Table 1: Interpreted FDA Recommendations

Category	Recommendation
A. Authenticate Users	A-1 User authentication
	A-2 Multi-factor authentication
	A-3 Strong passwords
B. Authenticate Commands	B-1 Safe crypto usage
	B-2 Authenticate connections
	B-3 Verify software
	B-4 Deny by default
C. Data Integrity	C-1 Verify incoming data
	C-2 Secure data transfer
	C-3 Protect essential local data
	C-4 Strong crypto algorithms
	C-5 Use unique key per device
D. Execution Integrity	D-1 Verify code integrity
E. Detect Security Events	E-1 Record security events
	E-2 Secure configuration

4 TRANSLATION AND COMPLIANCE VERIFICATION

As discussed in Section III, there are a few key challenges that make it difficult to translate regulatory requirements into a computation-friendly format. Existing work has achieved some success by applying ML and NLP [25]. However, these techniques may only be effective in some legal domains. Our key observation is that by translating not the legal text itself but "middleware" (i.e., non-legal, authoritative, guidance documents that clarify regulatory intent), we may be able to enjoy both the benefits of an open-ended, flexible legal framework and a descriptive regulatory environment that can be operationalized into a computational auditor. These clarifying documents may already be produced by regulatory bodies and can be independently developed by standards organizations and industry groups.

In the mHealth space, we operationalized the security recommendations in the 2018 FDA draft guidance document *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. As shown in Table 1, the recommendations in this document can be grouped into five categories: user authentication, authentication of safety-critical functions, data integrity, execution integrity, and the detection of cybersecurity incidents. We collected 182 FDA/CE-approved mHealth apps from healthskouts[1] in February 2021 and used our analysis framework to audit their compliance with these FDA recommendations.

Warnings were then manually analyzed. One common type of warning was the presence of hard-coded keys. Twenty-five apps hard-coded OAuth secrets and seventeen apps hard-coded API keys; these keys can be extracted and used for malicious purposes. Seven apps hard-coded cryptographic keys for pairing or inter-device communication. Finally, four apps hard-coded Android Keystore passwords and three apps hard-coded SQLite database keys.

5 CONCLUSION

In this project, we propose a new way to build automatic auditors for legal compliance. Our key observation is that instead of operationalizing legal text itself, we may find more success by translating non-legal, authoritative, guidance documents that clarify regulatory intent. By doing so, we enjoy both the benefits of an open-ended, flexible legal framework and a descriptive regulatory environment that can be translated into a computational auditor. These documents may already be available from regulatory bodies. Alternatively, standards organizations and industry groups can create them independently. We applied our principles to create an auditor and tested it on existing FDA/CE-approved mHealth apps. Our research suggests that the use of these non-legal, authoritative, guidance documents is a promising approach for computational auditing.

RESPONSIBLE DISCLOSURE

We have not publicly disclosed the vulnerabilities and are working with individual app vendors to fix them.

REFERENCES

[1] Adans-Dester et al. 2020. Can mHealth technology help mitigate the effects of the COVID-19 pandemic? *IEEE Open Journal of Engineering in Medicine and Biology* 1 (2020), 243–248.
[2] National Archives. 2019. Code of Federal Regulations Total Pages 1936 - 1949, And Total Volumes and Pages 1950 - 2019.
[3] Michael James Bommarito and Daniel Martin Katz. 2009. Properties of the United States code citation network. *Available at SSRN 1502927* (2009).
[4] Michael J Bommarito II and Daniel M Katz. 2010. A Mathematical Approach to the Study of the United States Code. *Physica A: Statistical Mechanics and its Applications* 389, 19 (2010), 4195–4200. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578094.
[5] U.S. Congress. 1934. United States Code: Table of Contents (1934).
[6] FDA. 2002. General Principles of Software Validation.
[7] FDA. 2005. Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software.
[8] FDA. 2005. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices.
[9] FDA. 2014. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.
[10] FDA. 2014. Distinguishing Medical Device Recalls from Medical Device Enhancements.
[11] FDA. 2016. Medical Device Reporting for Manufacturers.
[12] FDA. 2016. Postmarket Management of Cybersecurity in Medical Devices.
[13] FDA. 2017. Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices.
[14] FDA. 2018. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.
[15] FDA. 2019. General Wellness: Policy for Low Risk Devices.
[16] FDA. 2019. Off-The-Shelf Software Use in Medical Devices.
[17] FDA. 2019. Policy for Device Software Functions and Mobile Medical Applications.
[18] FDA. 2021. Search for FDA Guidance Documents. https://www.fda.gov/regulatory-information/search-fda-guidance-documents
[19] Dongjing He, Muhammad Naveed, Carl A Gunter, and Klara Nahrstedt. 2014. Security concerns in Android mHealth apps. In *AMIA Annual Symposium Proceedings*, Vol. 2014. American Medical Informatics Association, 645.
[20] Kathryn Howley. 2018. Role of mHealth in PHC. https://dukepersonalizedhealth.org/2018/10/role-of-mhealth-in-phc/.
[21] U.S. House of Representatives. 2020. United States Code: Public Law 116-259 (12/23/2020).
[22] Miloslava Plachkinova, Steven Andrés, and Samir Chatterjee. 2015. A taxonomy of mhealth apps–Security and privacy concerns. In *2015 48th Hawaii International Conference on System Sciences*. IEEE, 3187–3196.
[23] Connor Stewart. 2020. Growth in the number of medical apps downloaded during the COVID-19 pandemic by country in 2020. https://www.statista.com/statistics/1181413/medical-app-downloads-growth-during-covid-pandemic-by-country/.
[24] Brian Tung. 2021. *The Challenges of Applying Computational Legal Analysis to mHealth Security and Privacy Regulations*. Master's thesis. Washington University in St. Louis.
[25] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel R Reidenberg, N Cameron Russell, and Norman Sadeh. 2019. Maps: Scaling Privacy Compliance Analysis to a Million Apps. *Proc. Priv. Enhancing Tech.* 2019 (2019), 66.

[1] https://apps.healthskouts.com/