



CHRISTOPHER A. LONGHURST, MD, MS  
CLINICAL PROFESSOR OF PEDIATRICS AND BIOMEDICAL INFORMATICS  
CHIEF CLINICAL INNOVATION OFFICER AND ASSOCIATE DEAN  
EXECUTIVE DIRECTOR, JACOBS CENTER FOR HEALTH INNOVATION  
UC SAN DIEGO HEALTH SCIENCES

DEPARTMENT OF BIOMEDICAL INFORMATICS  
9560 TOWNE CENTRE DRIVE  
LA JOLLA, CALIFORNIA 92121

Phone: (858) 249-6880

January 9, 2024

Emma Schultheis, Legislative Clerk  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear colleagues,

Thank you for the opportunity to present to the Health Subcommittee on Nov 29, 2023 as well as the opportunity to respond to these follow up questions.

***The Honorable Earl “Buddy” Carter***

*1. Dr. Longhurst - AI relies on huge datasets to work, and that means we need to make sure that data is safe, secure, and private. Can you help me understand what the health care system does to first, protect patient health data, and second, what more might be needed to keep that information secure and private?*

All US health delivery organizations are subject to the Health Information Portability and Accountability Act (HIPAA), which defines the security and privacy regulations required to protect sensitive patient health information. healthcare system protects patient health data by implementing various measures to ensure the information is kept private and secure. Some key ways that we do this include:

- **Confidentiality:** Healthcare providers follow strict rules to keep patient information confidential. Only authorized personnel, such as doctors, nurses, and administrative staff, have access to patient records.
- **Access Controls:** Access to electronic health records is restricted, and only individuals with the right permissions can view or modify the information. This helps prevent unauthorized access and protects patient privacy.
- **Encryption:** Patient health data is often stored in electronic systems, and encryption is used to convert this information into a code that is difficult to decipher without the proper authorization. It adds an extra layer of security to the data.
- **Secure Communication:** Healthcare systems use secure methods for communication, especially when sharing sensitive information. This may involve encrypted emails or secure messaging systems to ensure that patient data is transmitted safely.
- **Regular Audits:** Healthcare organizations conduct regular audits to monitor who has accessed patient data and when. This helps identify any suspicious activity and ensures that access is only granted to those who need it for legitimate reasons.

- **Training and Awareness:** Healthcare staff undergo training to understand the importance of protecting patient health data. This includes educating them on best practices, security protocols, and the potential risks associated with mishandling sensitive information.
- **Physical Security:** In addition to digital safeguards, physical security measures are in place to protect paper records and other physical storage of patient data. Restricted access areas help prevent unauthorized individuals from gaining physical access to sensitive information.
- **Compliance with Regulations:** Healthcare systems adhere to strict regulations and laws governing the protection of patient health data, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Compliance ensures that organizations meet specific standards for safeguarding patient information.

By combining these measures, healthcare systems aim to create a robust and secure environment for patient health data, safeguarding it against unauthorized access, breaches, and potential misuse.

### *The Honorable Earl “Buddy” Carter*

*1. Dr. Longhurst - AI relies on huge datasets to work, and that means we need to make sure that data is safe, secure, and private. Can you help me understand what the health care system does to first, protect patient health data, and second, what more might be needed to keep that information secure and private?*

Additional measures that organizations like ours often implement to enhance the security and privacy of patient health data include:

- **Multi-Factor Authentication (MFA):** Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing patient data. This helps prevent unauthorized access even if login credentials are compromised.
- **Incident Response Plan:** Developing and regularly testing an incident response plan helps healthcare organizations respond quickly and effectively in the event of a security breach. This includes protocols for identifying, containing, and mitigating the impact of a security incident.
- **Regular Security Audits and Penetration Testing:** Conducting regular security audits and penetration testing helps identify vulnerabilities in the system. Addressing these vulnerabilities proactively can prevent potential security breaches.
- **Regular Risk Assessments:** Conducting regular risk assessments helps identify and prioritize potential risks to patient data. This allows organizations to allocate resources efficiently to address the most critical vulnerabilities.

This is an area of evolving knowledge, which is why UC San Diego established the nation’s first **Center for Healthcare Cybersecurity** (<http://cyberhealth.ucsd.edu/>), which was recently awarded a \$9.5M ARPA-H federal contract to help our researchers develop better ways to prevent and mitigate ransomware attacks in the healthcare setting.<sup>1</sup>

In addition, patients now have access to their digital records thanks to the 21<sup>st</sup> Century Cures Act, but once patient share this data with third parties, there are no safeguards in place. Regulation aimed at medical information provided to and from consumer healthcare apps would be helpful in keeping patient information secure and private.

---

<sup>1</sup> UC San Diego Awarded \$9.5 Million to Enhance Cybersecurity in Health Care, Oct 2, 2023. <https://today.ucsd.edu/story/uc-san-diego-awarded-9.5-million-to-enhance-cybersecurity-in-health-care>

***The Honorable Earl “Buddy” Carter***

*2. How do you think AI and medical liability intersect? Can you see litigation increase if doctors DON'T utilize AI in their clinical decision making.*

As of today, there are no instances where cases involving AI and medical care have been tried in court. This intersection is increasingly likely, and the potential outcomes of cases involving medical AI based on current law have been described by experts.<sup>2</sup> Based on current laws, physicians are judged in malpractice cases based on whether or not they followed the “standard of care,” regardless of whether this agrees with an AI recommendation. If and when AI recommendations become part of the standard of care, then physicians may certainly be expected to be judged on whether or not they followed AI recommendations.

Scenario	AI recommendation	AI accuracy	Physician action	Patient outcome	Legal outcome (probable)
1	Standard of care	Correct	Follows	Good	No injury and no liability
2			Rejects	Bad	Injury and liability
3		Incorrect (standard of care is incorrect)	Follows	Bad	Injury but no liability
4			Rejects	Good	No injury and no liability
5	Nonstandard care	Correct (standard of care is incorrect)	Follows	Good	No injury and no liability
6			Rejects	Bad	Injury but no liability
7		Incorrect	Follows	Bad	Injury and liability
8			Rejects	Good	No injury and no liability

Price et al.<sup>2</sup>

In the near term, it is more likely this intersection of AH and medical liability will occur around inappropriate uses of the technology, since it is so new and there is a paucity of outcomes published in the literature. However, as the evidence supporting use of AI in various medical conditions begins to accumulate over the next decade, it is likely that situations will emerge in which outcomes are consistently and demonstrably better when physicians are supported with AI tools. If and when this does occur, this would represent a new standard of care and it is conceivable that physicians who are not using these tools could face litigation and even liability.

***The Honorable Nanette Barragán***

*1. We know that addressing social determinants of health is critical to closing gaps in health disparities. However, this data – such as a person’s access to housing or their exposure to poor air quality – is not covered by HIPAA. Are you aware of any methods to ensure data used from third-party repositories were gathered with patient consent?*

We certainly agree that addressing social determinants of health is critical to closing health disparity gaps, and this often involves partnerships between health care systems and social service agencies.<sup>3</sup> Organizations within the social service sector working to address social determinants of health have established privacy practices and workflows that ensure individual consent to share personal identification information. Additionally, many such organizations (such as 2-1-1s, community information exchanges, health information exchanges, and whole person care networks) and their customer/agencies that coordinate care for individuals and are connected to a data exchange,

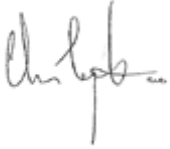
<sup>2</sup> Price WN 2nd, Gerke S, Cohen IG. Potential Liability for Physicians Using Artificial Intelligence. JAMA. 2019;322(18):1765-1766.

<sup>3</sup> Pilot Project to Help Patients with Transportation Barriers Get to Appointments, May 4 2023. <https://today.ucsd.edu/story/pilot-project-to-help-patients-with-transportation-barriers-get-to-appointments>

contractually agree to obtain and document the client's consent to the disclosure of personal information to other members of the network. Consent is documented in the client's record in a way that permits the other members of the network to verify the permission to share. Processes are also required to turn off permission and block access to client's information when the client revokes permission to share and security systems are in place to protect the security of information stored in the third-party repository and to notify client's and partner agencies in the event of a breach.

The requirement that a healthcare organization obtain an individual's express written consent before disclosing health information to a third party is well established under federal laws such as HIPAA. However, the same protections are not required of technology companies who build smartphone apps which collect data directly from consumers, and practices vary widely. This is an area ripe for scrutiny and possible federal regulation.

Sincerely,

A handwritten signature in cursive script, appearing to read "Chris Longhurst".

Christopher Longhurst, MD, MS