Comments of
The Health Record Banking Alliance
In response to
Federal Trade Commission
Notice of Proposed Rulemaking to Amend
The Commission's Health Breach Notification Rule
88 FR 37819 (June 9, 2023)
Health Breach Notification Rule, Project No. P205405

Submitted August 8, 2023 via https://www.regulations.gov

The Health Record Banking Alliance (HRBA)[1] offers comments responding to the FTC's Notice of Proposed Rulemaking (Notice) on proposed amendments to the Health Breach Notification Rule (Rule). (Defined terms in these comments are those used in the Notice.)

HRBA supports the FTC's proposed amendments to the Rule. HRBA also accepts the FTC's invitation to "comment on the proposed rule revisions generally [as well as] on the specific issues outlined [in the Notice]." Notice, 88 FR at 37822. Specifically, we offer comments placing the NPRM in the greater context of how the nation's health information infrastructure is critical to national security, national biodefense, and force medical readiness.

Summary of Recommendations to the FTC

The FTC should fashion changes to its Breach Notification Rule from the perspective of national security as a first priority. Secure systems design must become the unvarying norm, the essential foundation for our nation's health information architecture in this era of contstant threats. General comments regarding the NPRM in the context of national security, national biodefense, and force medical readiness are therefore wholly appropriates.

In these comments, HRBA recommends that the FTC:

1. Update the PHR breach notification rule to include ***presumed breaches*** based on, for example, AI (artificial intelligence)-enabled re-identification technology applied to supposedly anonymized data.
2. Recognize that the Office of the National Coordinator for Health Information Technology's (ONC's) planned architecture for TEFCA (the Cures Act's Trusted Exchange Framework and Common Agreement, which is mandated in Section 4003(b) of the 21st Century Cures Act as a

[1] The Health Record Banking Alliance, P.O. Box 6580, Falls Church, Virginia 22040, is recognized as a business league by the Internal Revenue Service under Section 501(c)(6) of the Internal Revenue Code. HRBA was founded in 2006 to advance the concept of Health Record (or Health Data) Banks. HDBs will hold consumers' owned and managed, aggregated, secure, lifetime health records compiled from diverse medical record systems. (The Appendix to these comments is a schematic of Health Data Banks.) HRBA's website is https://www.healthbanking.org/. HRBA documents filed with government agencies are available there. They deal with subjects including emergency clinical trials for biodefense, inherent vulnerabilities of the proposed national Trusted Exchange Framework (TEFCA), and the necessity for more rapid funding of a standardized national health data exchange standard based on FHIR (Fast Healthcare Interoperability Resources).

network to collect individuals' health data from multiple sources) will be so thoroughly insecure that PHR vendors, related entities, and their customers and counterparties should **not allow use of TEFCA for the sending or receipt of data**; and, if they do allow or inadvertently suffer any such use, breaches should be **presumed** and notifications triggered.

3. **Recommend, through the National Security Council, that the President intervene in health infrastructure planning** to require that TEFCA be thoroughly revamped. The reason for seeking such drastic intervention from the President is that ONC's current design for TEFCA is a convoluted, multi-network, layered and laddered design that is pervasively insecure. Each layer is an attack surface vulnerable to hostile penetration. The nodes connecting external networks to TEFCA, superfluous to secure point-to-point data exchanges, are all attack points. Having so many network nodes and layers inherently results in complex and insecure operating protocols, and violates the data exchange security requirements of Cures Act Section 4003(b). (**Alternative secure designs for TEFCA are explored in detail below.** They feature replacing fax exchange with direct, point-to-point, secure messaging based on Fast Healthcare Interoperability Resources (FHIR), and using secure Health Data Bank (HDB) repositories to hold patients' consolidated lifetime records that the patients control.) Thus, while Section 4003(b) requires ONC to implement TEFCA, **ONC has design options that are far less complicated, better engineered, more efficient, less costly, and – of utmost importance – designed from the foundation up to be secure**. **Because ONC has lost its way in designing TEFCA, the President must intervene** to assure that TEFCA implementation is put back on track, with ***secure systems design as the essential foundation for national health data infrastructure***. As part of this revamping, **the President is the only one in the position to require HHS/ONC to coordinate closely with Intelligence, Homeland Security, and Defense agencies. That coordination is the only way to assure that robust security is central to our national health data storage and exchange systems. Without that coordination, TEFCA (as ONC presently plans to implement it) will imperil security of the nation's health data and, perforce, will imperil national security, biodefense, and force readiness.**
4. Anticipate emergence of Health Data Banks (HDBs) as patient-centered components of secure nationwide health information networks, enabling patients to own and control their lifetime health data. Thus, the FTC will have the opportunity to analyze the extent to which patient control of their HDB-housed PHRs will, in the not-so-distant future, affect breach and breach notification regulatory considerations. (*Please refer to the Appendix for a schematic of Health Data Banks.*)
5. Look beyond immediate update of the FTC's Breach Notification Rule to advise Congress on enacting a regulatory framework for Health Data Banks; HDBs will emerge soon as a major sector of the health industry, and will adopt artificial intelligence/machine learning (AI) in operational

security and health data aggregation functions, as well as in patient advisory services including APIs (application programming interfaces).

The President Must Assure that ONC's Implementation Of The Cures Act's TEFCA Mandate Is Coordinated and Integrated with Intelligence Community, Homeland Security, and Law Enforcement Requirements, so that TEFCA's Architecture Becomes a Bulwark Rather than a Collection of Persistent National Security Vulnerabilities

HRBA is well aware of limits on the FTC's authority under Section 13407 of the Recovery Act. Yet, because of fundamental national security and patient privacy concerns, the FTC cannot consider PHR breach issues in isolation. Breach considerations must rather be analyzed as integral to a secure national health information infrastructure. Thus, in these comments, we identify pervasive vulnerabilities in ONC's implementation plans for TEFCA.

We observe that current policy at the Presidential level appears to silo ONC in its development and implementation of TEFCA. The result, intended or not, insulates ONC from security, systems architecture, and operational requirements that Intelligence, Homeland Security, and law enforcement agencies regard as essential. We demonstrate below the harm being done: TEFCA as ONC presently conceives it is *structurally insecure*, poised to become an incurable national security threat, besides being inefficient and therefore ineffective for care, medical research, force medical readiness, and biodefense.

If the President does not order a change of process now, TEFCA will emerge as a great waste of time and effort, a collection of ongoing security vulnerabilities that cannot in practice be secured, and a field of dreams for malevolent actors, both nation states and criminals.

Meanwhile,TEFCA's pending systems security debacle directly implicates the FTC's interest in security breach and breach notification rules for PHR vendors and their related entities. These considerations are part of the unitary whole of national biodefense in an era of known threats.

We call the FTC's attention to ongoing standardization of FHIR (Fast Healthcare Operability Resources) under ONC's Interoperability Rule as a developing national health data exchange standard. The Interoperability Rule supplies the first, FHIR-based iteration of a national, digital, health data exchange standard. The standard's scope will expand rapidly and infinitely using the Interoperability Rule's iterative Standards Version Advancement Process (SVAP).[2] (Parenthetically, we recommend that Congress appropriate federal funds to accelerate expansion of FHIR-based exchange standards through SVAP. The goal is to support an ever-widening, and ever-deepening, scope of medical specialty data requirements and associated research protocols.)

[2] For explanation of SVAP, see Department of Health and Human Services, *21st Century Cures Act:Interoperability and Information Blocking*, 85 Fed. Reg. 25642, 25644 (May 1, 2020).

Progressive standardization of FHIR will usher in HDBs as secure repositories available to consumers nationwide. HDBs will hold patient-owned and controlled, aggregated, lifetime health records. (HDBs are explained in more detail below and in the Appendix.)

In the next several years HDBs are likely to emerge as a significant operating sector in the nation's health data infrastructure. The government's task is to assure that this infrastructure is built based on security as its highest priority criterion. All other features of the infrastructure will depend on and follow from that foundation. [3]

A national health data infrastructure without security as its foundation would be dangerous, a national liability, unreliable, lacking public trust, and worse than useless.

Recommendations on Breach Issues Implicating National Security Imperatives, National Biodefense Strategy, and Force Medical Readiness

In comments filed earlier this year in context of national biodefense, HRBA asked OSTP to recommend to the President that he intervene with the Secretary of HHS. The purpose: to require ONC to re-do completely its plans for TEFCA. We reiterate that request in this forum; and we realize it is a startling request. ONC has devoted years, effort, and significant federal funding to its idea of implementing the Cures Act's TEFCA mandate. That includes designating an expensive "Recognized Coordinating Entity" to help develop and maintain TEFCA's Common Agreement.

But TEFCA, as ONC now is implementing it, is more than just a misuse of federal resources. *ONC's TEFCA architecture defies sound cybersecurity design principles. It envisions a complex mass of cobbled-together network nodes and pathways based on state-based or regional Health Information Exchanges ("HIEs") as network nodes.*[4] *The HIE nodes will not be connected by dependable, uniform communications and security protocols. Rather, ONC's design would move data using unwieldy, convoluted, non-uniform operating procedures.*[5] *That in turn would invite continuous successful security penetration. This concept of TEFCA is structurally insecure, an architecture made worse by deficient connectivity protocols suffused*

[3] Imperatives for secure cyber systems design in the healthcare sector are described in *China's Collection of Genomic and Other Healtcare Data from America: Risks to Privacy and U.S. Economic and National Security*, The National Counterintelligence and Security Center (February 2021), available at https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf .

[4] For a succession of graphics with text illustrating ONC's convoluted plans for TEFCA's architecture, see *User's Guide to the Trusted Exchange Framework and Common Agreement – TEFCA*, ONC Recognized Coordinating Entity (January 2022), available at https://rce.sequoiaproject.org/wp-content/uploads/2022/01/Common-Agreement-Users-Guide.pdf .

[5] The complexity of ONC's plans for TEFCA operations, necessited by ONC's labyrinthine TEFCA architecture, can be gleaned from *Qualified Health Information Network (QHIN) Technical Framework (QTF), Draft 2,* ONC Recognized Coordinating Entity (July 26, 2021), available at https://rce.sequoiaproject.org/wp-content/uploads/2021/07/QTF-V1-Draft.pdf .

with specific vulnerabilities, all gratuitous weaknesses. The result is that this TEFCA version could not, for any practical purpose, be secured to a satisfactory level. It is the opposite of ONC's professed goal of "a universal floor for [trusted] interoperability across the country."

The FTC is well aware that our nation's health data infrastructure faces constant, sophisticated attacks from nation states and criminals.[6] *They aim to compromise, contaminate, exploit, and otherwise damage health records in all corners of U.S. healthcare.*

This is an ongoing, pervasive threat that Senator Mark R. Warner, Chair of the Senate Select Committee on Intelligence, spelled out in his November 2022 report,"Cybersecurity is Patient Safety.[7] *This threat environment is so well known that there is no excuse for HHS/ONC's creating TEFCA as health data exchange network that – despite its being nominally labeled "Trusted"– is NOT built from the ground up on an advanced, robust, updatable security architecture. Rather, ONC's TEFCA plan is a cobbled-together, HIE-based, multi-HIE network, laddered, multi-layered, inherently insecure systems design. Each unnecessary external network node is a penetration attack point; each superfluous layer is an additional attack surface. If placed in operation, ONC's current TEFCA implementation plan would supply malevolent actors with unending, fertile breach opportunities. The targets would include the systems of any PHR vendors that used it, along with the systems and services of their related entities. These vulnerable uses would trigger endless streams of notification obligations for PHRs. They would be disastrous for patients; and notifications would become so frequent and routine that they would lose impact and fail to draw urgent attention.*

Section 4003(b) of the 21st Century Cures Act requires TEFCA to support information exchange between and among health information networks. However, that statutory requirement can be met just by supporting networks in hospitals and clinician offices. Nothing in the statute requires ONC to design TEFCA to preserve any particular classes of networks such as those of state and regional HIEs (Health Information Networks). But that is what ONC seeks to do. Unfortunately, cobbling together HIEs for TEFCA inevitably produces a layered, laddered, insecure network architecture with irremediable security vulnerabilities.

Note also that ONC's existing multi-HIE layered system design drastically and unnecessarily exposes patients' protected health information to examination by many, many network participants. Opportunities for unauthorized access would proliferate uncontrollably, and so of course would breaches that would have to be presumed, reported, and subject to

[6] See, e.g., Aynne Kokas, *Trafficking Data – How China is Winning the Battle for Digital Sovereignty*, Oxford University Press (2022), analyzing how China exploits U.S. government agency turf wars and fragmented, ineffective digital security requirements to gain increasing commercial, military, and political advantage; see also Dan Goodin, *Multiple Chinese APTs establish major beachheads inside US infrastructure*, Ars Technica (August 1, 2023), available at https://apple.news/ADdJ08NPbQJ64SFFUgt32WQ .

[7] Senator Mark R. Warner (D.VA.), Chairman of the Senate Select Committee on Intelligence, *Cybersecurity is Patient Safety* (November 2022, available at *https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf [press release at https://www.warner.senate.gov/public/index.cfm/2022/11/warner-releases-policy-options-paper-addressing-cybersecurity-in-the-health-care-sector]).*

HIPAA's breach notification requirements. But any use of this ONC iteration of TEFCA by PHRs and their related entities would be contaminated by TEFCA's breaches under HIPAA. That would in turn trigger application of the FTC's PHR Breach Notification Rule.

Instead, the Cures Act statutory mandate for network exchange is satisfied if a new, simplified TEFCA design adopts FHIR-based, point-to-point, secure messaging available to all network users, from individual consumers and patients to very large institutions and businesses. Such a streamlined architecture preserves the ability of hospital and clinician networks to exchange health data securely among themselves, with patients, and with entities such as health insurers and clearinghouses for treatment, payment, and health care operations. A streamlined design is capable of supporting trusted, high-volume data exchange for business-to-business purposes. Its advantage is significant: a streamlined, point-to-point network can be maintained and operated on zero-trust, high-security design principles.[8] *ONC's current design cannot.*

The FTC should update its Breach Notification Rule from this perspective. Further, the FTC is well advised to look beyond breach notification problems among PHR vendors and PHR related entities; it must address the larger security environment that is for the moment the disjointed, vulnerable collection of U.S. health information systems.

Two examples. First, technological advances, including in artificial intelligence (and not limited to AI), have long since altered concepts of de- and re-identification of data. The existing protocols for PHRs' or their related entities' sharing of supposedly de-identified data are obsolete. **Today, sharing data labeled "de-identified" must be presumed readily vulnerable to breaches. *Thus arises the concept and reality of presumed data breaches*.**

We understand that sharing supposedly de-identified health records might not in years past have raised expectations, or the certainty, of breaches. But the technology of re-identification is now widely available, very powerful, and easily applied.

Questions for the FTC involve how the health industry's sharing patterns of "de-identified" data should be treated under updates to the Rule. How often should breaches be presumed? Always? Whether the FTC asks these questions in this rulemaking or in follow-on proceedings, the FTC should begin to confront the issues now.

A second example arises from plans by ONC to adopt an inherently insecure architecture and insecure operating protocols for TEFCA. Section 4003(b) of the 21st Century Cures Act (Cures Act) mandates TEFCA's implementation and also lists high-level functional design and related engineering specifications premised on achieving secure data exchange.

TEFCA as currently envisioned by ONC fails to meet the high-level statutory specifications for secure health data exchange and for "computability." TEFCA's designed-in

[8] Zero-trust principles are widely used. See Security and Infrastructure Security Agency (CISA), *Zero Trust Maturity Model*, at https://www.cisa.gov/zero-trust-maturity-model ; see also, e.g., Kapil Raina, Crowdstrike, *Zero Trust Security Explained: Principles of the Zero Trust* Model (April 17, 2023), available at https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/ .

specific vulnerabilities raise the specter of *ongoing presumed data breaches* under the Rule. If PHR vendors and related entities were to use TEFCA as currently planned to exchange consumers' health data – for example, in service to treatment, payment, and health care operations ("TPO" in HIPAA terminology) – there would be constant opportunities for the data to be acquired, misused, and contaminated by hostile actors.

HRBA has argued this point repeatedly to ONC and, recently, to OSTP.[9] It remains important for national security, force medical readiness, and biodefense, as well as for patients' privacy protections and breach-related issues, to call out this failure and continue emphasizing it.

The fact that many TEFCA Qualified Health Information Networks (QHINs) and other "participants" will be HIPAA Covered Entities – and not PHR data sources holding consumer-controlled records and subject to the FTC's Breach Notification Rule – does not mean that the FTC should disregard TEFCA's many inherent security issues. The health industry is a frequently breached sector of the U.S. economy. Virtually all those breached facilities are today managed by HIPAA Covered Entities. Participating in the ONC's version of TEFCA would greatly increase their exposure to successful attacks. To the extent non-HIPAA Covered Entities, such as PHRs, ingest data sent into them through TEFCA from such compromised HIPAA Covered Entities and their business associates, the vulnerabilities, errors, viruses, ansd other contaminants that occur in the HIPAA world must be presumed to pass into the non-HIPAA, PHR world. Those contaminated data streams can be extremely difficult for PHR systems to detect. They may still, however, cause PHR privacy breaches subject to the FTC's Rule.

Therefore, in updating the Breach Notification Rule for the moment, FTC may as a policy matter caution PHR vendors (including HDBs) and their related entities ***not to use TEFCA****, once it begins operating, to gather, exchange, or otherwise use health data. This* ***cautionary policy*** *should be the rule so long as ONC's current TEFCA implementation plans remain in place.*

There is no disadvantage here. PHR vendors (including HDBs) and their related entities, along with hospitials and clinician offices, will have no use for a structurally insecure Trusted Exchange Framework as ONC has conceived it. In contrast, hospitals, clinician offices, insurers, researchers, and others in the health industry *would* use a Trusted Exchange Framework that is designed using a secure, streamlined, and efficient architecture.

[9] See, e.g., HRBA Comments at https://www.healthbanking.org/uploads/9/6/9/4/9694117/hrba_tefca_comments_20180220.pdf (criticizing ONC's TEFCA plans for failing to meet Cures Act engineering specifications); https://www.healthbanking.org/uploads/9/6/9/4/9694117/hrba_comments_rce_qtf_20210917.pdf (criticizing ONC's TEFCA plans for being institution- rather than patient-centered, and for failing to meet data quality and security standards, among other failings); https://www.healthbanking.org/uploads/9/6/9/4/9694117/ostp_rfi1_clin_res_infra_emerg_clin_trials_20230125.pdf, and https://www.healthbanking.org/uploads/9/6/9/4/9694117/ostp_rfi2_data_capture_emerg_clin_trials_20230125.pdf (comments to OSTP on emergency clinical trial infrastructure and data capture for purposes of national biodefense, requiring a full reassessment of TEFCA planning).

In that alternative streamlined design to implement TEFCA, users would exchange patients' data using secure, FHIR-based, point-to-point digital messaging systems that replace faxing. Patients, or HDBs and other PHR operators acting as patients' agents, would obtain records of various hospital and provider encounters by making verified HIPAA requests under 45 CFR Sections 164.524 and 164.501. An additional benefit: these PHR and provider digital messaging systems, engineered for efficiency and security, would wholly obviate the need for the cumbersome, wasteful TEFCA design that ONC is attempting to implement. And that change would be a defensible re-direction of federal funds.

The Looming National Security Problems of ONC's Plans For TEFCA

While the Cures Act mandates TEFCA, it by no means authorizes ONC to adopt an insecure network architecture, structurally vulnerable to constant attacks and successful breaches, and otherwise unsuited to exchange data efficiently for patient care, biomedical research, or national biodefense. There are other design options based on the foundation of secure network design principles. ONC should be re-directed to those options.

ONC's current exchange framework under the Common Agreement requires TEFCA signatories – "Qualified Health Information Networks" ("QHINs") and downstream "participants" and "sub-participants" – to respond endlessly to successive nationwide query messages seeking data on each particular patient being seen at any and every point of care throughout the nation. This discredited "shotgun query" or "record locator query" design cannot feasibly be implemented at scale. It would *overwhelm networks' capacities for throughput*, create unsolvable patient matching problems generating streams of privacy rule violations, and generate cascading liability issues.

ONC's plans to use record locator protocols makes TEFCA problems worse by inserting regional brokers and disparate, local, voluntary exchanges as central to the national data exchange network. This setup makes the system not only unnecessarily costly and chaotic, but fraught with embedded security and privacy issues. Access control and user authentication are well known problems that multiply at an accelerated rate at scale when disparate network operating, communications, and control systems are forced together in uncoordinated network combinations. There is no reason to support this inefficient, error-prone architecture.

TEFCA deficiencies can be illustrated when considering emergency clinical trials for biodefense, as OSTP seeks to do. Supporting clinical trial research, whether or not in emergency conditions during biodefense attacks, requires reliable communications between researchers and patients for recruitment, ongoing trial protocol execution, and follow-up. These requirements cannot be met by TEFCA's SOP for Individual Access Services.[10] That protocol is beyond cumbersome. It is in practical effect a barrier to patients' obtaining their

[10] TEFCA's numbingly elaborate Individual Access Services SOP is available at https://rce.sequoiaproject.org/wp-content/uploads/2022/09/Final-SOP-IAS-Exchange-Purpose-Implementation.pdf .

complete medical records and, at each patient's individual election, communicating those records to providers and trialists under research protocols.

If forced to use ONC's current version of TEFCA, the clinical trial community – research institutions, clinical trialists, health care providers interested in clinical research (including community health care organizations), contract research organizations (CROs) and other clinical trial service providers, pharmaceutical and biotechnology companies, and research sponsors – would face constant unnecessary recruitment obstacles, process delays, ongoing regulatory compliance problems, and undue expense.

As the FTC considers *presumed* breaches arising from ONC's current TEFCA plans, note how far ONC's SOP for Individual Access Services departs from the Cures Acts *mandatory* functional systems design specifications. These design requirements, essentially high-level engineering specifications, are centered on patients, not institutions. They are found in sections 4002 of the Cures Act, as it amends HITECH sections 3001(c)(5) and adds section 3009(a), as follows:

- Health information technology must "*[enable] the **secure** exchange of electronic health information . . . without special effort*" on the part of users. (Patients and physicians are among "users" under the Cures Act.) (HITECH as amended, new §3000(10)(A), as added by Cures Act §4003(a); emphasis added.)

- EHR data exchange must allow "*complete* access, exchange, and use of all electronically accessible health information for ***authorized use*** [under applicable law]." (HITECH as amended, new §3000(10)(B), as added by Cures Act §4003(a); emphasis added.)

- EHR data exchange cannot be implemented by ONC in ways that restrict "exporting *complete information sets*" as part of access to, or exchange of, health information. (HITECH new §3022(a)(2)(C)(i), as added by Cures Act §4004; emphasis added.) This means export of all of a patient's health records in the EHR system if a patient so requests.

- EHR data exchange must allow "access *to all data elements* of a patient's electronic health record" permitted by privacy laws. (HITECH new §3001(c)(5)(D)(iv) as added by Cures Act §4002; emphasis added.)

- EHR data exchange *cannot* be implemented by ONC in ways that *"are likely to substantially increase the complexity or burden"* of access to, or exchange of, health information. (HITECH new §3022(a)(2)(B) as added by Cures Act §4004; emphasis added. This provision perforce imposes a specific requirement for nationwide standardized exchange.)

- EHR data exchange must be enabled through the use of application programming interfaces or *successor technology or standards*. (HITECH new §3001(c)(5)(D)(iv) as added by Cures Act §4002; emphasis added. *FHIR-based* *data exchanges and HDBs are successor technologies.*)

- EHR data exchange must provide *the patient or an authorized designee* with a *complete copy* of his or her health information from an electronic record *in a computable format*. (HITECH new §3000(10)(B) as added by Cures Act §4003; emphasis added.)

TEFCA's SOP for Individual Access Services fails all these statutory functional specifications. And it is centered on institutions, not patients. It is a formidable barrier to convenient, comprehensive, secure use by patients and consumers for health data exchange purposes – as is true of ONC's overall concept for TEFCA.

ONC has anticipated FHIR's continuing development as the de facto means for national health data exchange. In that context, ONC has sought to promote its current design for TEFCA by stressing the desirability of "Network-Facilitated FHIR Exchange" and " QTF (QHIN Technical Framework) Brokered FHIR Exchange."[11] But ONC's (and its TEFCA Recognized Coordinating Entity's) attempt to justify TEFCA this way only illustrates the superfluity of the convoluted, HIE-based TEFCA architecture on which ONC has settled.

Reading the FHIR Roadmap for TEFCA Exchange v.1 demonstrates that "network-facilitated" and network-brokered" exchange will only supply new security vulnerabilities (more attack surfaces and a greatly increased number of network nodes) and added network cost and complexity without adding useful functionality. The functions that ONC touts – "business-to-business (B2B) clinical interoperability supporting simple, high-volume, high-reliability, high-trust exchange patterns" – can be more efficiently accomplished with greater security using streamlined point-to-point exchanges of FHIR-based data. That is the alternate network design that ONC must be directed to adopt for TEFCA implementation under the Cures Act.

To continue this point, the industry's embrace of TEFCA does *not at all* "[make] it imperative that TEFCA include a deliberate strategy to add FHIR-based exchange."[12] The better approach is for TEFCA to abandon both "network-facilitated FHIR exchange" and "QTF brokered exchange." Why insert unnecessary network nodes, attack points, and attack surfaces into otherwise straightforward, point-to-point exchanges? There is no reason for these complexities other than to preserve existing, but obsolete, bureaucratic structures.

While ONC's present TEFCA architecture may attempt to preserve a continued role for HIEs, that is no reason to compromise network security, add complexity to network architecture, and increase cost and network load without improving functionality. (HIEs operating today may themselves consider the possibility of converting to Health Data Banks; but that is an option for

[11] ONC Recognized Coordinating Entity, *FHIR® Roadmap for TEFCA ExchangeVersion 1* (January 2022), available at https://rce.sequoiaproject.org/wp-content/uploads/2022/01/FHIR-Roadmap-v1.0_updated.pdf .

[12] *FHIR Roadmap* at 4.

later exploration.) Thus, in its *FHIR Roadmap for TEFCA,* ONC only succeeds in demonstrating the deficiencies of its present implementation plans.

Health Data Banks Will Be a Significant Industry Sector in a Secure Nationwide Health Information Infrastructure

The U.S. can engineer a secure, nationwide health information exchange network based on Health Data Banks (HDBs). The network design would be FHIR-enabled, streamlined, and point-to-point, and it would feature robust security.

HDBs will emerge as potent contributors to such a secure, convenient network architecture. The reason is that the core business of HDBs will be collection and storage of patients' health data, the protection of patients' health data, and the execution of patients' wishes regarding their data.

With HDBs, medical record data can be extracted efficiently from hospitals' and clinicians' electronic health record (EHR) systems using standardized FHIR. Each exchange is direct between source and HDB, so only the receiving HDB "touches" the data. There are no gratuitous intermediaries. In addition, HDB can accept patient-provided information, such as from the growing number of FDA-approved mobile and other personal sensor devices.

Patient health data received in FHIR from hospitals and clinicians will be normalized, compiled, and held in patients' HDB PHRs. The compiled records will be available in HDB accounts under patient control in problem-oriented, lifetime health reference records. (Hospitals and clinicians' offices will continue to maintain their own records documenting their encounters and processes with respect to each patient. Those regulatory requirements will not change.)

HDBs will employ AI for security and data aggregation and normalization, among other operating functions. HDBs will also offer analytical and advisory services to help PHR account holders interpret what is in their lifetime health records, including to aid in diagnosis and treatment. AI and machine learning systems will enhance these functions.Third parties will also offer complementary advisory and AI/machine learning analytical services to help patients use HDB-based PHRs. A precondition for AI use in any of these advisory services is demonstrating a reliable understanding of how and why AI generative language and image models work, and how to engineer systems to exclude fabrications (hallucinations) and similar spurious outputs.

Patients can elect to employ their lifetime HDB reference records for care (by granting full or tailored, partial access to providers at points of care), research, and participation in national biodefense. These attributes will among other benefits complement force medical readiness data requirements (and medical force data needs).

Secure, convenient, point-to-point, FHIR-based health data exchange as described earlier will enable routine patient-mediated digital communications and much more: point-to-point data flows between consumers and providers, providers and other providers, sconsumers and payors, providers and payors, payors and other payors, patients and researchers, clinical trial administrators and patients, clinical trial administrators and clinicians, clinical trial administrators and government agencies – all will benefit from standardized FHIR-based interoperability.

Because protection and secure management of patients' information is the core business of a Health Data Bank, authorized disclosures of PHR-identifiable information and notification to patients about disclosures are both standard operating procedures for HDBs. All disclosures are authorized, audited, and routinely reported to the HDB's PHR account holders. Reliable and meaningful authorization is central to an HDB's operations, and will be highly personal and customized to each specific account holder. Depending on specific HDB business models, authorizations and approvals of disclosures will be annotated and available for account holders' examination and follow-up.

Clinician and researcher burdens due to data system complexities and lack of data normalization will be ameliorated when HDB PHR account information is readily available as a *reference* "single source of truth" for use by clinicians via *compartmentalized import* into hospital and medical office EHR systems. Reliable patient data with provenance, aggregated from diverse providers, and supplemented with contemporaneous patient observations and with data from wearables and other personal devices, will be readily searchable in problem-oriented PHRs or other enhanced formats that HDBs may adopt.

For research purposes, patients with HDB PHR accounts will be able at their election to participate voluntarily in public health initiatives such as emergency clinical trials. Consumers will have convenient means to report voluntarily to clinicians and, as appropriate, public health authorities, to seek evaluation of symptoms, advice on potential treatments or vaccinations, and research projects related to public health emergencies. These HDB PHR capabilities will complement mandatory public health reporting requirements applicable to clinicians and other provider institutions.

HDBs also will eventually be infrastructure resources for decentralized clinical trial networks. They will enable points of care across the nation where, increasingly today, *both* clinical care and clinical research are being performed.[13] HDBs can provide two-way channels for communications with patients during public health emergencies at the grass roots level of U.S. health care. HDB functionality will, for example, aid rapid collection of data, including novel digital endpoints, as needed for new disease or bio attack outbreaks.

HDBs, created initially as a care resource to benefit patients and their providers, will thus also offer a permanent, standing resource for "warm-base" clinical research. All this will contribute to national biodefense strategy as well as to force medical readiness.

These are key health care priorities for a nationwide health IT infrastructure as contemplated in section 3001(b) of the Public Health Service Act (PHSA). They illustrate *the inherently efficient, superior systems design of integrating health data around the patient*, which bestows enormous improvement in the efficiency and utility of health information exchange. That is the core systems advance that HDBs will contribute as an industrial sector to U.S. health care, the health industry, and the health research enterprise.

[13] See: Point-of-Care Clinical Trials: Integrating Research and Care Delivery, Duke-Margolis White Paper, May 11, 2021. See also: The Coalition for Advancing Clinical Trials at Point of Care (ACT@POC).

The FTC Should Advise Congress on the Importance of Legislating a Regulatory Framework for HDBs to Preserve Public Trust and Prevent Abuse of the HDB Concept by Bad Actors

A proponent of HDB PHRs since 2006, HRBA is also an advocate both for industry self-regulation and standards of conduct, and for federal regulation of HDBs and other private-sector repositories of consumers' health data. Federal regulation is a necessity to keep bad actors from offering predatory HDB services. Regulation must also be tailored so HDBs can innovate continually in the storage, analytical, and advisory services they make available to consumers and to employers who understand the advantages of encouraging (and in many cases subsidizing) PHR use by their employees.

Early industry resistance to regulatory oversight for use of AI in EHR systems[14] highlights the need for Congress to craft a national regulatory framework for HDBs and other PHR services. Congress should consider delegating to an appropriate agency or agencies the responsibility, through notice and comment rulemaking, to develop legal, technical, and financial qualification requirements as elements of a certification or licensing process for PHR vendors. Consumers' security and privacy interests should be at the center of such a regulatory framework. So should the necessity for network security design to be the foundation for HDBs' structure and operations.

The FTC's consultations with Congress, HHS, and other departments and agencies for these purposes cannot begin soon enough

Conclusion

HDBs'design of patient-centered technology for PHR services, really a bundle of technologies, will emerge as a significant segment of infrastructure for health care and research in the U.S. The FTC's update of its breach and breach notification rules for PHR vendors and their related entities should be a platform for consideration of foundational national security and biodefense concerns – and opportunities – in the regulation of PHR systems for the present and in future.

In the interim, we urge the FTC to participate aggressively in consultations with intelligence, defense, and other cabinet-level agencies on PHR data breach issues and the larger national security and network design questions of which they are a part. Those consultations should center on the necessity for developing a coherent, secure architectural concept for the nation's digital health information infrastructure. This is a practical and unavoidable responsibility in the high threat environment we face today and will face for the foreseeable future.

No other approach will protect the nation's health information infrastructure, our capacity for biodefense and force medical readiness, and the privacy of patients and consumers across the

[14] See, e.g., Casey Ross, *As fear rises over AI, Google and Epic fight stronger regulation of the technology in health care*, STAT News (July 17, 2023), available at https://www.statnews.com/2023/07/17/ai-regulation-google-health-epic/ .

nation. We urge the FTC to support conducting those urgent consultations through the National Security Council, and then taking them to the President.

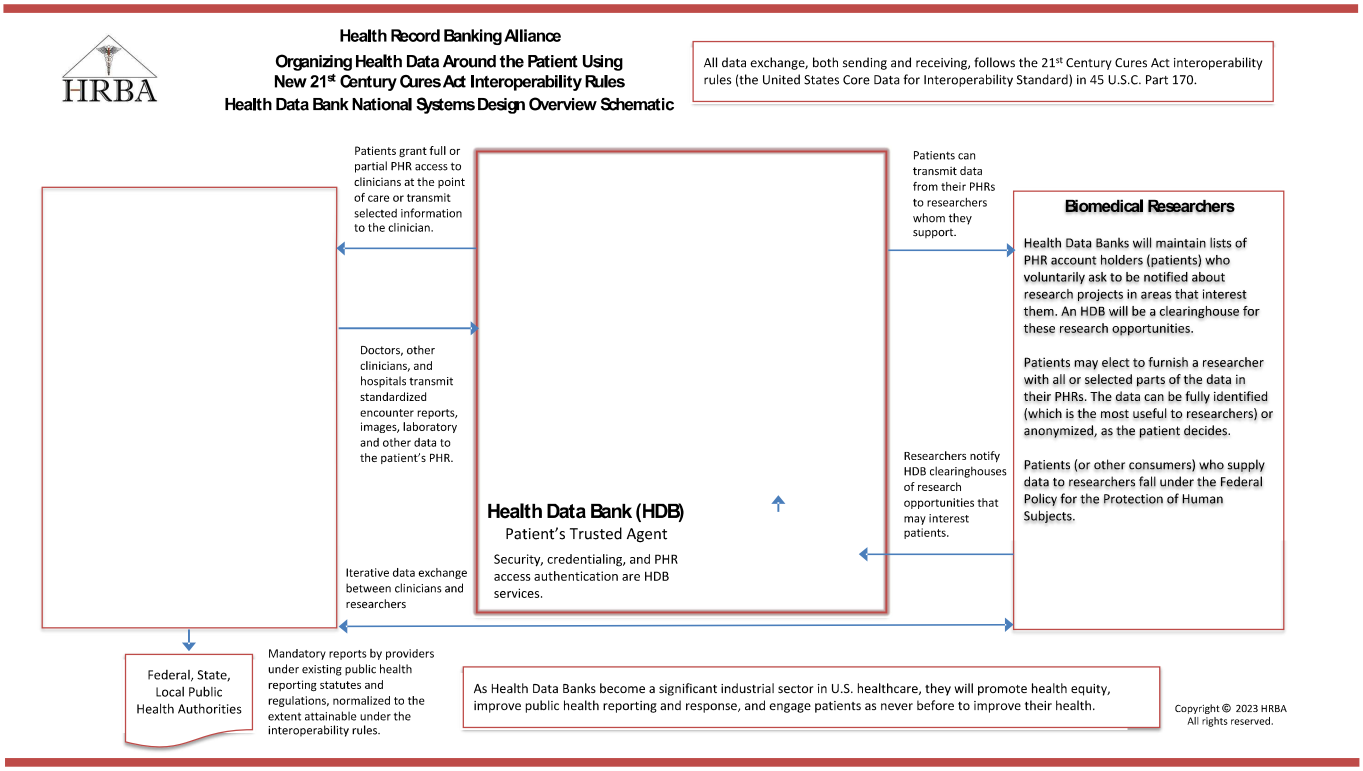
Respectfully submitted,

The Health Record Banking Alliance

/s/ Richard D. Marks
Richard D. Marks, Vice President
richardmarks@earthlink.net

Appendix

Health Data Bank (Health Record Bank) Schematic Overview
And
Descriptive Summary



HRBA

Health Record Banking Alliance

Organizing Health Data Around the Patient Using New 21st Century Cures Act Interoperability Rules

Health Data Bank National Systems Design Overview Schematic

All data exchange, both sending and receiving, follows the 21st Century Cures Act interoperability rules (the United States Core Data for Interoperability Standard) in 45 U.S.C. Part 170.

Patients grant full or partial PHR access to clinicians at the point of care or transmit selected information to the clinician.

Doctors, other clinicians, and hospitals transmit standardized encounter reports, images, laboratory and other data to the patient's PHR.

Iterative data exchange between clinicians and researchers

Health Data Bank (HDB)

Patient's Trusted Agent

Security, credentialing, and PHR access authentication are HDB services.

Patients can transmit data from their PHRs to researchers whom they support.

Researchers notify HDB clearinghouses of research opportunities that may interest patients.

Biomedical Researchers

Health Data Banks will maintain lists of PHR account holders (patients) who voluntarily ask to be notified about research projects in areas that interest them. An HDB will be a clearinghouse for these research opportunities.

Patients may elect to furnish a researcher with all or selected parts of the data in their PHRs. The data can be fully identified (which is the most useful to researchers) or anonymized, as the patient decides.

Patients (or other consumers) who supply data to researchers fall under the Federal Policy for the Protection of Human Subjects.

Federal, State, Local Public Health Authorities

Mandatory reports by providers under existing public health reporting statutes and regulations, normalized to the extent attainable under the interoperability rules.

As Health Data Banks become a significant industrial sector in U.S. healthcare, they will promote health equity, improve public health reporting and response, and engage patients as never before to improve their health.

Please see accompanying text on the following page.

Health Record Banking Alliance

Organizing Health Data Around the Patient Using New 21st Century Cures Act Interoperability Rules

Health Data Bank National Systems Design Overview

A **Health Data Bank** (**HDB**, also called a Health Record Bank) is an **integrated patient information services institution**. As a **trusted agent**, it offers a **secure repository** for each individual to collect and compile their **"interoperable"** digital health information in a **smart Personal Health Record (PHR).** Individuals own and control their Personal Health Records, as in a bank checking account. With these **new information flows**, consumers will:

- exchange medical records and other health data in their Personal Health Records conveniently with doctors' offices and hospitals for better, faster care; improve patient safety; and reduce information burden on physicians by supplying an aggregated, lifetime, searchable medical record for easy and immediate reference.

- control Personal Health Record access for doctors and hospitals; family, friends, and health coaches; medical researchers; members of the press; and others as they wish.

- use their Personal Health Records to help manage their health and healthcare, and to help shop for doctors, hospitals, and health insurance.

- view their Personal Health Records on smartphones, tablets, and other computers.

Health Data Banks and Efficiency: Integrating health information around each patient via HDBs is the most efficient way to aggregate and use **"interoperable"** health data under 21st Century Cures Act regulations. It is far more efficient and useful than a collection of "apps."

HRBA's Education and Policy Advocacy: HRBA advocates government policies promoting Health Data Banks as **a major new structural sector in U.S. health care**. This systems design includes a **national regulatory framework for Health Data Banks**.

Health Data Banks and Health Equity: Health Data Banks will promote **health equity** because **everyone** can have a Personal Health Record in a Health Data Bank.

Health Data Banks as Medical Research Clearinghouses: Medical researchers cannot get enough patient data to make fast or sufficient progress. HDBs can be clearinghouses between patients and researchers. Patients can **voluntarily** list themselves with their HDBs to be informed of research projects they are interested in, and to which they want to **contribute or sell their data**. This also is a path to developing **national federated diagnostic and research databases** while respecting **patients' privacy rights** (because patients are in control). Better research will improve treatment for acute, chronic, and orphan diseases.

Health Data Banks, Security, and Patient Matching: Security, credentialing, and patient authentication and efficient matching are systems design features of HDBs.

Advanced Features of Smart Personal Health Records: Systems design features such as artificial intelligence (AI) and search capabilities, robust family history, and genomic analytics will deliver **problem-oriented data and analysis** to **mesh** with clinicians' Electronic Health Record (EHR) systems **at the point of care**. Availability of this aggregated **reference record** will reduce burdens on clinicians while improving diagnosis, treatment, and patient outcomes.