FROM MEANINGFUL USE TO MEANINGFUL USES:
GETTING THE MOST FROM MEANINGFUL PATTERNS IN DATA TO IMPROVE HEALTH
It seems odd, at first blush, that the largest, most sophisticated sector in the world’s most advanced economy should only recently have devoted significant resources to adopt and use electronic health records and other health information technology (IT). Yet, leading up to the passage of the 2009 HITECH Act, only a handful of American health providers used secured messaging in their daily routines. Fewer than two percent of hospital systems had comprehensive IT systems capable of tracking patients’ symptoms and treatments across care settings. Only after 2010, with the “carrot” of $35 billion in “Meaningful Use” grants and the “stick” of Medicare payment penalties, did medicine begin its grudging en masse march into the 21st century and the Information Age.

While today that journey remains far from complete, a growing array of IT-enabled technologies are queuing up to reinvent medicine in ways that promise to make it better, cheaper, and more customer-friendly. Nine years into the era of smartphones and distributed cloud-based computing, an emerging medical “Internet of Things,” and the algorithms that power them—from self-teaching artificial intelligence apps to digitally connected subcutaneous sensors—are making it possible to detect, diagnose, monitor, and treat conditions with ever greater efficiency. Advances in the laboratory are raising hopes of a hundred-fold increase in the introduction of new drugs, many of them personalized to each individual’s genetic makeup.

But first, America must modernize its bulky health regulatory system—a structure that, by design, is wary of innovation, and zealously guards patient privacy, raising the cost of data and limiting its beneficial use by clinicians and researchers alike. Implicit in this bargain is the belief that the benefits of slow and deliberate change outweigh the associated economic and human costs, but accelerating developments are challenging this calculus. Warns Dr. Joseph Smith, Chief Medical Officer for West Health Institute, “We may be protecting patients to death.”

High costs are known to deter patients from seeking treatments. Supporting evidence is also found in research showing that well-designed and integrated clinical decision support (CDS) tools produce better, safer outcomes with fewer costly readmissions. In part because of regulatory roadblocks, such tools are not widely used. Often, they cannot incorporate the improving state of the art because research is hampered by civil and criminal liabilities.

This suggests that patients may benefit from a health regulatory framework that is more trusting of IT and less ossifying in its view of how medicine must be practiced. But less regulation is not always best. Maximizing the game-changing potential of health IT requires improved interoperability—not simply within the clinic but between settings, as well as with researchers whose analytics shed light on what practitioners are seeing and how best to respond, and of course, with patients. Patients and the public at large stand to benefit most from a regulatory framework that promotes the sharing, rather than the hoarding and resale, of patient health data. This white paper reflects a collaboration between Apervita, a health data analytics firm, and Health IT Now, a broad-based coalition of patient groups, provider organizations, employers, and payers that supports incentives to deploy health IT to improve outcomes and lower costs. The information presented here was generated at a full day symposium of industry experts, hosted at MATTER, a Chicago-based association of health technology developers and users, for the purposes of identifying regulatory barriers to health technology and presenting possible solutions.

To this end, we outline the current health care landscape, identify the federal laws and regulations that inhibit innovation, and offer policy recommendations to decision makers. Representing the collective input of more than 100 conference attendees and speakers, this paper intends to serve as a roadmap for leaders who see innovation as the key to improving care and lowering costs.

We recommend a two-step regulatory solution, consisting first of supporting interoperability; and second, of implementing thorough legal and regulatory reforms geared toward the democratization of health data analytics. Specifically, we call for:

- **MEANINGFUL USE REFORM.** The United States Government Accountability Office (GAO) reported in September 2015 that America has a long way to go to realize the HITECH Act’s stated goal of electronic health record (EHR) interoperability. We believe that progress on this front will require a new Meaningful Use policy that promotes interoperability. Such rules should penalize providers and their vendors that commercially benefit from information blocking. Only interoperable EHR systems should qualify under Meaningful Use.

- **FDA REFORM.** Innovation is most productive in a defined regulatory environment where risks are understood. The Federal Food and Drug Administration’s (FDA’s) current lack of fixed regulatory boundaries creates both actual risk and the perception of risk, which inhibits not only the scope of product design, but also the willingness of investors to support the necessary research and development of IT-enabled tools and products.

- **DATA POLICY REFORM.** Health IT’s changing landscape includes institutional shifts toward value-based payment. Whereas the measurement of inputs, such as procedures or tests, is straightforward, the discovery of value is data-intensive. Value is a comparative concept, and its measurement involves not just before and after metrics for the patient being treated, but similar data from a great many patients. Such comparisons can tell us which set of diagnoses and treatments achieve desired outcomes efficiently while broadening our knowledge of best practices—an important public good. A new generation of data apps are needed if Medicare and private insurers are to successfully transition toward payment systems that reward health outcomes rather than input volume. Freeing data for this use will require better, smarter privacy laws. HIPAA, HITECH, the Common Rule, and other federal and state regimes prohibit the efficient collection, transfer, and beneficial use of the health data. This regulatory structure, enforced by criminal and extraordinary financial sanctions, fuels an overabundance of caution that inhibits permissible research.
I. DISCUSSION—BARRIERS TO IMPROVING HEALTH CARE

The Information Age is changing nearly every aspect of life, and that could especially be true in health care—if only we would let it. The trend toward individualized medicine, outlined in President Obama’s Precision Medicine Initiative, reflects the insight that diseases, such as diabetes, once thought to have common causes and effects, in fact are highly specific to each individual’s unique genetics, environment, and lifestyle—and hence require individualized interventions. Though this approach is more widely applied to cancer, heavy restrictions on the uses and transmission of health data inhibit it for other disease populations. The more access researchers have to population-wide genetic and phenotypic information, the more they can learn about trends in diseases, which in turn will allow for more accurate and efficacious treatments.5

Two specific barriers prevent us from tapping into this wellspring of data: (1) the lack of interoperable health systems; and (2) health IT regulation, where the second problem contributes significantly to the first.

Lack of interoperability across health care settings greatly impedes providers’ ability to administer coordinated patient care and eliminate unnecessary tests as well as treatments for avoidable (and often dangerous) drug interactions. Additionally, business practices that employ information blocking weaken the quality of care in ways that harm patients both directly and indirectly. Establishing interoperability requires the reexamination of the Health Insurance Portability and Accountability Act (HIPAA), the Meaningful Use (MU) Program under the Office of the National Coordinator (ONC), and, relatedly, ONC’s Health IT Certification Program.

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996,6 sets out to protect patient privacy through strict controls on the use and sharing of information on health treatments, payments, and related administrative data, enforced by criminal and civil penalties. These rules pose significant barriers to interoperability, not the least because communicating in an unsecured format carries significant regulatory risks.

Patient data can only be transmitted if it is first statistically de-identified—an expensive and, due to technology, increasingly impossible undertaking.

Additionally, as patient data becomes the key to value discovery, institutions have stronger incentives to “hoard” the data in their control, thus creating data “silos.” Notably, institutions that hold protected data can use it for internal research with relatively few constraints. Thus, for example, the merger of hospital systems or insurance carriers gives the merged entities access to data they did not previously have. As value discovery grows in economic importance, such troves have emerged as lucrative profit centers.

HIPAA’s privacy regime consists of two main elements. The first of these is the implementing of regulations related to privacy. These regulations set forth the so-called “minimum necessary” standard, which limits the use or disclosure of a patient’s protected health information (PHI) to the minimum amount necessary to carry out the purpose of the disclosure.7 Exceptions include health treatment (the main purpose of EHRs), payment and health care operations, and the disclosure of information to the patient and the U.S. Department of Health and Human Services (HHS).8

The rules permit very limited third party use of multi-patient data sets if certain patient identifiers are removed prior to use.

The second key element is the Security Rule.9 This rule pertains specifically to electronic protected health information (ePHI) and sets standards for its de-identification, including: (1) statistical determination; or (2) a safe harbor method that involves removing 18 identifiers. Statistical de-identification requires that patients cannot be re-identified using available data not in the health record.10 For example, if there were only a handful of patients in a given county, the inclusion of county data for those patients might permit their re-identification using data sources from the census and grocery store purchases. One new line of thinking holds that a more practical means for protecting privacy would be to penalize the misuse of data derived from analytics, a rule that is already in effect when researchers inadvertently re-identify patients.11

It remains that HIPAA was drafted to allow for the use and sharing of information for treatment of individuals, payment, and health care operations, largely without regard to the value of collecting population data or sharing data between institutions. Created well before modern apps and mobile devices were produced or imagined, the law stunts the development of current IT apps designed to discover value based on large patient datasets. Removing this barrier could broadly improve population health, and open doors to better medical care such as precision medicine.12

B. MEANINGFUL USE PROGRAM

The Meaningful Use (MU) Program has spurred the growth of EHRs, but not in a manner conducive to interoperability. The Centers for Medicare and Medicaid Services (CMS) administered program has given out $32 billion in incentive payments as of February 2016. The latest report from ONC shows that, as of 2014, almost three-quarters of Medicare providers had adopted certified EHRs, but only 26 percent had shared electronic patient information with unaffiliated providers.13 Burdensome and user-unfriendly standards are partly to blame. One result is that federal programs are not fully capitalizing on the potential of interoperable health technologies to improve patient health and create new cures.

The ONC also runs the Health IT Certification Program (Certification Program), designed to provide assurance to purchasers and other users that an EHR system meets the technological capability, functionality, and security requirements adopted by HHS, including interoperability.14 The Certification Program15 is voluntary and was established to provide for the certification of product functionality against health IT standards, implementation specifications, and certification criteria adopted by the HHS Secretary.
C. FDA REGULATION OF HEALTH IT

Laws—and their implementing regulations—are inherently ambiguous regarding technologies not contemplated at the time of their drafting. The Food, Drug and Cosmetic Act (the Act) contemplated that health care products were exclusively tangible. At the time, “medical device” referred to physical instruments intended for use in the diagnosis or cure of disease. Nothing in the Act defines health software as a device. Yet given the broad reach of FDA’s regulatory authority, this ambiguity has created real and perceived financial risks for IT developers—which, in turn, impede the pace and adoption of cost- and life-saving technologies in the clinic.

FDA has taken pains to reassure health IT developers that it does not currently plan to subject software—a new class of algorithms that do everything from organizing ePHI to running the artificial intelligence in CDS tools—to certification as medical devices. At the same time, the agency claims broad authority to classify health data software as devices.

FDA’s pronouncements on software regulation have come in the form of non-binding sub-regulatory guidance. Sub-regulatory tools include guidance documents, interpretive rules, advisories, bulletins, manuals, and information sheets that limit the opportunity for public input. These lack the force and effect of law and are designed merely to represent the agency’s current thinking. Their advantage is to allow FDA to keep its options open while avoiding costly and cumbersome formal rulemaking or judicial review. But such guidance is, by its nature, perennially subject to change. This impermanence breeds an abundance of caution among both developers and the investment community. Instead of encouraging innovation, FDA’s reliance on sub-regulatory tools has fostered hesitation at great cost to the industry and the public.

Were FDA to change its mind and subject all software to regulation as devices, the effect would be highly disruptive. The 510(k) medical device approval process is costly, time-consuming, and badly out of sync with the rapid evolution guiding the software industry. For example, mapping apps on smartphones are updated several times every month and are designed to evolve continually—ideally, at an ever-quickening pace. Medicine, likewise, is starting to change more rapidly. Clearly, if patients are to be served by CDS systems, the best practices they are designed to incorporate will evolve continually—ideally, at an ever-quickening pace.

II. SOLUTIONS

A. ACHIEVING INTEROPERABILITY BY UPDATING HEALTH IT AND USING ENFORCEMENT AND DETERRENCE

A fully interoperable health care system will break down data silos and facilitate the adoption of value-driven care delivery models. To this end, Congress should define and require “interoperability” in federal statute, and enforce this requirement with sanctions designed to prevent health data blocking.

Interoperable EHRs are able to share information across platforms according to industry-based standards. We do not envision that such standards would impose a common EHR design; rather, it would mandate that the information they contain is conceptually equivalent and can be exchanged across platforms. Once equivalency is established, implementing a common exchange format is relatively straightforward.

Other aspects of the health IT policy architecture should be renovated to accommodate interoperability. HIPAA, in particular, should be modified to eliminate those features that discourage health IT. Such reforms must make clear that HIPAA’s role is to balance patient privacy—a private good—with the public interest in making patient data available for research purposes. In addition, patients benefit directly when data sharing across care settings leads to higher value care.

Despite improvements in technology, HIPAA is becoming harder to implement. The capabilities of data analytics are such that access controls alone no longer provide the level of privacy protection their advocates once envisioned. An alternative approach—controlling the use of data derived from analytics—has shown to achieve better results with fewer costs. Access controls impede patients’ access to their own health information, which means they are harmed by rules designed to help them.
To address these problems, Congress should:

1. Modify HIPAA standards that restrict third-party data storage vendors, who hold data on behalf of health systems and insurance carriers (e.g., covered entities), from releasing PHI directly to patients and their providers. Legislative permissions are required so business associates can directly provide patients with their health information.

2. CMS should utilize its authority under the Medicare Access and CHIP Reauthorization Act (MACRA)\(^2\) to make conforming updates to the MU Program to reduce extraneous and burdensome requirements on physicians and vendors. Any current MU objectives and measures not focused on meaningful and relevant information exchange among providers or patients should be removed entirely or re-categorized into a more appropriate Merit-Based Incentive Payment System (MIPS) category. Reforms to MIPS should go beyond the simple repackaging of existing programs. Each requirement in the Physician Quality Reporting System, Value-Based Modifier program, and MU program should be evaluated to determine whether it should be eliminated, moved to another category, or combined with similar (often duplicative) measures.

3. CMS must rein in the proliferation of voluntary and mandatory incentive programs. This proliferation has increased program complexity and administrative burden, and is reducing satisfaction and success rates among the provider community. Such reforms would be consistent with Congress’s intent under MACRA to consolidate and simplify programs measuring quality, resource use, EHR use, and clinical practice improvement activities. Finally, Congress must put regulatory teeth into rules designed to enforce interoperability and deter data blocking, either directly or through software or business agreements. Enforcement mechanisms should include a system of monetary penalties similar to those under the federal False Claims Act, Anti-Kickback Statute, and Stark Law. Augmenting these efforts should be an extensive educational program designed to ensure that such changes are understood and observed. The severity of fines imposed by the HHS Office of Inspector General (OIG) should be commensurate with the seriousness of the violation and consistent for information developers as well as providers. In the extreme case, the penalties should include MU Program product decertification—a “nuclear option” with consequences on providers who use decertified products.

4. Reporting mechanisms should account for provider and patient reports of electronic health record transmission errors. This will help to ensure that technologies are continuously improving, establishing an ongoing process by which errors may be addressed and lessons learned and applied collectively.\(^2\)

These changes are achievable and realistic, and will help realize a better framework for technology development.

B. CLARIFYING REGULATORY PARAMETERS

Congress should pass new laws designed to eliminate ambiguities regarding the regulatory status of health IT data and software. Providing a clear and predictable regulatory landscape in the health care marketplace will promote innovative use of current health care data for value discovery and clinical advances, thus improving care and lowering costs.

The solution to addressing regulatory ambiguities rests in specifying through legislation what should and should not be regulated by the FDA based on each product’s specific intended use and its potential harm to patients. The new system should also allow the FDA to bring products back within its regulatory jurisdiction if there is potential for patient harm. This system must protect patients, yet be clear to innovators and flexible enough to accommodate future technologies.

Any legislation setting the parameters of FDA’s regulatory jurisdiction should be cognizant of the speed at which new devices and technologies develop. Further, the growth of health IT has demonstrated that medical care is both participatory and personalized, important characteristics that must be carefully considered when developing a framework. Therefore, legislative policy should focus on a health technology’s intended outcome as well as that outcome’s implications for patients.

Greater clarity regarding the FDA’s role in regulating health IT is essential to ensuring that patients can benefit from the health IT revolution and allow agencies to focus their limited resources, staff, and expertise in assuring the safety of new medical technologies that pose the highest potential risk to patients. Establishing this risk-based framework for the regulation of health IT will protect patient safety, provide regulatory certainty, and promote innovation, which will ultimately improve care and lower costs.
III. CONCLUSION

Ten years ago, only a special few imagined the revolution that would overtake the world with the introduction of smartphones, the powerful, digitally connected computers that almost everyone carries in his or her pocket. The sophistication and convenience of technology in the hands of today’s teenagers is vastly greater than anything governments had at their disposal just two decades ago. Nor is there reason to believe that the IT revolution will do anything but accelerate. The medical industry—with its expensive, labor-intensive ways—stands increasingly at odds with the technical society that supports it. This seemingly stubborn resistance to change is the byproduct of rules that hardwire old ways of operating to developing innovations in the IT architecture.

It is therefore all the more urgent that medicine be cured, not with more bludgeoning or bribing, but by opening new horizons.

The technologies are at hand to vastly improve the value of care, and they are accessible through regulatory changes that promote rather than inhibit the development of health IT. Removing the roadblocks to a fully interoperable health IT state will allow medicine to innovate and mature much as the internet has—using data and consumer preference to determine what comes next.

Updating health IT laws and programs and also adding new enforcement mechanisms will create the united effect of augmenting the data sharing process, thus creating a more health IT friendly environment. This in turn will allow for the collective endeavor of determining the best means and measures for delivering health care when assessing outcomes. This group determination, which will be ongoing and continuously improving through the reporting mechanisms outlined above, will ease the transition for providers to turn to an outcome-based payment model while also benefiting the population as a whole.

Congress and regulators should act on these improvements with haste.
The conference was held on December 7, 2015 at MATTER in Chicago, Illinois. The conference brought together leading policy insiders, experts, and stakeholders exploring the intersection of a rapidly expanding market of data and analytics solutions that support health care, engagement, research, and government policy.


See also Summary of the HIPAA Privacy Rule, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (explaining the Privacy Rule’s minimum necessary disclosure requirement).

45 C.F.R. § 164.502(b), 164.514(d) (2016).

See also Summary of the HIPAA Privacy Rule, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (explaining the Privacy Rule’s minimum necessary disclosure requirement).

45 C.F.R. § 164.502(b), 164.514(d) (2016).


President’s Council of Advisors on Science and Technology (PCAST) Report to the President, Big Data & Privacy: A Technological Perspective, 38 (2014).


Id.

See generally, Proposed Strategy and Recommendation for a Risk-Based Framework, FOOD AND DRUG ADMINISTRATION HEALTH IT REPORT (FDASIA) (Apr. 2014) (stating that the U.S. Food and Drug Administration does not intend to regulate low-risk software).

A medical “device” is, “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man . . . .” FEDERAL FOOD, DRUG, AND COSMETIC ACT (FDCA) § 201(h) (2013), 21 U.S.C. § 321(h) (2012).


42 U.S.C. § 1320a-7b(b) (2012).


These provisions have already been considered in the 21st Century Cures Act as well as the Senate’s Health IT bill.
ACKNOWLEDGMENTS

From Meaningful Use to Meaningful Uses: Getting the Most from Meaningful Patterns in Data to Improve Health is a white paper written by Health IT Now and Apervita based on findings by participants at a conference held in Chicago, Illinois in December 2015. Both organizations would like to thank Reese S. Kim and Paul Hewitt, the leading authors of this white paper, as well as those conference participants who took the time to read and comment on the paper’s drafts. Furthermore, we would like to thank emids, JEN Associations, and MATTER for their support of the conference.

ABOUT HEALTH IT NOW

Health IT Now is a broad-based coalition of patient groups, provider organizations, employers, and payers that support incentives to deploy health information technology to improve quality, outcomes, and patient safety and to lower costs. For more information, please go to www.healthitnow.org.

ABOUT APERVITA

Apervita is the new platform and marketplace for health analytics and data. With the Apervita platform, enterprises can quickly create, distribute and scale analytics across entire organizations and teams. The Apervita marketplace allows health enterprises to publish and subscribe to health analytics and data from world-leading institutions. Its foundations have been built on a powerful, yet simple goal: the democratization of health analytics. Learn more at www.apervita.com.