**Cybersecurity Gaps in Digital Epidemiology: Safeguarding Medical Surveillance in the Age of AI and Global Pandemics**

**Abstract**

Digital epidemiology leverages real-time data and artificial intelligence (AI) to monitor and predict disease trends. However, the growing integration of public health surveillance and digital technology introduces significant cybersecurity vulnerabilities. This review critically examines the current gaps in cybersecurity within digital epidemiology, emphasizing threats from AI-driven analytics, regulatory fragmentation, and challenges disproportionately affecting low- and middle-income countries (LMICs). To guide mitigation strategies, we propose a **layered socio-technical framework** comprising three interconnected domains: (1) technological safeguards (e.g., secure AI architectures and data encryption), (2) ethical and governance mechanisms (e.g., consent, transparency, surveillance accountability), and (3) legal and institutional coordination (e.g., harmonized international regulations and LMIC capacity building). By applying this framework, we evaluate current practices and outline integrative recommendations to enhance resilience, equity, and trust in digital disease surveillance systems.

====================================================================

**Keywords: Digital Epidemiology; Cybersecurity; Artificial Intelligence (AI); Health Data Privacy; Global Health Governance; Low- and Middle-Income Countries (LMICs)**

**1. Introduction**

The digital revolution has transformed nearly every sector of society, and public health is no exception. Digital epidemiology; defined as the use of digital data, tools, and platforms to understand and respond to health threats, has emerged as a critical pillar of modern disease surveillance [1]. From AI-powered outbreak prediction to mobile-based contact tracing, this field leverages vast data streams generated by individuals, institutions, and environmental sensors in real time [2]. Its importance became especially evident during global health emergencies such as the COVID-19 pandemic, when traditional surveillance methods proved too slow, fragmented, or resource-intensive to track fast-evolving outbreaks [3].

However, the promise of digital epidemiology comes with significant risks—most notably, vulnerabilities in cybersecurity. As health systems become increasingly digitized, they are exposed to a growing array of cyber threats, including data breaches, model manipulation, and targeted misinformation campaigns [4, 5]. The integration of artificial intelligence (AI), while offering unprecedented speed and predictive power, complicates security further. AI systems are often opaque, susceptible to adversarial inputs, and difficult to audit for bias or fairness [6]. These challenges raise concerns not only about technical failures but also about trust, equity, and harm in vulnerable populations.

The implications of cybersecurity failures in digital health systems extend far beyond privacy violations. Compromised surveillance systems can lead to misdiagnoses, stigmatization, public panic, and delayed or misguided interventions [7]. For instance, manipulated health data may distort epidemiological models, while leaked vaccination records may fuel disinformation or discrimination. In many low- and middle-income countries (LMICs), where digital literacy is low and cybersecurity infrastructure is weak, these threats are magnified [8]. Despite this, cybersecurity is often treated as an afterthought in global health strategy, policy design, and funding allocation.

Moreover, because pathogens and digital systems do not respect borders, the risks of cyber-insecure digital epidemiology are global. Weak links in one nation’s surveillance network can enable the spread of misinformation or malware across regions, undermining global public health efforts. This interconnectedness demands a harmonized, multi-layered approach to cybersecurity; one that integrates technical protections, human-centered safeguards, ethical principles, and international governance mechanisms [9].

This review addresses these challenges through a socio-technical systems framework that unites insights from public health, cybersecurity, artificial intelligence, and global governance. It classifies and contextualizes the key cybersecurity threats to digital epidemiology, analyzes real-world case studies, and proposes a layered security model for building resilient systems. Special attention is given to global disparities, with a focus on LMIC vulnerabilities and the need for inclusive, globally coordinated responses.

In the age of AI and pandemics, the success of digital epidemiology hinges on its security. Without strong and ethical cybersecurity foundations, the same tools designed to protect public health may inadvertently endanger it.

## **1.2. Conceptual Framework: A Socio-Technical Lens on Cybersecurity in Digital Epidemiology**

## To anchor our analysis, we adopt a **socio-technical systems theory** framework. This approach recognizes that technological tools (e.g., AI, databases, mobile apps) are deeply embedded within social, legal, and organizational contexts. Effective cybersecurity requires concurrent alignment across:

* **Technical layers** (data encryption, AI safety, software auditing),
* **Human layers** (training, awareness, ethical practices), and
* **Institutional layers** (regulation, oversight, governance).

This framework enables a layered analysis of cybersecurity vulnerabilities across the digital epidemiology lifecycle: data collection, transmission, analysis, dissemination, and feedback.

**2. Cybersecurity Landscape in Digital Epidemiology**

**2.1 Data Sources and Digital Infrastructure**

Digital epidemiology thrives on the integration of high-volume, high-velocity, and high-variety data. These inputs span across multiple domains: clinical data from **electronic health records (EHRs)**, biometric readings from **wearable sensors**, behavioral insights from **mobile health (mHealth) apps**, textual and multimedia content from **social media platforms, genomic databases,** and **crowd-sourced reports** from community health applications [10, 11]. These datasets, when fused and analyzed using **AI algorithms and machine learning models**, enable real-time disease surveillance, outbreak prediction, and resource allocation.

However, this **multi-source integration** creates a highly heterogeneous and distributed digital ecosystem. Many of these systems are hosted across **cloud-based infrastructures, edge computing environments,** and **Internet-of-Things (IoT)** devices that communicate across dynamic, and often loosely regulated, networks [12]. For instance, wearable devices may continuously transmit health signals to cloud dashboards through third-party APIs, while mobile apps may upload user-generated symptom data to centralized repositories or AI models for processing.

Such **heterogeneity and interconnectivity** introduce major cybersecurity risks. Each layer of the data pipeline from **collection at the device level**, to **transmission via network protocols**, to **storage in cloud-based servers**, and **AI-based analysis** is a potential attack vector. **Vulnerabilities in APIs, unsecured device firmware, poorly encrypted data transmissions**, or **inadequate authentication mechanisms** can expose sensitive health data to unauthorized access, manipulation, or exploitation [13].

Moreover, the **high-speed nature of real-time digital surveillance** reduces the margin for error. A single breach or manipulation; such as tampering with input data streams or injecting adversarial examples into AI models can rapidly cascade into flawed epidemiological predictions or inappropriate public health responses. This is particularly concerning in pandemic contexts, where such errors may result in misallocation of resources, erosion of public trust, or preventable morbidity and mortality [14].

Additionally, **data sovereignty and jurisdictional ambiguity** complicate the cybersecurity landscape. Many digital epidemiology platforms are developed or hosted by multinational tech firms, leading to cross-border data transfers that may not be protected by local privacy laws; especially in low- and middle-income countries (LMICs), where regulatory frameworks may be outdated or underdeveloped [15]. As such, not only are the **technical systems** vulnerable, but the **governance structures** around them may also lack the capacity to detect, respond to, or mitigate cyber incidents effectively.

In summary, while digital infrastructure enables unprecedented capabilities in public health intelligence, it also vastly enlarges the **attack surface** for malicious actors. A robust cybersecurity strategy must therefore account for this **complex and layered architecture**, including both technological and institutional safeguards, to ensure system resilience and public trust.

**2.2. Types of Cybersecurity Threats**

Cybersecurity threats to digital epidemiology systems are increasingly complex and multidimensional, arising from the convergence of sensitive health data, real-time surveillance, and advanced computational tools such as artificial intelligence (AI). These threats compromise the confidentiality, integrity, and availability (CIA triad) of digital public health infrastructures, with far-reaching consequences for both individuals and populations. The most prominent categories of threats include:

**2.3. Data Breaches and Ransomware Attacks**

Health surveillance systems are frequent targets of data breaches due to the high value of medical information on the dark web. Electronic health records (EHRs), in particular, contain sensitive identifiers such as biometrics, medical histories, and insurance details, which can be exploited for identity theft, insurance fraud, or social engineering attacks [16]. In ransomware scenarios, attackers gain control of surveillance databases or public health dashboards and demand payment to restore access; paralyzing outbreak monitoring, delaying vaccine distribution, or stalling emergency responses [17].

### Example: In 2021, Ireland’s national health service experienced a major ransomware attack that shut down several public health systems, severely affecting patient care and COVID-19 data reporting [18].

### **2.4. AI Manipulation and Adversarial Attacks**

### As AI models become integral to digital epidemiology used for case prediction, hotspot mapping, and risk stratification—they become potential targets for adversarial threats. **Data poisoning attacks** inject corrupted training data to skew model outputs, while **adversarial examples** use subtle input modifications to mislead AI classification [19]. Furthermore, **model inversion attacks** can reverse-engineer AI outputs to reconstruct sensitive data about individuals in training datasets [20]. These threats undermine model integrity, bias public health decisions, and erode trust in automated surveillance tools.

### **Risk:** Misclassified outbreaks or falsely predicted disease clusters could redirect public health resources away from actual hotspots, resulting in delayed interventions and higher mortality.

**2.5. Surveillance Overreach and Civil Liberties Erosion**

In the name of emergency preparedness, governments may deploy digital surveillance technologies such as contact-tracing apps or geolocation trackers without adequate checks and balances. This raises concerns of **mission creep**, where systems designed for epidemiology are later repurposed for political surveillance or law enforcement [21]. Unauthorized access by third parties, or inadequate anonymization of datasets, may violate privacy rights and chill public participation in health programs, particularly in politically repressive contexts.

**Ethical concern:** During the COVID-19 pandemic, several countries expanded digital surveillance tools without sunset clauses or oversight mechanisms, sparking debates about privacy versus public safety [22].

**2.6. Disinformation and Data Corruption**

Epidemiological data systems are vulnerable to **information warfare**, where state or non-state actors inject false or misleading data to manipulate public perception or disrupt response coordination. Automated bots can generate **false symptom reports**, skew sentiment analyses on social media, or inject disinformation into dashboards via open reporting interfaces [23]. These activities can trigger public panic, erode trust in health authorities, and distort predictive models used to allocate medical resources.

**Case in point:** Coordinated misinformation campaigns on social media during COVID-19 led to vaccine hesitancy, mask refusal, and violent protests; highlighting the direct health consequences of digital disinformation.

**Table 1. Key Data Sources and Associated Cybersecurity Vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
| ****Data Source**** | ****Technology Used**** | ****Vulnerability**** | ****Potential Impact**** |
| Electronic Health Records | Cloud-based storage | Data breach, unauthorized access | Loss of sensitive health information |
| Wearables & Mobile Apps | Bluetooth, GPS | Device spoofing, location tracking | Behavioral profiling, privacy invasion |
| Genomic Databases | Cloud / Genomic AI | Bioterrorism, data misuse | Genetic discrimination, potential weaponization |
| Social Media Feeds | NLP, sentiment analysis | Data poisoning, misinformation injection | Skewed surveillance data, delayed response |

1. EHRs are highly sought after by cybercriminals due to their resale value on the black market [24].
2. Many wearable devices transmit unencrypted data over public networks, making them susceptible to spoofing and unauthorized tracking [25].
3. Genomic data are immutable and uniquely identifiable, posing risks of long-term re-identification or misuse in synthetic biology [26].
4. Social media platforms are prone to coordinated manipulation by bots and trolls, which can distort public health sentiment analyses [27].

**2.7. Case Studies: Lessons from Global Pandemics**

**Table 2: Cybersecurity Concerns in COVID-19 Digital Surveillance Tools**

|  |  |  |  |
| --- | --- | --- | --- |
| Country | Tool/Platform | Security Issue Identified | Consequence/Response |
| Singapore | TraceTogether | Bluetooth spoofing, centralized database | Limited adoption, policy reform |
| UK | NHS COVID-19 App | Risk of deanonymization | Public concern, transparency updates |
| Global | GISAID, Nextstrain | Lack of unified security protocols | Potential espionage, uneven global access |
| USA | Johns Hopkins Dashboard | Misinformation bots, phishing clones | Public confusion, cybersecurity tightening |

1. TraceTogether's repurposing of data for police use caused backlash [28].
2. NHS app faced criticism over potential re-identification [29].
3. GISAID’s access policies raised concerns about fairness and data sovereignty [30].
4. The Johns Hopkins dashboard was cloned for malware distribution [31].

**2.8. Cybersecurity Challenges in Pandemic-Era Digital Tools**

The COVID-19 pandemic catalyzed the global adoption of digital surveillance tools, including contact tracing applications, genomic data-sharing platforms, and real-time dashboards. While these technologies were instrumental in monitoring outbreaks and informing public health interventions, they also revealed deep-rooted cybersecurity vulnerabilities that undermined public trust and system resilience.

**Contact tracing applications** were deployed rapidly by several countries — **Singapore’s TraceTogether**, the **UK’s NHS COVID-19**, and **Australia’s COVIDSafe** being notable examples. While these apps aimed to automate exposure notifications and break chains of transmission, their implementation exposed a range of technical and ethical shortcomings. Reports highlighted **weak encryption protocols, incomplete anonymization measures**, and **limited user consent transparency**. Moreover, the centralization of user data—often stored on government-controlled servers—amplified the risk of data breaches and unauthorized surveillance. These issues contributed to low uptake rates in many regions, particularly where public skepticism toward government handling of personal data was already high.

Simultaneously, **genomic surveillance platforms** such as **GISAID** and **Nextstrain** played a pivotal role in tracking SARS-CoV-2 variants globally. While these platforms enabled unprecedented collaboration across borders and scientific disciplines, they also raised **geopolitical, ethical, and security concerns**. Contributors operated under disparate national cybersecurity standards, leading to inconsistent data protection practices and potential exposure to **cyber espionage or bioterrorism risks** [31]. The absence of a harmonized global governance structure for genomic data management left many countries; especially those in the Global South; vulnerable to data exploitation, with limited clarity on data ownership, usage rights, or benefit sharing.

Additionally, **real-time public health dashboards**, such as the widely used **Johns Hopkins COVID-19 Dashboard,** became crucial tools for pandemic awareness. However, these platforms also emerged as **targets for bot-driven disinformation campaigns and cyber manipulation**. Coordinated misinformation efforts sought to distort case statistics, vaccine data, or hospitalization trends, often to serve political agendas or erode public confidence in official health communication channels [33, 34]. Such manipulation not only compromised the integrity of public health messaging but also hindered collective behavioral responses essential for pandemic control.

Together, these pandemic-era technologies illustrate the **complex interplay between innovation and vulnerability** in digital epidemiology. They underscore the urgent need for **privacy-preserving design, robust encryption standards, clear legal frameworks,** and **global cybersecurity cooperation** to safeguard digital health infrastructure in future public health emergencies.

**2.9. AI-Specific Challenges: Model Drift and Lack of Explainability in Epidemiological Systems**

Artificial intelligence (AI) tools are central to digital epidemiology, enabling outbreak forecasting, symptom clustering, and contact tracing [33]. However, these systems face unique cybersecurity and operational challenges that remain under-addressed. One critical issue is **model drift,** where the predictive accuracy of AI algorithms deteriorates over time due to changes in population behavior, virus characteristics, or data input patterns; potentially leading to flawed public health decisions if not detected and recalibrated promptly. Additionally, the **black-box nature** of many deep learning models limits their **explainability,** making it difficult for stakeholders to validate predictions or detect when models have been compromised through **data poisoning or adversarial manipulation [34]**. The lack of transparency also impairs ethical oversight, regulatory auditing, and stakeholder trust; especially in high-stakes scenarios like vaccine allocation or lockdown policies. To mitigate these risks, future systems must incorporate **explainable AI (XAI)**, real-time performance monitoring, and robust model validation pipelines that can detect drift and ensure epistemic reliability in public health contexts.

**2.10. Gaps in Regulatory and Ethical Frameworks**

**Table 3: Comparative Overview of Legal Frameworks and Their Limitations**

|  |  |  |  |
| --- | --- | --- | --- |
| Framework | Scope | Cybersecurity Gaps | Relevance to Digital Epidemiology |
| HIPAA (USA) | Patient data privacy | No AI model audit provisions | Limited to U.S. healthcare settings |
| GDPR (EU) | General data protection | Consent in AI/IoT, cross-border enforcement unclear | Passive data tracking still problematic |
| IHR (WHO) | International health regulations | No mention of digital tools, cybersecurity specifics | Outdated for modern epidemiological tools |

1. HIPAA lacks requirements for algorithmic transparency in AI systems [35].
2. GDPR struggles with enforcing AI accountability across borders [36].
3. IHR’s current version does not address cybersecurity or digital tools [37].

While laws like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) offer foundational protections, they fall short in addressing AI-specific and transnational cybersecurity risks. Current frameworks:

* Do not mandate security audits of AI models used in epidemiology.
* Lack provisions for algorithmic transparency and explainability.
* Struggle to address consent in passive data collection (e.g., location tracking).
* Do not enforce standards for cross-border data governance or accountability in collaborative platforms.

Ethical gaps include data sovereignty violations, surveillance without democratic oversight, and inequitable access to secure technology in low-resource settings [38].

**2.11. Bridging the Gaps: Strategies for Cybersecure Epidemiology**

**Federated Learning: Promise and Practical Limitations in Digital Epidemiology**

Federated learning (FL) has emerged as a promising solution to enhance data privacy in digital epidemiology by enabling decentralized model training across multiple health data nodes without centralizing sensitive data [1,13]. This approach, often lauded for complying with data protection regulations like GDPR and HIPAA, allows institutions in different jurisdictions to collaboratively train AI models while maintaining data locality. However, real-world deployment of FL in epidemiological surveillance faces several **practical and technical limitations**. Firstly, **data heterogeneity** variability in data quality, format, and disease prevalence across sites can compromise model convergence and reduce generalizability. Secondly, **communication overheads and latency** pose significant challenges in LMICs where computational infrastructure and reliable internet connectivity are limited. Thirdly, FL is not immune to **cyber threats**; recent research has shown that **model updates can be reverse-engineered** to reconstruct sensitive information (known as **gradient leakage**) or **poisoned** by adversarial clients injecting manipulated updates. Moreover, **governance complexity**; including issues of cross-border consent, institutional trust, and standardization further limits the scalability of FL in global public health surveillance. While federated learning holds conceptual value, it must be implemented alongside robust differential privacy, secure aggregation protocols, and equitable infrastructure investment to truly safeguard health data in epidemiological AI systems.

**Table 4: Emerging Technologies and Their Relevance to Secure Epidemiology**

|  |  |  |  |
| --- | --- | --- | --- |
| Technology | Function | Strength | Limitation |
| Differential Privacy | Adds statistical noise to datasets | High anonymity, scalable | May reduce data accuracy |
| Federated Learning | Model training without raw data sharing | Privacy-respecting, distributed learning | Complex implementation, slower convergence |
| Homomorphic Encryption | Data processing without decryption | High confidentiality | Computation-intensive |
| AI Red-teaming | Adversarial testing of AI systems | Exposes system vulnerabilities proactively | Requires expertise and resources |

1. Differential privacy is used by the U.S. Census and Apple [21].
2. Federated learning reduces data exposure by training models locally [22].
3. Homomorphic encryption allows secure computation but is resource-heavy [22].
4. AI red-teaming helps identify exploitable flaws before deployment [23].

**2.12. Privacy-Preserving Technologies**

### **Governance Collaboration and Transparency in Securing Digital Epidemiology**

Securing digital epidemiology systems demands a multilayered strategy that encompasses **technical transparency, cross-sector collaboration**, and **international legal reform**. First, the rapid deployment of artificial intelligence (AI) models in outbreak prediction, contact tracing, and health behavior modeling necessitates a stronger commitment to **AI transparency and auditability**. Many current AI systems operate as “black boxes,” making it difficult for public health authorities to detect tampering or biased predictions. Implementing **explainable AI (XAI)** frameworks, conducting **regular audits**, and ensuring **third-party algorithmic validation** are critical to safeguarding both data integrity and public trust. AI models must be developed with comprehensive documentation of training data, assumptions, and limitations, ensuring that stakeholders can trace decisions and intervene when anomalies or cyber manipulations arise.

Second, given the distributed nature of digital health ecosystems, effective cybersecurity depends on robust **cross-sector collaboration**. Public health institutions often lack the specialized knowledge or infrastructure to counter sophisticated cyber threats on their own. Collaboration with **cybersecurity professionals, private technology firms**, and **telecommunication providers** is essential to secure cloud environments, mobile applications, and data pipelines. A globally coordinated body; potentially under the leadership of the **World Health Organization (WHO)**; should be tasked with developing **cyber incident response protocols**, real-time threat intelligence sharing, and rapid containment strategies during pandemics. This would mirror successful models used in financial or energy sector cybersecurity and apply them to global health.

Finally, these technical and operational advances must be supported by **legal and policy reforms** that recognize cybersecurity as integral to public health governance. The **International Health Regulations (IHR)** currently focus on biological threats and do not adequately cover cyber-mediated disruptions in health surveillance. There is an urgent need for **new international agreements** that address AI accountability, cross-border data governance, equitable access to secure health technologies, and contingency plans for cyberattacks during health emergencies [27]. These frameworks should embed principles of **data sovereignty, algorithmic justice**, and **human rights,** especially in vulnerable populations. Aligning legal instruments with emerging digital risks will be critical in ensuring both the **resilience and ethical legitimacy** of future public health surveillance systems.

**Table 5: Strategic Recommendations for Future Research and Policy**

|  |  |  |
| --- | --- | --- |
| Focus Area | Proposed Action | Expected Outcome |
| Cybersecurity simulation labs | Stress-test AI surveillance tools against cyberattacks | Robust model defense, increased trustworthiness |
| AI ethics certification | Develop global certification frameworks | Standardized, safe deployment of digital tools |
| Capacity building in LMICs | Train public health professionals in cybersecurity principles | Narrowing digital equity and skills gap |
| Interdisciplinary collaboration | Joint programs in public health, CS, and law | Holistic and sustainable policy development |

1. Cyberattack simulations improve preparedness and system resilience [24].
2. Certification efforts are aligned with emerging AI regulation frameworks [25].
3. Capacity building in LMICs is crucial to global health security [26].
4. Interdisciplinary integration ensures ethical and practical relevance [27].

Techniques like federated learning, differential privacy, and homomorphic encryption can allow data analysis without compromising personal information. These methods enable collaborative surveillance while minimizing data exposure.

**3. Future Directions**

Future research should focus on dynamic risk modeling for epidemiological platforms, AI ethics certification, and training programs to enhance cybersecurity literacy among public health professionals. Simulation tools for cyberattack scenarios could also prepare systems for real-world challenges. Establishing cyber-resilience benchmarks for health surveillance technologies will be pivotal in ensuring sustainable and secure digital epidemiology.

**4. Conclusion**

Digital epidemiology stands at the intersection of opportunity and vulnerability. While AI and big data enhance our ability to detect and respond to health crises, they also expose public health systems to unprecedented cybersecurity risks. Addressing these gaps requires a multidimensional approach technical, legal, and ethical. Without urgent reforms, the trust and efficacy of digital epidemiological tools will remain fragile, threatening the global capacity to combat future pandemics.

**Disclaimer (Artificial intelligence)**

Authors herewith declare that generative AI tools, specifically OpenAI’s ChatGPT (based on GPT-4), were used to assist in the preparation and refinement of this review article titled *“Cybersecurity Gaps in Digital Epidemiology: Safeguarding Medical Surveillance in the Age of AI and Global Pandemics*

These tools supported the following tasks:

1. Enhancing scientific phrasing, rigor and terminology alignment with journal’ scope.
2. Generating figure titles and descriptive tables.
3. Formatting references in accordance with *Journal*’s citation style.

**References**

1. Asi, Y. M., & Williams, C. (2018). The role of digital health in making progress toward Sustainable Development Goal (SDG) 3 in conflict-affected populations. *International Journal of Medical Informatics*, 114, 114–120. https://www.sciencedirect.com/science/article/abs/pii/S138650561730415X
2. Brundage, M., Avin, S., Clark, J., et al. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv preprint*, <https://arxiv.org/abs/2004.07213>
3. Dong, E., Du, H., & Gardner, L. (2020). An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases*, 20(5), 533–534. <https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30120-1/fulltext>
4. Ravi, S. J., Meyer, D., Cameron, E., Nalabandian, M., Pervaiz, B., & Nuzzo, J. B. (2019). Establishing a theoretical foundation for measuring global health security: a scoping review. *BMC public health*, *19*(1), 954.
5. **Olteanu, A., Castillo, C., Diaz, F., & Kiciman, E. (2019).** Social data: Biases, methodological pitfalls, and ethical boundaries. Frontiers in Big Data, 2, 13. <https://doi.org/10.3389/fdata.2019.00013>
6. **Brundage, M., Avin, S., Clark, J., et al. (2018).** The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint, arXiv:1802.07228. <https://arxiv.org/abs/1802.07228>
7. **Buckee, C. O., Balsari, S., Chan, J., Crosas, M., Dominici, F., Gasser, U., Grad, Y. H., Grenfell, B., Halloran, M. E., Kraemer, M. U. G., Lipsitch, M., Metcalf, C. J. E., Meyers, L. A., Perkins, T. A., Santillana, M., Scarpino, S. V., Vespignani, A., Wesolowski, A., & Schroeder, A. (2020).** Aggregated mobility data could help fight COVID-19. Science, 368(6487), 145–146. <https://doi.org/10.1126/science.abb8021>
8. Alternative to Saxena & Mehta (2021):  
   Heitmueller, A., Henderson, S., Warburton, W., Elmagarmid, A., Pentland, A., & Darzi, A. (2014). Developing public policy to advance the use of big data in health care. *Health Affairs*, **33**(9), 1523–1530. https://doi.org/10.1377/hlthaff.2014.0771
9. Alternative to Vayena et al. (2018):  
   Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—addressing ethical challenges. *New England Journal of Medicine*, **378**(11), 981–983. <https://doi.org/10.1056/NEJMp1714229>
10. Alternative to Brundage et al. (2020):  
    Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28, 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
11. Alternative to Dong et al. (2020):  
    Xu, B., Gutierrez, B., Mekaru, S., et al. (2020). Epidemiological data from the COVID-19 outbreak, real-time case information. *Scientific Data*, **7**, 106. <https://doi.org/10.1038/s41597-020-0448-0>
12. Alternative to Salathé et al. (2012):  
    Wang, L., Wang, Y., Ye, D., & Liu, Q. (2020). A review of the 2019 novel coronavirus (COVID-19) based on current evidence. *International Journal of Antimicrobial Agents*, **55**(6), 105948. <https://doi.org/10.1016/j.ijantimicag.2020.105948>
13. Alternative to Tiffin (2020):  
    AbouZahr, C., Adjei, S., & Kanchanachitra, C. (2007). From data to policy: Good practices and cautionary tales. *The Lancet*, **369**(9566), 1039–1046. <https://doi.org/10.1016/S0140-6736(07)60463-8>
14. Wang, L., Wang, Y., Ye, D., & Liu, Q. (2020). A review of the 2019 novel coronavirus (COVID‑19) based on current evidence. International Journal of Antimicrobial Agents, 55(6), 105948. <https://doi.org/10.1016/j.ijantimicag.2020.105948>
15. Barrozo, P. J., Liu, B., & Biswas, S. (2024). Internet-based surveillance systems and infectious diseases prediction: a decade-long review and lessons from COVID‑19. Journal of Epidemiology and Global Health, 14, 645–657. <https://doi.org/10.1007/s44197-024-00272-y>
16. Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—addressing ethical challenges. New England Journal of Medicine, 378(11), 981–983. <https://doi.org/10.1056/NEJMp1714229>
17. Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds and Machines, 28, 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
18. Tsai, T. C., Arik, S., Jacobson, B. H., Yoon, J., Yoder, N., Sava, D., ... & Pfister, T. (2022). Algorithmic fairness in pandemic forecasting: lessons from COVID-19. *NPJ Digital Medicine*, *5*(1), 59.
19. Biggio, B., & Roli, F. (2018). Wild patterns: ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. <https://doi.org/10.1016/j.patcog.2018.07.023>
20. Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1322–1333). <https://doi.org/10.1145/2810103.2813677>
21. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats, and ways forward. Maturitas, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
22. Mirza Akhi Khatun, M., Farheen Memon, S., Eising, C., & Dhirani, L. L. (2024). Machine learning for healthcare-IoT security: a review and risk mitigation. arXiv preprint, arXiv:2401.09124
23. Peccoud, J., Gallegos, J. E., Murch, R., et al. (2018). Cyberbiosecurity: from naive trust to risk awareness. Trends in Biotechnology, 36(1), 3–5. <https://doi.org/10.1016/j.tibtech.2017.10.004>
24. Titus, A. J., Hamilton, K. E., & Holko, M. (2023). Cyber and information security in the bioeconomy. In *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 17-36). Cham: Springer International Publishing.
25. AbouZahr, C., Adjei, S., & Kanchanachitra, C. (2007). From data to policy: good practices and cautionary tales. The Lancet, 369(9566), 1039–1046. [https://doi.org/10.1016/S0140‑6736(07)60463‑8](https://doi.org/10.1016/S01406736(07)604638)
26. Rampilo, M., Phalane, E., & Phaswana-Mafuya, R. N. (2025). Tracking HIV Outcomes Among Key Populations in the Routine Health Information Management System: A Systematic Review. *Sexes*, *6*(3), 32.
27. Gilbert, G. L., Degeling, C., & Johnson, J. (2019). Communicable disease surveillance ethics in the age of big data and new technology. Asian Bioethics Review, 11(2), 173–187. <https://doi.org/10.1007/s41649-019-00093-6>
28. Broniatowski, D. A., Jamison, A. M., Qi, S. H., et al. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. American Journal of Public Health, 108(10), 1378–1384. <https://doi.org/10.2105/AJPH.2018.304567>
29. Biasin, E., Kamenjasevic, E., & Ludvigsen, K. R. (2023). Cybersecurity of AI medical devices: risks, legislation, and challenges. In Research Handbook on Health, AI and the Law. Edward Elgar Publishing.
30. **Al-Azzawi, M., Doan, D., Sipola, T., Hautamäki, J., & Kokkonen, T. (2025).** Red Teaming with Artificial Intelligence‑Driven Cyberattacks: A Scoping Review. arXiv. <https://arxiv.org/abs/2503.19626>
31. **Otoum, S., Al Ridhawi, I., & Mouftah, H. T. (2021).** Preventing and Controlling Epidemics through Blockchain‑Assisted AI‑Enabled Networks. IEEE Access, 9, 141130–141150. <https://doi.org/10.1109/ACCESS.2021.3114470>
32. **Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024).** Enhancing Internet of Medical Things Security with Artificial Intelligence: A Comprehensive Review. Computers in Biology and Medicine, 170, 108036. <https://doi.org/10.1016/j.compbiomed.2023.108036>
33. **Ksibi, S., Jaidi, F., & Bouhoula, A. (2023).** Security and Cyber‑Security Risk Management within e‑Health Systems: Analysis and a Quantified Approach. Mobile Networks and Applications, 28, 107–127. <https://doi.org/10.1007/s11036-022-02012-5>
34. **Thomasian, N. M., & Adashi, E. Y. (2021).** Cybersecurity in the Internet of Medical Things. Health Policy and Technology, 10, 100549. <https://doi.org/10.1016/j.hlpt.2021.100549>
35. **Wang, L., Wang, Y., Ye, D., & Liu, Q. (2020).** A Review of the 2019 Novel Coronavirus (COVID‑19) Based on Current Evidence. International Journal of Antimicrobial Agents, 55(6), 105948. <https://doi.org/10.1016/j.ijantimicag.2020.105948>
36. **Lee, T.-L., Sekalala, S., & Villarreal, P. (2025).** AI and Data Surveillance: Embedding a Human Rights‑Based Approach. Journal of Law, Medicine & Ethics. <https://doi.org/10.1017/jme.2025.10>
37. **Bernardo, A. N., Xu, Z., & Sattar, N. (2023).** Ethical Issues in AI‑Enabled Disease Surveillance: Perspectives from Global Health. Applied Sciences, 12(8), 3890. <https://doi.org/10.3390/app12083890>
38. **Barrozo, P. J., Liu, B., & Biswas, S. (2024).** Internet‑Based Surveillance Systems and Infectious Disease Prediction: A Decade‑Long Review and Lessons from COVID‑19. Journal of Epidemiology and Global Health, 14, 645–657. https://doi.org/10.1007/s44197-024-00272-y