Pronto Soccorso illustra cosa accade quando queste protezioni mancano: un'infermiera esausta, un'email che sfrutta il suo altruismo, una password condivisa che era "l'unico modo per lavorare", e un paziente che ha rischiato la vita.

Con l'HS-CPF, quel Convergence Index di 44.3 avrebbe generato alert prima che l'infermiera vedesse l'email. Il sistema avrebbe riconosciuto le condizioni di vulnerabilità estrema e avrebbe attivato protezioni compensative. Il paziente non avrebbe mai corso quel rischio.

La cyber-resilienza in sanità non è un optional. È un parametro vitale, da monitorare con la stessa attenzione che dedichiamo alla pressione arteriosa e alla saturazione di ossigeno. L'HS-CPF fornisce gli strumenti per questo monitoraggio.

Perché ogni minuto di downtime in ospedale non è un costo. È un rischio per qualcuno che si è affidato a noi.

Nota sull'Uso di Strumenti AI

Questo manoscritto presenta il framework teorico originale e i contributi intellettuali dell'autore. Nel processo di composizione, l'autore ha utilizzato un modello linguistico di grandi dimensioni come strumento ausiliario per il raffinamento stilistico e la coerenza formattativa. Le idee core, l'architettura HS-CPF, l'integrazione teorica, e l'analisi strategica sono esclusivamente prodotto dell'expertise dell'autore. L'autore è interamente responsabile per l'accuratezza e l'integrità del contenuto pubblicato.

Ringraziamenti

L'autore ringrazia i professionisti sanitari che hanno condiviso le loro esperienze quotidiane con i sistemi informatici ospedalieri, e i team IT ospedalieri che operano nella difficile posizione di proteggere sistemi critici senza poter rallentare le cure.

References

[1] Greenberg, A. (2020). A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death. *Wired*, November 2020.

[2] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.

[3] U.S. Department of Health and Human Services. (2024). *Healthcare Sector Cybersecurity: 2024 Threat Landscape*. HHS Office of Information Security.

[4] Busch-Vishniac, I. J., et al. (2017). Noise levels in Johns Hopkins Hospital. *The Journal of the Acoustical Society of America*, 118(6), 3629-3645.

[5] Westbrook, J. I., et al. (2010). Association of interruptions with an increased risk and severity of medication administration errors. *Archives of Internal Medicine*, 170(8), 683-690.

[6] Dawson, D., & Reid, K. (1997). Fatigue, alcohol and performance impairment. *Nature*, 388(6639), 235-235.

[7] Shanafelt, T. D., et al. (2022). Changes in burnout and satisfaction with work-life integration in physicians during the first 2 years of the COVID-19 pandemic. *Mayo Clinic Proceedings*, 97(12), 2248-2258.

[8] Dameff, C., et al. (2019). Cybersecurity concerns and medical devices: Lessons from a pacemaker advisory. *Annals of Internal Medicine*, 171(5), 375-376.

[9] Milgram, S. (1974). *Obedience to Authority: An Experimental View*. New York: Harper & Row.

[10] Hofling, C. K., et al. (1966). An experimental study in nurse-physician relationships. *The Journal of Nervous and Mental Disease*, 143(2), 171-180.

[11] Batson, C. D. (2011). *Altruism in Humans*. Oxford: Oxford University Press.

[12] Sendelbach, S., & Funk, M. (2013). Alarm fatigue: A patient safety concern. *AACN Advanced Critical Care*, 24(4), 378-386.

[13] Gordon, W. J., et al. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open*, 2(3), e190393.

[14] Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

[15] Bion, W. R. (1961). *Experiences in Groups*. London: Tavistock Publications.

[16] Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). San Francisco: Jossey-Bass.