ISBN: 978-65-986235-9-3

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: DESAFIOS DE PRIVACIDADE E SEGURANÇA CIBERNÉTICA

https://doi.org/10.63330/aurumpub.009-002

Mirian Esquárcio Jabur
Grau de formação mais alto: Mestre em Educação Tecnológica
Instituição acadêmica: CEFET/MG
E-mail: mirianjabur@gmail.com

RESUMO
Este artigo analisa os avanços e desafios da transformação digital na saúde, com foco na adoção de inteligência artificial (IA) e suas melhorias comprovadas, como a redução do tempo em diagnósticos e dos erros médicos. Aborda também as questões críticas relacionadas à segurança da informação, privacidade de dados sensíveis e ética no uso de tecnologias emergentes. São apresentados casos reais de incidentes cibernéticos, discute a relevância das regulamentações, como a Lei Geral de Proteção de Dados (LGPD), e sugere diretrizes para garantir uma inovação responsável que equilibre progresso tecnológico e proteção dos direitos fundamentais dos pacientes.

Palavras-chave: Saúde digital; Inteligência Artificial; Segurança da informação; Privacidade de dados; Ética em IA; LGPD.

1 INTRODUÇÃO

A transformação digital tem provocado mudanças profundas e irreversíveis na área da saúde, impulsionada por tecnologias emergentes como a inteligência artificial (IA), a Internet das Coisas Médicas (IoMT) e a análise de grandes volumes de dados. Essas inovações oferecem potencial significativo para aprimorar a qualidade e a eficiência do atendimento, evidenciado pela redução do tempo de diagnóstico em radiologia em até 44% (ESTEVA et al., 2017) e pela diminuição de erros médicos em até 80%, especialmente em processos críticos como a administração de medicamentos e diagnósticos incorretos (RAJPURKAR et al., 2018).

No entanto, junto a esses avanços, emergem desafios complexos relacionados à segurança da informação e à privacidade dos dados sensíveis dos pacientes. Incidentes como o vazamento de 1,5 milhão de registros no sistema SingHealth em 2018 destacam a vulnerabilidade dos sistemas de saúde diante de ameaças cibernéticas e reforçam a urgência de práticas rigorosas de proteção de dados (SINGAPORE MINISTRY OF HEALTH, 2018). Esse cenário alarmante reforça a necessidade urgente de uma governança robusta que garanta segurança e responsabilidade no uso dessas tecnologias.

Frente a esses desafios, o desenvolvimento de diretrizes claras e eficazes é imprescindível. Elas devem equilibrar o avanço tecnológico com a proteção dos direitos fundamentais, assegurando que a inovação na saúde seja, acima de tudo, ética, segura e centrada no paciente.

Este artigo está estruturado em seis seções, que abordam os avanços tecnológicos, a vulnerabilidade dos dados, o marco regulatório, as ameaças cibernéticas, estratégias de proteção e dilemas éticos. Conclui ressaltando a importância de equilibrar inovação e proteção de direitos.

A tecnologia avança rapidamente, trazendo novos desafios e oportunidades. Para entender essas transformações, a metodologia deste estudo é qualitativa.

Este trabalho adota uma abordagem qualitativa, de caráter exploratório e retrospectivo, fundamentada em revisão narrativa da literatura e análise documental. Foram utilizados dados secundários obtidos de artigos científicos, relatórios institucionais, legislações vigentes e estudos de caso.

2 METODOLOGIA

Este trabalho adota uma abordagem qualitativa, exploratória e retrospectiva, fundamentada em revisão narrativa da literatura e análise documental. Foram utilizados dados secundários de artigos científicos, relatórios institucionais, legislações vigentes e estudos de caso no contexto da saúde digital.

A seleção das fontes considerou atualidade (publicações a partir de 2018), relevância temática e diversidade de origem — pública, privada e internacional. Os estudos práticos foram escolhidos por sua representatividade em diagnóstico, gestão hospitalar, prevenção e atendimento ao paciente, priorizando instituições reconhecidas nacionalmente e com divulgação pública de resultados.

Buscou-se também diversidade regional e níveis variados de maturidade digital para um panorama abrangente. As informações dos casos foram validadas por triangulação com fontes confiáveis, como documentos oficiais, reportagens e estudos científicos, garantindo consistência e credibilidade.

Com essa metodologia, exploramos a aplicação da inteligência artificial na saúde, destacando avanços e desafios.

3 MITOS COMUNS SOBRE IA: DESMISTIFICANDO A TECNOLOGIA

Sabemos que, para muitos profissionais de saúde, a ideia de usar IA pode parecer intimidadora. Vamos esclarecer alguns mitos e mostrar como essa tecnologia está aqui para ajudá-lo.

1) **Será que a IA vai substituir os médicos?**

   Não. A IA é uma ferramenta de apoio. Ela pode ajudar a analisar exames ou sugerir diagnósticos, mas a decisão final sempre será do profissional de saúde. Essa é uma distinção fundamental: a tecnologia não veio para tomar o lugar do médico, e sim para ampliar sua capacidade de diagnóstico e decisão.

2) **E se for difícil demais para eu usar no meu dia a dia?**

   Embora a tecnologia por trás da IA seja avançada, as interfaces são projetadas para serem intuitivas. Muitos sistemas de IA podem ser integrados diretamente nos fluxos de trabalho existentes, como prontuários eletrônicos, facilitando a adoção sem que o profissional precise ser um expert em tecnologia.

3) **Posso confiar nos diagnósticos feitos por IA?**

   A confiabilidade da IA depende dos dados com os quais foi treinada. Além disso, sistemas de IA são projetados para complementar seu trabalho, oferecendo suporte baseado em dados, mas sempre sob sua supervisão. Portanto, o julgamento humano permanece insubstituível e essencial para garantir segurança e ética no atendimento.

Embora a IA ofereça grande potencial, seu uso sem regulamentação adequada pode resultar em superdiagnóstico e tratamentos desnecessários, gerando custos e ansiedade. Portanto, os avanços técnicos impressionam, mas seu sucesso depende da implementação responsável, que respeite os princípios éticos fundamentais do cuidado em saúde.

4 AVANÇOS E APLICAÇÕES DA IA NA SAÚDE

A inteligência artificial vem transformando a saúde com resultados mensuráveis em todas as áreas:

1) **Diagnóstico por Imagem:** O sistema DeepMind Health do Google alcançou 94% de precisão na detecção de doenças oculares (DE FAUW et al., 2018), superando especialistas humanos.

No Brasil, o Hospital Albert Einstein utiliza IA para análise de tomografias, reduzindo o tempo de diagnóstico de 30 para 5 minutos.

2) **Medicina Personalizada:** A startup brasileira Mendelics desenvolveu um sistema de análise genômica que reduziu o tempo para diagnóstico de doenças raras de anos para semanas, com um custo 60% menor.
3) **Gestão Hospitalar:** O Hospital das Clínicas de São Paulo implementou algoritmos preditivos que reduziram em 40% as readmissões hospitalares (HC-FMUSP, 2021).
4) **Pesquisa de Medicamentos:** A BenevolentAI identificou em 48 horas potenciais tratamentos para COVID-19 que normalmente levariam meses (RICHARDSON et al., 2021).

Estes exemplos demonstram o potencial transformador da IA, mas exigem infraestrutura tecnológica de segurança e proteção de dados, além da governança ética.

Apesar dos avanços tecnológicos, a proteção dos dados sensíveis é fundamental para garantir a privacidade e a segurança dos pacientes.

Entretanto, para que esses avanços sejam sustentáveis, é imprescindível garantir a proteção rigorosa dos dados sensíveis.

Depois de explorar as aplicações promissoras da IA, é necessário entender os desafios e riscos que acompanham essa tecnologia.

Apesar dos avanços promissores e das aplicações concretas que transformam a saúde, é fundamental compreender os desafios e riscos que acompanham essa tecnologia. Somente conhecendo essas limitações poderemos garantir que a inovação ocorra de forma segura, ética e eficaz.

5 DESAFIOS E RISCOS RELACIONADOS À IA NA SAÚDE

Apesar dos avanços tecnológicos, a proteção dos dados sensíveis é fundamental para garantir a privacidade e a segurança dos pacientes. Informações sobre a saúde de uma pessoa são pessoais e sensíveis, exigindo um cuidado extra quando são coletadas, armazenadas ou utilizadas.

5.1 PRIVACIDADE E REGULAMENTAÇÃO

No Brasil, a Lei Geral de Proteção de Dados (LGPD) define claramente que esse tipo de informação deve ser tratado com máxima proteção e apenas pode ser usado em situações específicas e justificadas por lei.

Tanto a LGPD (Lei nº 13.709/2018) no Brasil quanto o GDPR na Europa (o regulamento europeu de proteção de dados) apontam que, como regra, o consentimento explícito do paciente é a principal base legal para o uso de dados de saúde.

Portanto, o titular (dono do dado) precisa concordar de forma clara e específica com o uso de seus dados, informando para qual finalidade eles serão utilizados; esse consentimento deve ser livre, apresentado de forma clara e destacada, com linguagem acessível e objetiva.

5.2 COMO ESSES DADOS DEVEM SER PROTEGIDOS?

Além do consentimento, existem cuidados adicionais que as instituições (como hospitais, clínicas ou pesquisadores) devem seguir para garantir que os dados de saúde sejam usados de forma segura e responsável. Veja alguns deles:

1) Pseudonimização: Em pesquisas científicas, é obrigatório usar técnicas que "despersonalizem" os dados. Isso significa que os dados são tratados de forma que não identifiquem diretamente a pessoa. Isso está previsto no Art. 89 do GDPR.
2) Tempo de retenção: Os dados só podem ser guardados pelo tempo necessário para cumprir sua finalidade. Depois disso, devem ser eliminados de forma segura. A LGPD trata disso no Art. 15.
3) Acesso restrito: O acesso às informações deve ser limitado apenas a pessoas autorizadas, como médicos ou profissionais da área da saúde diretamente envolvidos no atendimento. O Conselho Federal de Medicina (Resolução CFM 2.217/2018) determina que todo acesso deve ser registrado.

Os dados de saúde não são como qualquer outro tipo de dado. Eles dizem respeito à parte mais íntima da vida de uma pessoa. Por isso, tanto a LGPD quanto outras legislações internacionais colocam regras rígidas para proteger essas informações. Sempre que possível, é essencial que o paciente esteja no controle, por meio de um consentimento claro e informado.

Com a metodologia estabelecida, analisamos a incidência e os impactos dos ataques cibernéticos no setor de saúde.

Diante dos requisitos legais e éticos para proteção dos dados, é fundamental compreender as ameaças cibernéticas que vulnerabilizam o setor.

5.3 RISCOS PARA USO DE IA EM ATIVIDADES ADMINISTRATIVAS E MÉDICAS

Além dos riscos gerais relacionados à segurança da informação e à privacidade dos dados sensíveis, o uso da inteligência artificial (IA) na saúde apresenta desafios específicos tanto na esfera administrativa quanto na prática clínica. Esses riscos demandam atenção redobrada para evitar impactos negativos operacionais, éticos e legais.

1) Automação de Processos Inadequada

A automação de tarefas administrativas por meio de bots e sistemas inteligentes pode não considerar todas as variáveis e nuances das atividades humanas. Isso pode resultar em erros ou decisões incorretas. Por exemplo, processos de agendamento, processamento de documentos ou comunicação automatizada podem apresentar distorções que comprometem a eficiência e geram retrabalho, afetando o fluxo do atendimento hospitalar e a experiência do paciente.

2) **Falta de Transparência**

Muitos sistemas de IA operam como "caixa preta", entregando resultados sem explicar claramente o processo que levou àquela decisão. Essa opacidade dificulta a rastreabilidade das ações e a justificativa de decisões automatizadas, o que gera perda de confiança por parte de colaboradores e pacientes, além de complicar a conformidade com regulamentações que exigem auditoria e transparência.

3) **Dependência Excessiva de Sistemas Automatizados**

A alta dependência de sistemas automatizados pode tornar a organização vulnerável a falhas técnicas ou ataques cibernéticos. Em situações de instabilidade, a inabilidade de realizar tarefas manualmente, como controle financeiro, gestão de recursos humanos ou suporte ao paciente, pode levar à paralisação das operações essenciais, colocando em risco a continuidade dos serviços na área da saúde.

4) **Exposição a Ameaças Cibernéticas**

Bots e sistemas automatizados de IA são alvos potenciais de ataques cibernéticos, como phishing, injeção de código malicioso e outras vulnerabilidades exploradas por hackers. O comprometimento desses sistemas pode resultar em acessos indevidos, vazamento de dados sensíveis e interrupção dos serviços administrativos, agravando ainda mais os riscos de segurança da informação no ambiente hospitalar.

5) **Erros na Interpretação de Dados**

A IA depende da correta interpretação dos dados inseridos nos sistemas. Erros na leitura ou análise dessas informações podem levar a decisões administrativas equivocadas, afetando o desempenho organizacional e prejudicando o planejamento estratégico. Na área médica, interpretações incorretas podem gerar diagnósticos errôneos, comprometendo o tratamento do paciente.

6) **Viés de Dados**

Os modelos de IA aprendem com dados históricos que, se contaminados por vieses sociais, econômicos ou culturais, reproduzem e amplificam essas distorções. Isso pode resultar em decisões injustas ou discriminatórias, como priorização inadequada em processos

administrativos ou diagnósticos imprecisos para grupos minoritários, comprometendo a equidade e a ética na saúde.

7) **Qualidade dos Dados**

A qualidade dos dados é fundamental para o desempenho da IA. Dados desatualizados, incompletos ou incorretos prejudicam a precisão das análises, levando a resultados distorcidos. Isso pode impactar negativamente as operações hospitalares e a qualidade do atendimento médico.

8) **Interpretação Incorreta de Padrões**

A IA pode identificar correlações ou padrões errôneos em conjuntos de dados, resultando em interpretações equivocadas. Isso pode levar à implementação de estratégias ineficazes, desperdício de recursos e riscos à segurança do paciente.

9) **Risco de Overfitting**

Modelos de machine learning treinados excessivamente em conjuntos de dados específicos podem apresentar baixa capacidade de generalização, falhando ao serem aplicados a novos dados ou cenários. Isso reduz a eficácia e confiabilidade dos sistemas de IA em saúde.

A IA aplicada em diagnóstico por imagem frequentemente utiliza redes neurais convolucionais (CNNs), que são capazes de identificar padrões visuais complexos.

Frente a esses desafios complexos, torna-se imperativo estabelecer uma governança estruturada, pautada em ética e responsabilidade, para mitigar riscos e assegurar a proteção dos pacientes e profissionais envolvidos. Entre os desafios, os riscos éticos merecem atenção especial, pois a falta de transparência e os vieses podem comprometer a justiça e equidade no atendimento.

6 GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: ESTRUTURA, BENEFÍCIOS E DESAFIOS

A implementação de um framework de governança para a inteligência artificial (IA) na saúde é imperativa diante dos desafios éticos, técnicos e operacionais que essa tecnologia apresenta. Mais do que uma exigência legal, a governança representa uma estratégia essencial para garantir que os sistemas de IA sejam utilizados de forma segura, justa, transparente e alinhada aos interesses dos pacientes, profissionais de saúde e instituições.

6.1 ESTRUTURA DA GOVERNANÇA: PILARES FUNDAMENTAIS E FUNÇÕES

Para que a governança seja eficaz, é necessário que ela se baseie em pilares interdependentes, que atuem em sinergia para garantir inovação responsável e mitigação de riscos:

1) **Comitês Multidisciplinares: Decisões Compartilhadas e Responsáveis**

A criação de comitês multidisciplinares é o primeiro passo para assegurar uma governança ética e técnica. Esses comitês devem ser compostos por profissionais das áreas médica, tecnológica, jurídica, bioética e representantes dos pacientes, garantindo uma visão ampla e equilibrada.

Esses grupos atuam como guardiões da ética e segurança no uso da IA avaliando previamente algoritmos para identificar potenciais vieses, falhas técnicas e impactos negativos na prática clínica. Além disso, acompanham continuamente a aplicação dos sistemas, corrigindo rumos e ajustando processos sempre que necessário para preservar o cuidado humano e a qualidade assistencial. Essa supervisão evita decisões automatizadas erradas ou injustas que possam comprometer a saúde dos pacientes.

2) **Auditorias Periódicas: Fiscalização Contínua e Preventiva**

Apenas a existência dos comitês não é suficiente para garantir segurança e responsabilidade. Auditorias regulares e sistemáticas, preferencialmente trimestrais, são indispensáveis para revisar o funcionamento dos sistemas de IA, especialmente em ambientes críticos, como a geração de laudos médicos ou suporte à decisão clínica.

Essas auditorias têm a função de detectar desvios éticos, falhas técnicas, vieses e possíveis ameaças à segurança da informação. Elas também avaliam a conformidade dos sistemas com a legislação vigente, incluindo a Lei Geral de Proteção de Dados (LGPD) e normas internacionais aplicáveis. Além disso, asseguram que as decisões automatizadas sejam explicáveis e justifiquem o direito dos pacientes à transparência, fundamental para o respeito à autonomia e confiança.

3) **Transparência e Revisão Humana: Garantia de Controle e Confiança**

A transparência é uma condição indispensável para a aceitação e sucesso da IA na saúde. Médicos, pacientes e demais envolvidos devem receber informações claras e acessíveis sobre o funcionamento dos sistemas, os critérios adotados e as decisões automatizadas. Relatórios compreensíveis e comunicação efetiva criam um ambiente de confiança e colaboração.

Além disso, a supervisão humana deve ser parte integrante do processo. Os profissionais de saúde precisam poder revisar, contestar e, quando necessário, reverter decisões automatizadas que possam colocar em risco a segurança do paciente. Os pacientes, por sua vez, devem ter canais para questionar diagnósticos ou tratamentos gerados pela IA solicitando uma segunda opinião quando desejarem. Esse equilíbrio assegura que a IA seja uma ferramenta de apoio e não um árbitro exclusivo.

4) **Benefícios da Governança Bem Estruturada**

Quando esses pilares operam de forma integrada e efetiva, os ganhos são evidentes. Pesquisas indicam que a implementação de uma governança sólida pode reduzir em até 72% os litígios

envolvendo diagnósticos automatizados, enquanto a confiança dos pacientes aumenta em cerca de 40% quando lhes são prestadas informações claras e transparentes sobre o uso da IA.

Além disso, as instituições que adotam práticas rigorosas de governança se protegem contra multas e sanções previstas em legislações como a LGPD, reduzindo riscos legais e garantindo maior segurança jurídica. A governança, portanto, transforma-se em um instrumento de valorização institucional, qualidade assistencial e sustentabilidade econômica.

5) **Desafios e Riscos da Ausência de Governança**

Por outro lado, a negligência com a governança expõe as organizações de saúde a graves consequências. Sistemas de IA sem supervisão adequada podem gerar erros, decisões enviesadas e injustas, além de falhas que comprometam a segurança do paciente e a integridade dos dados. Essas falhas resultam em prejuízos financeiros, danos à reputação e desconfiança tanto dos profissionais quanto dos pacientes.

A desconfiança profissional é um fator crítico. Pesquisa do CREMESP (2023) revela que 68% dos médicos brasileiros não confiam em sistemas de IA que não são submetidos a auditorias ou supervisão ética. Essa rejeição pode dificultar a implementação e o uso efetivo da IA limitando seu potencial transformador.

6) **Papéis e Responsabilidades Claras: O Alicerce da Governança**

Para que a governança deixe de ser um conceito abstrato e se torne prática eficaz, é fundamental que as responsabilidades sejam claramente definidas. Desenvolvedores, equipes técnicas, profissionais de saúde, gestores e órgãos reguladores precisam atuar coordenadamente, com papéis específicos na supervisão, auditoria, treinamento e comunicação.

Essa rede de responsabilidades cria um ambiente seguro e confiável, em que a IA é uma aliada do cuidado humano, sempre com a presença e o julgamento clínico e ético dos profissionais.

A seguir, apresentamos uma matriz de responsabilidades que define claramente os papéis essenciais na governança da inteligência artificial na saúde, garantindo que cada ator envolvido saiba suas atribuições para um uso ético, seguro e eficaz da tecnologia.

Matriz de Responsabilidade e Desafios das Ameaças Cibernéticas na Saúde Digital						
Atividades / Papéis	**Desenvolvedores**	**Comitê Multidisciplinar**	**Profissionais de Saúde**	**Gestores Hospitalares**	**Órgãos Reguladores**	**Pacientes**
Desenvolvimento do sistema de IA	R	C	I	I	I	I
Avaliação ética e legal do sistema	I	R	C	C	C	I
Validação clínica e testes	C	R	R	I	I	I
Monitoramento contínuo do sistema	C	R	C	I	I	I
Auditorias periódicas	I	R	C	C	A	I
Treinamento dos profissionais de saúde	I	C	R	A	I	I
Comunicação e transparência com pacientes	I	C	C	R	I	A
Revisão e contestação de decisões da IA	I	C	R	I	I	A
Conformidade com LGPD e normas legais	C	R	I	A	A	I
Definição de políticas internas de IA	I	R	C	A	C	I

Legenda:

- R (Responsável): Executa a atividade A (Aprovador): Autoridade final que aprova a atividade
- C (Consultado): Consulta e contribui com informações I (Informado): Recebe informações sobre o progresso ou resultados

Definir essas responsabilidades é fundamental para garantir que a governança da IA na saúde funcione de maneira eficaz, contemplando todos os aspectos técnicos, éticos e legais envolvidos.

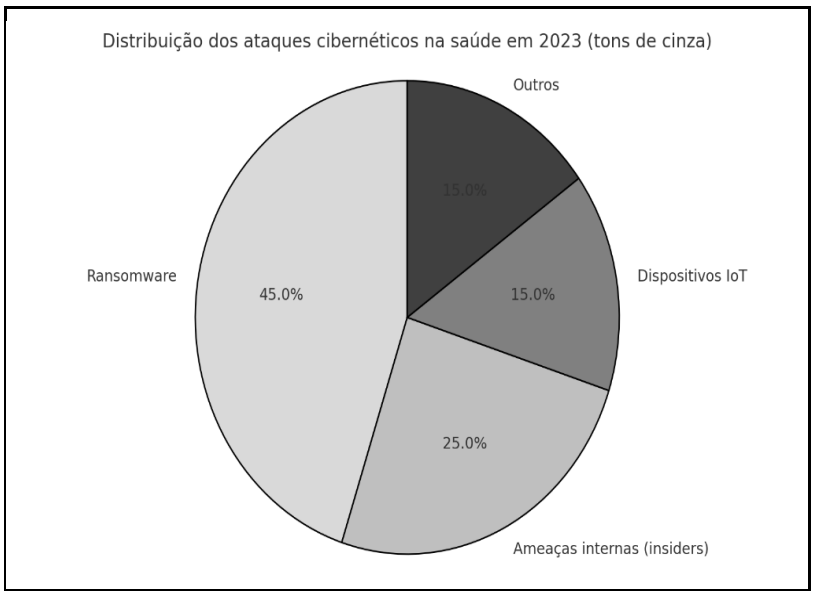
Entretanto, a governança não atua isoladamente. Ela é peça-chave para enfrentar as ameaças cibernéticas, que representam um dos maiores desafios para o setor da saúde. Esses ataques podem comprometer dados sensíveis, afetar a operação dos serviços clínicos e colocar em risco a segurança dos pacientes.

Por isso, é imprescindível que as equipes técnicas, clínicas, gestores e órgãos reguladores atuem de forma coordenada, com responsabilidades bem definidas, para prevenir, detectar e responder rapidamente a essas ameaças digitais.

Assim, a matriz de responsabilidades torna-se um instrumento crucial para fortalecer a defesa cibernética da saúde, promovendo um ambiente digital resiliente, ético e seguro, onde a inteligência artificial possa ser uma verdadeira aliada do cuidado humano.

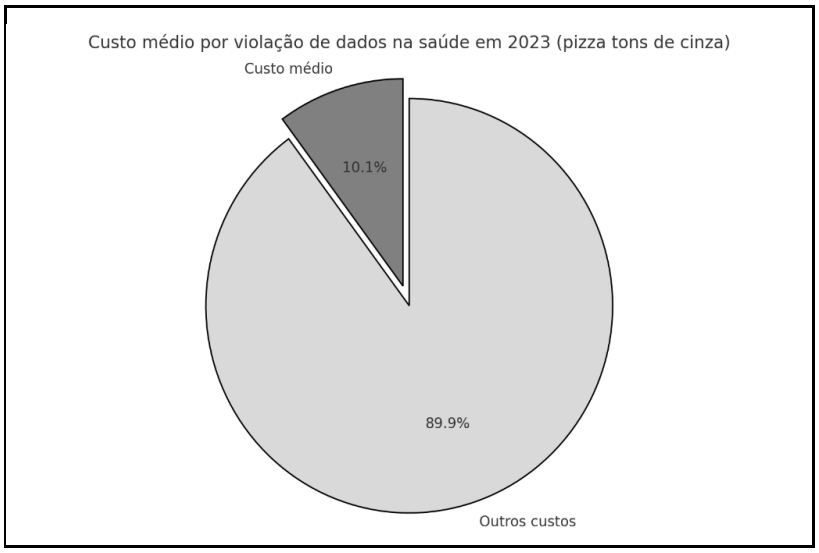
7 AMEAÇAS CIBERNÉTICAS

Em paralelo à necessidade de governança ética, o setor da saúde enfrenta uma crescente ameaça no campo da segurança digital. Em 2023, aproximadamente 34% dos ataques virtuais foram direcionados a hospitais, clínicas e operadoras, destacando sua alta vulnerabilidade (CHECK POINT, 2023). Entre as ameaças mais comuns, o ransomware lidera com 45% dos incidentes, seguido por invasões internas e ataques a dispositivos médicos conectados. Esses dados evidenciam não só a frequência das ameaças, mas também seu impacto financeiro significativo, que será detalhado a seguir.



Fonte: CHECK POINT, 2023.Adaptada pela autora

Esses dados não apenas revelam a frequência e variedade das ameaças, mas também destacam seu impacto financeiro significativo. Em 2023, o custo médio por violação de dados no setor de saúde foi estimado em US$ 10,1 milhões, evidenciando que os ataques comprometem não só a segurança dos dados, mas também causam prejuízos econômicos substanciais. Esse cenário reforça a necessidade de investimentos em governança e medidas eficazes de proteção.



Fonte: CHECK POINT, 2023. Adaptada pela autora

7.1 RISCOS ESPECÍFICOS PARA IA EM ATIVIDADES ADMINISTRATIVAS E MÉDICAS

Além dos riscos gerais de segurança e privacidade já mencionados, a adoção da inteligência artificial traz desafios específicos que exigem atenção redobrada, tanto na esfera administrativa quanto na prática médica.

1) **Automação inadequada pode gerar erros operacionais.**

   Muitos processos administrativos são padronizados para humanos, que conseguem captar nuances e exceções. Bots e sistemas automatizados podem falhar ao lidar com essas variações, causando erros como agendamentos duplicados, falhas no processamento de documentos ou respostas automáticas incorretas. Esses erros podem impactar diretamente a eficiência operacional, gerar retrabalho e até comprometer a experiência do paciente.

2) **Falta de transparência dificulta auditoria e confiança.**

   IA frequentemente opera como uma "caixa preta": o sistema entrega um resultado sem explicar claramente como chegou a ele. Essa opacidade cria barreiras para que auditores, gestores e até mesmo os próprios profissionais de saúde entendam e validem as decisões tomadas pela IA. Sem transparência, cresce a desconfiança e aumenta o risco de uso indevido ou erros não detectados.

3) **Dependência excessiva pode comprometer continuidade operacional.**

   A dependência total de sistemas automatizados cria um ponto único de falha. Se o sistema de IA apresentar instabilidade, for alvo de ataques cibernético ou sofrer uma pane técnica, toda a rotina administrativa ou clínica pode parar, sem que a equipe esteja preparada para assumir manualmente. Essa vulnerabilidade ameaça a continuidade dos serviços, que no setor da saúde é uma questão crítica, pois atrasos podem causar danos irreparáveis.

4) **Viés de dados pode reforçar desigualdades.**

Os algoritmos aprendem com dados históricos. Se esses dados contiverem vieses sociais, culturais ou econômicos, a IA replicará e até amplificará essas distorções. Isso pode levar a decisões injustas, como priorizar determinados grupos em processos administrativos ou diagnosticar incorretamente pacientes de minorias, prejudicando a equidade no atendimento e a ética do sistema.

5) **Erros diagnósticos por interpretação incorreta.**

Na avaliação de laudos e exames, a IA pode interpretar incorretamente imagens, sinais ou dados clínicos, especialmente quando os dados são incompletos ou de baixa qualidade. Esses erros podem resultar em diagnósticos equivocados, levando a tratamentos inadequados, atrasos ou danos à saúde do paciente.

6) **Falta de supervisão humana pode colocar vidas em risco.**

A automação completa sem supervisão médica adequada elimina a camada crítica de verificação que garante a segurança do paciente. Decisões automatizadas, quando não revisadas por profissionais capacitados, podem falhar em identificar sinais sutis ou alertas importantes, aumentando o risco de eventos adversos e colocando vidas em perigo.

7) **Questões legais e éticas mal definidas.**

A responsabilidade por erros e falhas da IA ainda é um território nebuloso. Não está claro quem responde legalmente quando um sistema de IA comete um erro, se o médico, a instituição ou o desenvolvedor do software. Essa falta de definição cria insegurança jurídica para os profissionais de saúde e abre espaço para conflitos éticos, o que pode reduzir a confiança dos pacientes e comprometer a adoção segura da tecnologia.

7.2 CAUSAS DA VULNERABILIDADE

Para entender por que o setor de saúde é tão suscetível a esses ataques, é essencial analisar os principais fatores que aumentam essa exposição.

Essa vulnerabilidade não é por acaso. Ela se deve a três fatores principais:

1) **Alto valor dos dados médicos:** Informações de saúde são extremamente valiosas. Um prontuário completo pode chegar a valer até US$ 1.000 no mercado negro (FBI, 2022). Para os criminosos, representam um alto valor para práticas ilícitas como fraudes, extorsões e comercialização ilegal de informações.
2) **Tecnologia desatualizada:** Muitos hospitais ainda usam sistemas antigos, que não recebem mais atualizações de segurança. Estima-se que 68% dessas instituições operam com softwares obsoletos (HIPAA Journal, 2023), o que abre brechas fáceis para ataques.

3) **Pressão por continuidade dos serviços:** Diferente de outros setores, os hospitais não podem parar. Essa urgência faz com que as instituições de saúde sejam até três vezes mais propensas a pagar resgates rapidamente em casos de sequestro de dados (ransomware) (Sophos, 2023).

7.3 TIPOS DE ATAQUES MAIS COMUNS

Em média, organizações no mundo todo sofreram 1.248 ataques por semana em 2023 (Check Point). No setor da saúde, os mais comuns incluem:

1) **Ransomware:** Em 2021, um ataque desse tipo ao SUS causou a paralisação de mais de 600 unidades de saúde por semanas.
2) **Ameaças internas (insiders):** Em 2022, um caso ganhou destaque quando um enfermeiro foi flagrado vendendo dados sigilosos de celebridades.
3) **Dispositivos médicos conectados (IoT):** Equipamentos como marcapassos e bombas de insulina podem ser invadidos por hackers, o que levanta sérias preocupações de segurança (FDA, 2023).

Diante desses fatores, é urgente implementar estratégias eficazes que mitiguem os riscos e fortaleçam a segurança.

Diante dos riscos evidenciados, torna-se essencial implementar estratégias robustas de proteção e governança.

Além das medidas técnicas, a transformação digital impõe importantes dilemas éticos que merecem análise aprofundada.

7.4 A IMPORTÂNCIA DA PREVENÇÃO E TRÊS ESTRATÉGIAS EFICAZES

Em vez de reagir após um ataque, o caminho mais estratégico e seguro, é agir antes que o problema aconteça. E é nesse momento que entra a adoção da governança para segurança e privacidade, que não deve ser vista como um custo, mas como uma parte necessária para a continuidade dos serviços de forma segura.

A adoção da governança significa ter processos claros, responsabilidades definidas e uma cultura de segurança e proteção de dados que envolva todos os setores da instituição. Ela permite antecipar e mitigar riscos, reduzir vulnerabilidades e responder rapidamente a qualquer sinal de ameaça.

Além disso, algumas soluções práticas e tecnológicas têm se mostrado especialmente eficazes:

1) **Criptografia:** Uma espécie de “cadeado digital” que protege os dados mesmo se forem interceptados. Assim, informações de pacientes continuam seguras.
2) **Microssegmentação:** É como dividir o hospital em áreas digitais isoladas. Se um sistema for atacado (por exemplo, o da recepção), outros setores críticos, como as UTIs digitais, continuam protegidos.

3) **Inteligência Artificial aplicada à cibersegurança:** Sistemas inteligentes conseguem identificar comportamentos suspeitos em tempo real, como acessos estranhos ou movimentações fora do padrão, e agir antes que o dano ocorra (MITRE, 2023).
4) **Treinamento e conscientização:** Mesmo com toda a tecnologia disponível, o fator humano continua sendo uma das principais portas de entrada para ataques. Por isso, é imprescindível investir continuamente na capacitação de todos os profissionais envolvidos, desde áreas administrativas até a equipe médica e de gestão.

Além dos aspectos técnicos e financeiros, a adoção da inteligência artificial na saúde traz consigo complexos dilemas éticos.

8 DILEMAS ÉTICOS EM TECNOLOGIAS EMERGENTES

Cuidar da ética na saúde digital significa garantir que o uso de tecnologia seja seguro, justo, transparente e, acima de tudo, humano e equilibrado. Com o avanço acelerado da tecnologia na área da saúde, como a inteligência artificial (IA), algoritmos preditivos e sistemas automatizados surgem também novos dilemas éticos que não podem ser ignorados. Lidar com essas questões de forma responsável não é um opcional, é um requisito. Quando se trata da vida e da saúde das pessoas, agir com ética é o que garante que a tecnologia seja aliada e não um risco.

Ignorar esse debate pode colocar em jogo a confiança, a segurança e até a credibilidade das instituições. Veja alguns dos dilemas mais urgentes:

1) **Perda de confiança dos pacientes**

   A confiança é a base de qualquer relação na área da saúde. No entanto, 62% dos pacientes ainda desconfiam do uso de inteligência artificial em diagnósticos e tratamentos (PEW, 2023). Se a tecnologia não for apresentada com transparência e empatia, garantindo total segurança e integridade ela pode afastar as pessoas em vez de ajudá-las.

2) **Viés nos algoritmos**

   Sistemas de IA aprendem com dados. Se esses dados forem incompletos ou mal distribuídos, por exemplo, com pouca representação de determinados grupos étnicos ou sociais, os resultados podem ser injustos ou equivocados. Um estudo mostrou que modelos com esse tipo de viés erram em 34% dos diagnósticos (Obermeyer, 2023). Isso significa que a tecnologia pode reforçar desigualdades, em vez de corrigi-las.

3) **Responsabilidade sobre o uso das tecnologias**

   Se um diagnóstico automatizado falha, quem assume a responsabilidade? O médico? O hospital? O desenvolvedor do software? Essa é uma questão ainda em aberto, e a falta de clareza pode gerar insegurança jurídica e ética para todos os envolvidos, inclusive os pacientes.

Essas ameaças demonstram que a governança não pode ser vista como uma obrigação burocrática, mas como uma estratégia vital para proteger pacientes, profissionais e instituições. Somente com políticas integradas de segurança, auditorias constantes e colaboração multidisciplinar será possível enfrentar o complexo ambiente de riscos digitais da saúde.

9 CASO PRÁTICO

A teoria e as diretrizes são fundamentais, mas é na prática que se mede a verdadeira eficácia da inteligência artificial na saúde. Os desafios técnicos, éticos e de segurança só ganham sentido quando confrontados com as experiências reais de instituições que adotaram essas tecnologias.

Nesta seção, apresentamos exemplos concretos de como hospitais e clínicas,— no Brasil e no mundo, têm integrado a IA em suas rotinas, enfrentando as complexidades do ambiente digital, garantindo a proteção dos dados sensíveis e aplicando governança robusta para mitigar riscos.

Esses casos ilustram não apenas os benefícios tangíveis da inovação, como a redução de tempos de diagnóstico e a melhora na gestão hospitalar, mas também mostram como a adoção consciente da tecnologia pode ser um diferencial estratégico para segurança, eficiência e qualidade do atendimento.

Ao analisar essas experiências, fica evidente que a implementação da IA na saúde não é um caminho linear nem isento de desafios. Por isso, entender os sucessos e as lições aprendidas nessas instituições é essencial para quem deseja navegar com segurança e responsabilidade nesse cenário em rápida evolução.

9.1 CASO 01: DRGBRASIL

- **Desafio:** Dificuldade na gestão hospitalar eficiente, prevenção de complicações e uso racional de recursos.
- **Solução:** Implementação de algoritmos de *machine learning* para analisar grandes volumes de dados clínicos e operacionais.
- **Resultado:** Identificação precoce de doenças, otimização de leitos e processos assistenciais, com melhoria da segurança do paciente e redução de desperdícios.

Leia mais: https://www.drgbrasil.com.br/valoremsaude/inteligencia-artificial-na-saude/

9.2 CASO 02: SIRIO-LIBANES

- **Desafio:** Tornar o atendimento médico mais ágil, seguro e livre de burocracias.
- **Solução:** Criação da plataforma Sofya, com uso de IA e reconhecimento de voz para automatizar a anamnese e preencher prontuários.

- **Resultado:** Maior eficiência clínica, redução de erros e tempo gasto com tarefas administrativas. Fortalecimento da governança e da ética digital com uso de dados anonimizados.

Leia mais: https://www.projetodraft.com/transformacao-digital-e-uma-questao-de-saude-o-sirio-libanes-vem-evoluindo-para-tornar-o-cuidado-medico-mais-agil-e-seguro

9.3 CASO 03: CLÍNICA CEU

- **Desafio:** Melhorar a precisão e rapidez no diagnóstico por imagem, especialmente para doenças em estágio inicial.
- **Solução:** Utilização de IA para análise de radiografias, tomografias e correlação com outros dados clínicos.
- **Resultado:** Diagnósticos mais precoces e confiáveis, aumento da segurança no cuidado e apoio ao monitoramento contínuo de pacientes crônicos.

Leia mais: https://www.clinicaceu.com.br/blog/ia-qual-seu-papel-no-rastreio-de-doencas/

9.4 CASO 04: UNIMED-BH

- **Desafio:** Agilizar o processo de autorização de exames e procedimentos, reduzindo o tempo de espera do paciente.
- **Solução:** Uso de IA com algoritmos de machine learning para classificar e aprovar automaticamente solicitações com base em padrões históricos.
- **Resultado:** Aprovação instantânea de 30% dos pedidos, com 99,8% de acurácia e queda no tempo médio de resposta para 10 minutos. Aumento na satisfação dos usuários.

Leia mais: https://www.plano-de-saude-saopaulo.com.br/noticias-planos-de-saude/unimed-bh-agiliza-consultas-e-exames/

9.5 CASO 05: HOSPITAL ALEMÃO OSWALDO CRUZ

- **Desafio:** Monitorar e acompanhar continuamente pacientes com doenças crônicas (como diabetes, hipertensão e insuficiência cardíaca), reduzindo internações evitáveis e melhorando a adesão ao tratamento.
- **Solução:** Desenvolvimento de um sistema preditivo com IA para identificar riscos de descompensação clínica com base em sinais vitais, exames laboratoriais e histórico eletrônico do paciente. O sistema aciona equipes de saúde para intervenções remotas ou presenciais em tempo oportuno.

- **Resultado:** O modelo de engenharia clínica, inteligência artificial e *wearables* contribuem para a eficiência e segurança no atendimento aos pacientes, mas não detalha o caso específico do sistema preditivo para pacientes crônicos com os resultados quantitativos citados.

Leia mais: https://www.hospitaloswaldocruz.org.br/imprensa/releases/engenharia-clinica-inteligencia-artificial-e-wearables-trazem-maior-eficiencia-e-seguranca-no-atendimento-aos-pacientes/

A adoção de tecnologia não traz apenas benefícios, nos últimos anos, o setor de saúde no Brasil tem enfrentado desafios significativos relacionados à segurança da informação, com diversos incidentes de exploração de vulnerabilidades resultando em comprometimento de dados sensíveis. A seguir, apresento três casos recentes que ilustram essas questões:

9.6 CASO 01: HOSPITAL UNIVERSITÁRIO DA USP (HU-USP)

- **Descrição do Incidente:** Em 23 de março de 2024, o Hospital Universitário da Universidade de São Paulo sofreu um ataque cibernético que paralisou serviços essenciais e afetou o atendimento à população.
- **Impacto:** O ataque interrompeu operações críticas do hospital, comprometendo a prestação de serviços médicos e expondo vulnerabilidades nos sistemas de segurança da instituição.

Leia mais: https://tecnoblog.net/noticias/hospital-da-usp-sofre-ataque-hacker-e-suspende-consultas-e-exames-de-rotina/

9.7 CASO 02: MINISTÉRIO DA SAÚDE

- **Descrição do Incidente:** Em novembro de 2022, foi constatada a venda ilegal de bases de dados administrativas oriundas de sistemas governamentais, incluindo o CADSUS (Sistema de Cadastramento de Usuários do Sistema Único de Saúde) e dados de imunização do e-SUS Notifica.
- **Impacto:** Embora não tenha sido possível afirmar se as bases de dados comercializadas ilegalmente eram atualizadas ou antigas, o incidente evidenciou falhas na proteção de informações sensíveis dos cidadãos.

Leia mais: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais

9.8 CASO 03. HOSPITAL DE CÂNCER DE BARRETOS

- **Descrição do Incidente:** O Hospital de Câncer de Barretos foi alvo de um ataque cibernético no qual os criminosos utilizaram ransomware para criptografar dados e exigiram um resgate para a liberação das informações.
- **Impacto:** Os atacantes solicitaram US$ 300 por máquina afetada, totalizando um custo potencial de US$ 360 mil (aproximadamente R$ 1,08 milhão) para o hospital.

Leia mais: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.22.pdf

Esses casos ressaltam a importância de investimentos contínuos em cibersegurança no setor de saúde, visando proteger informações e garantir a continuidade dos serviços à população. Entretanto, para que essas ações sejam efetivas e sistemáticas, é necessário estabelecer diretrizes claras e abrangentes que guiem o uso seguro e ético da inteligência artificial na saúde.

10 DIRETRIZES ORIENTATIVAS E SEGURANÇA NA IA EM SAÚDE

A inteligência artificial promete revolucionar a saúde, mas a adoção dessa tecnologia enfrenta desafios que vão muito além do desenvolvimento de algoritmos sofisticados. A questão central não é quantos sistemas inteligentes criamos, mas se conseguimos garantir que esses sistemas não causem danos, respeitando o princípio hipocrático fundamental: primum non nocere (antes de tudo, não causar dano).

Para navegar nesse terreno complexo, são propostas três diretrizes essenciais: adoção obrigatória de padrões rigorosos de segurança cibernética; criação de diretrizes éticas e técnicas com participação multidisciplinar para auditorias contínuas; e transparência real com os pacientes sobre o uso de seus dados e decisões automatizadas que impactam seus tratamentos.

Porém, aqui reside o grande dilema prático: será que estamos prontos para implementar essas medidas de forma eficaz? A experiência dolorosa do Hospital Universitário de Vermont, que sofreu um ataque ransomware que cancelou cirurgias por semanas, é um alerta cruel. Esse tipo de incidente expõe que a fragilidade digital na saúde pode custar vidas, não é mais uma questão hipotética, é uma realidade brutal.

Além disso, a ameaça vai além da interrupção operacional. Imagine se um ataque não apenas paralisa exames, mas altera silenciosamente dosagens em prontuários eletrônicos. Ou que dados genéticos vazem e sejam usados para discriminar famílias em seguros de saúde e vida. Essas possibilidades não são ficção científica, mas riscos concretos que desafiam nossa capacidade regulatória, técnica e ética.

A discussão crítica deve, portanto, abordar o quanto as instituições e governos estão preparados para enfrentar essa realidade. O custo para garantir segurança e ética é alto, e envolve investimentos, capacitação, mudanças culturais e legislação eficaz. Sem isso, corremos o risco de transformar a promessa da IA em uma fonte de novos danos, ampliando desigualdades e fragilizando ainda mais a confiança dos pacientes.

Em última análise, a verdadeira medida do progresso na saúde digital será a capacidade de prevenir tragédias, e não apenas a velocidade em que implantamos tecnologias. A escolha está posta: seremos pioneiros na construção de um futuro ético, seguro e responsável, ou simples espectadores, e vítimas de crises anunciadas.

11 GLOSSÁRIO

- **Anonimização de Dados:** Processo de remoção ou alteração de informações que permitam a identificação direta ou indireta de um indivíduo, conforme definido no Art. 12 da LGPD.
- **Aprendizado de Máquina (Machine Learning):** Subcampo da inteligência artificial que permite aos sistemas aprenderem e melhorarem automaticamente a partir de dados, sem serem explicitamente programados para tarefas específicas.
- **Aprendizado Federado (Federated Learning):** Técnica de aprendizado de máquina distribuído onde os dados permanecem localizados nos dispositivos de origem, permitindo o treinamento colaborativo de modelos sem a necessidade de centralizar informações sensíveis.
- **Auditoria (técnica, ética):** Processo sistemático de avaliação dos sistemas de IA para verificar conformidade técnica, legal e ética, identificando falhas, vieses e riscos.
- **Auditoria Contínua:** Processo permanente de monitoramento e revisão dos sistemas de IA para assegurar sua conformidade e desempenho ao longo do tempo.
- **Big Data:** Conjunto massivo de dados estruturados e não estruturados que, quando analisados por ferramentas específicas, revelam padrões e tendências aplicáveis à pesquisa em saúde.
- **Blockchain:** Tecnologia de registro distribuído que armazena informações em blocos criptografados e imutáveis, utilizada para garantir rastreabilidade e segurança em bancos de dados médicos.
- **Comitê Multidisciplinar:** Grupo formado por profissionais de diversas áreas (medicina, direito, tecnologia, bioética e pacientes) que supervisiona o desenvolvimento e aplicação da IA para garantir decisões equilibradas e éticas.
- **Consentimento Informado:** Direito dos pacientes de receber informações claras e completas sobre o uso de seus dados e sistemas automatizados que influenciam seu tratamento, podendo aceitar ou recusar.
- **Criptografia:** Método avançado de criptografia que permite processar dados mantendo-os criptografados, usado para análises seguras sem expor informações sensíveis.
- **Dados Sensíveis:** Informações pessoais que demandam maior proteção devido à sua natureza íntima, como dados de saúde, genéticos, biométricos e outros.

- **Decisão Automatizada:** Resultado gerado por sistemas de IA que influencia ações clínicas sem intervenção humana direta.
- **Diagnóstico Automatizado:** Processo em que sistemas de IA auxiliam na análise e interpretação de dados clínicos para sugerir diagnósticos médicos.
- **Ética em IA:** Conjunto de princípios que orientam o desenvolvimento e uso responsável da inteligência artificial, garantindo respeito à dignidade humana, justiça e transparência.
- **Falha Técnica:** Erro ou defeito em sistemas de IA que pode afetar seu funcionamento ou gerar resultados incorretos.
- **Framework de Governança:** Estrutura organizacional e normativa que define políticas, processos e responsabilidades para o uso da IA.
- **GDPR (General Data Protection Regulation):** Regulamento europeu (UE 2016/679) que estabelece diretrizes para proteção de dados pessoais, servindo como base para leis como a LGPD.
- **Governança:** Conjunto de processos, políticas e estruturas organizacionais que garantem o uso responsável, seguro e ético da inteligência artificial na saúde.
- **IA Generativa:** Subcampo da inteligência artificial capaz de gerar conteúdos novos (textos, imagens médicas etc.) a partir de dados de treinamento, como os modelos GPT.
- **Incidente de Segurança:** Evento que compromete a confidencialidade, integridade ou disponibilidade de dados e sistemas.
- **Inteligência Artificial (IA):** Campo da ciência da computação dedicado ao desenvolvimento de sistemas capazes de realizar tarefas que normalmente exigem inteligência humana, como reconhecimento de padrões, tomada de decisões e aprendizado.
- **IoMT (Internet of Medical Things):** Rede de dispositivos médicos conectados (como wearables e equipamentos hospitalares) que coletam e transmitem dados em tempo real.
- **LGPD (Lei Geral de Proteção de Dados):** Lei brasileira (nº 13.709/2018) que regulamenta o tratamento de dados pessoais, incluindo requisitos como consentimento e notificação de violações.
- **Litígios:** Processos judiciais decorrentes de danos ou erros associados ao uso da IA envolvendo responsabilidade legal.
- **Medicina de Precisão:** Abordagem médica que customiza tratamentos com base em dados genéticos, ambientais e de estilo de vida do paciente.
- **Pseudonimização:** Técnica que substitui dados pessoais identificáveis por pseudônimos, reduzindo o risco de identificação direta dos indivíduos durante análises e processamento.

- **Proteção de Dados:** Conjunto de políticas e práticas para assegurar a privacidade e segurança das informações pessoais.
- **Ransomware:** Tipo de malware que sequestra dados através de criptografia, exigindo pagamento para liberá-los (ex.: ataques a hospitais).
- **Redes Neurais Convolucionais (CNN):** Tipo de arquitetura de rede neural especialmente eficaz no processamento de dados visuais, amplamente usada para análise de imagens médicas e diagnóstico assistido.
- **Responsabilidade Compartilhada:** Distribuição clara de obrigações e deveres entre todos os atores envolvidos no ciclo de vida da IA, para garantir segurança e ética.
- **Segurança da Informação:** Conjunto de medidas e práticas para proteger dados e sistemas contra acessos não autorizados, danos ou interrupções.
- **Segurança Jurídica:** Garantia de que o uso da IA está em conformidade com as leis e regulamentos vigentes, minimizando riscos legais para instituições e pacientes.
- **Supervisão Humana:** Participação ativa de profissionais no monitoramento e revisão das decisões tomadas por sistemas automatizados.
- **Transparência:** Princípio que exige clareza e acessibilidade das informações sobre como os sistemas de IA operam e tomam decisões, facilitando a compreensão por profissionais e pacientes.
- **Transparência Algorítmica:** Capacidade dos sistemas de IA de explicarem suas decisões de forma compreensível para humanos, facilitando a auditoria e confiança.
- **Validação Clínica:** Processo de confirmação científica e clínica da eficácia e segurança dos sistemas de IA antes e durante sua aplicação no ambiente de saúde.
- **Viés (Bias):** Tendência ou distorção sistemática nos dados ou algoritmos que pode levar a decisões injustas ou imprecisas.
- **Vulnerabilidade Cibernética:** Fraqueza ou falha em sistemas de informação que pode ser explorada por agentes mal-intencionados para comprometer dados ou serviços.
- **XAI (Explainable AI):** Inteligência Artificial explicável, que fornece transparência sobre suas decisões por meio de interpretações humanamente compreensíveis.
- **Zero Trust Architecture:** Modelo de segurança que pressupõe que nenhum usuário ou dispositivo interno à rede é confiável por padrão, exigindo verificação contínua.

12 CONCLUSÃO

A saúde digital está no epicentro de uma revolução que combina avanços tecnológicos sem precedentes com desafios éticos, operacionais e de segurança igualmente complexos. A inteligência

artificial, por sua capacidade de transformar diagnósticos, tratamentos e gestão hospitalar, representa uma ferramenta poderosa para elevar o padrão de cuidado e eficiência no setor. Contudo, seu impacto positivo depende diretamente da maneira como essa tecnologia é adotada, governada e controlada.

Mais do que inovar, é fundamental que profissionais e instituições desenvolvam uma cultura sólida de responsabilidade e transparência. A proteção dos dados sensíveis, o respeito aos direitos dos pacientes e a supervisão humana constante são pilares inegociáveis para garantir que a IA seja uma aliada confiável e não uma fonte de riscos e prejuízos.

A adoção de diretrizes rigorosas de governança, o investimento contínuo em segurança cibernética e a promoção de auditorias independentes devem ser vistos não como custos adicionais, mas como elementos essenciais para a sustentabilidade da saúde digital. O setor precisa caminhar com firmeza, alinhando a rapidez da inovação à prudência e ética necessárias para preservar a confiança pública.

13 DICAS FINAIS PARA QUEM ATUA NA SAÚDE DIGITAL:

- **Pondere a implementação da IA sempre com foco no princípio *primum non nocere*.** Antes de qualquer inovação, assegure-se de que o sistema não trará danos inesperados ou invisíveis.
- **Invista em governança multidisciplinar.** Tecnologia, ética, direito e medicina precisam andar lado a lado para garantir decisões seguras e justas.
- **Não subestime a importância da transparência.** Pacientes e profissionais devem entender como a IA atua, podendo questionar e revisar decisões automatizadas.
- **Esteja preparado para responder rapidamente a incidentes de segurança.** Planos de contingência e treinamentos constantes são imprescindíveis.
- **Mantenha o humano no centro do cuidado.** A IA é ferramenta, não substituta da inteligência, empatia e julgamento clínico humanos.

Somente assim, a inteligência artificial na saúde poderá cumprir sua promessa de transformação benéfica, equilibrando inovação com responsabilidade, e garantindo que a evolução digital seja um aliado da vida, e não um risco a mais a ser temido.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 2018.

CHECK POINT. Cyber Attack Trends: 2023 Mid-Year Report. Disponível em: https://blog.checkpoint.com. Acesso em: 22 mar. 2025.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.324, de 8 de dezembro de 2022. Uso de IA na prática médica. Brasília, 2022.

ESTEVA, A. et al. Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, v. 542, n. 7639, p. 115-118, 2017. DOI: 10.1038/nature21056.

ESTEVA, A. et al. A guide to deep learning in healthcare. *Nature Medicine*, 2019.

FBI. Data Breach Investigations Report, 2022. Disponível em: https://www.fbi.gov. Acesso em: 22 mar. 2025.

HOSPITAL SÍRIO-LIBANÊS. Relatório de Governança em IA 2022. São Paulo: HSL, 2023.

HOLZINGER, A. et al. Causability and explainability of artificial intelligence in medicine. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2019.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. Ethics and governance of artificial intelligence for health. Genebra: OMS, 2021.

PEW RESEARCH CENTER. Public Trust in Artificial Intelligence in Health, 2023. Disponível em: https://www.pewresearch.org. Acesso em: 22 mar. 2025.

RAJPURKAR, P. et al. Deep learning for detecting pneumonia from chest X-rays. arXiv preprint, arXiv:1711.05225, 2018. Disponível em: https://arxiv.org/abs/1711.05225. Acesso em: 21 jun. 2025.

SINGAPORE MINISTRY OF HEALTH. SingHealth cyber attack – official statement, 2018. Disponível em: https://www.healthcareitnews.com/news/singhealth-cyberattack-raises-concerns-over-health-data-security. Acesso em: 21 jun. 2025.

SMITH, M. L. et al. Algorithmic accountability in healthcare. *Journal of Medical Ethics*, v. 49, n. 3, p. 172-178, 2023.

SOPHOS. The State of Ransomware in Healthcare 2023. Disponível em: https://www.sophos.com. Acesso em: 22 mar. 2025.

TOPOL, E. J. Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. New York: Basic Books, 2019.

WIENS, J.; SHENOY, E. S. Machine Learning for Healthcare: On the Verge of a Major Shift in Healthcare Epidemiology. *Clinical Infectious Diseases*, 2018.

APÊNDICE A – CHECKLIST DETALHADO PARA GOVERNANÇA E USO ÉTICO DA IA NA SAÚDE

GOVERNANÇA E ESTRUTURA ORGANIZACIONAL

1) Formar comitê multidisciplinar com representantes das áreas técnica, médica, jurídica, bioética e pacientes.

   Detalhe: O comitê deve reunir especialistas que tragam diferentes perspectivas para avaliar riscos técnicos, implicações legais, impactos éticos e garantir o respeito aos direitos dos pacientes.

2) Definir claramente papéis e responsabilidades para todos os envolvidos na governança da IA.

   Detalhe: Documentar quem é responsável por desenvolvimento, aprovação, auditoria, supervisão clínica, comunicação e resposta a incidentes, evitando lacunas e conflitos.

3) Estabelecer processos formais para avaliação ética e legal dos sistemas de IA antes da implantação.

   Detalhe: Criar protocolos para análise prévia dos algoritmos, incluindo avaliação de vieses, impacto social e conformidade com normas vigentes.

CONFORMIDADE LEGAL E SEGURANÇA

1) Garantir conformidade rigorosa com a LGPD e demais normativas nacionais e internacionais aplicáveis.

   Detalhe: Implementar políticas de privacidade, coleta e uso de dados que respeitem o consentimento informado, armazenamento seguro e direitos dos titulares.

2) Implementar políticas de proteção e privacidade de dados sensíveis dos pacientes.

   Detalhe: Utilizar técnicas como pseudonimização, criptografia e controle de acesso, além de limitar o tempo de retenção conforme regulamentação.

3) Criar protocolos para resposta rápida a incidentes de segurança e vazamentos de dados.

   Detalhe: Desenvolver planos de contingência claros, com responsáveis designados, fluxos de comunicação e ações imediatas para mitigação.

1) Auditoria e Monitoramento

1) Realizar auditorias periódicas (preferencialmente trimestrais) para revisar o funcionamento e impacto dos sistemas de IA.

   Detalhe: Avaliar desempenho, precisão, transparência, impactos clínicos e conformidade contínua, com registro detalhado dos resultados.

2) Monitorar continuamente os sistemas para detectar vieses, falhas técnicas e desvios éticos.

Detalhe: Utilizar ferramentas de monitoramento e análise para identificar padrões anômalos, erros recorrentes ou decisões que possam causar discriminação.

3) Documentar resultados das auditorias e implementar ações corretivas quando necessário.

Detalhe: Garantir que os relatórios sejam formalizados e que melhorias sejam aplicadas em prazos definidos, com acompanhamento das correções.

2) Transparência e Participação Humana

1) Disponibilizar relatórios claros e acessíveis sobre decisões automatizadas para profissionais de saúde e pacientes.
2) Detalhe: Garantir que os relatórios usem linguagem compreensível, destacando critérios usados pela IA e justificativas das decisões.
3) Estabelecer mecanismos para revisão humana das decisões da IA, com possibilidade de contestação.
4) Detalhe: Permitir que médicos revisem os resultados e que pacientes possam solicitar uma reavaliação ou segunda opinião.
5) Oferecer canais de comunicação para que pacientes possam questionar e solicitar segunda opinião sobre diagnósticos ou tratamentos baseados em IA.
6) Detalhe: Disponibilizar canais diretos, como ouvidoria ou atendimento especializado, para atender dúvidas, reclamações e recursos.

3) Capacitação e Cultura Organizacional

1) Promover treinamentos regulares para equipes técnicas e clínicas sobre uso ético, seguro e eficaz da IA.
2) Detalhe: Desenvolver programas educativos que envolvam aspectos técnicos, legais e éticos, atualizando os profissionais sobre melhores práticas.
3) Incentivar uma cultura organizacional que valorize a responsabilidade, ética e segurança na adoção de tecnologias.
4) Detalhe: Implantar políticas internas e campanhas que reforcem os valores éticos e o compromisso com a segurança do paciente.
5) Fomentar o diálogo contínuo entre as áreas técnica, clínica e administrativa para alinhar expectativas e práticas.
6) Detalhe: Realizar reuniões periódicas e grupos de trabalho para discutir desafios, atualizações e melhorias na governança da IA.