Jeffrey P. Brown, Esq., CIPP/US
Counsel
Data Ethics, Policy, & Privacy
120 Fifth Avenue Place
Suite 2114
Pittsburgh, PA 15222
(412)544-8751

November 6, 2018

VIA ELECTRONIC SUBMISSION to privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
ATTN: Privacy RFC
Washington, D.C. 20230

RE: Developing the Administration's Approach to Consumer Privacy
Federal Register Docket No. 180821780-8780-01

To Whom It May Concern:

The Highmark Health organization has a diversified portfolio of businesses with more than 40,000 employees. Highmark Health is an integrated healthcare delivery and financing network headquartered in Pittsburgh, Pennsylvania. Our enterprise is comprised of an integrated health system (Allegheny Health Network), an insurance business (Highmark Inc.), a technology business (HM Health Solutions), and various diversified subsidiaries offering dental, vision, and stop-loss coverage and/or products. At Highmark Health, our mantra is "the customer is at the center of everything we do," and we feel our organization is uniquely positioned to act as an agent of change for the benefit of all of our stakeholders. Our robust enterprise privacy and data ethics program reflects our commitment to safeguarding information while enabling our workforce to use data to enhance, enrich, and improve our customers' lives.

We appreciate the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) request for public comments on "Developing the Administration's Approach to Consumer Privacy," captioned fully above.

Our response addresses two themes: i) NTIA's set of espoused consumer-focused privacy outcomes and ii) NTIA's proposed outlines of the ecosystem designed to enable privacy outcomes. We note references to "Sellers" are meant to denote organizations in a communal sense when offering products and/or services to consumers and collecting, using, and disclosing personal information.

Many of our responses are currently part of the Highmark Health philosophy, as we view ourselves as a progressive organization which leads by example. Of note, we are proffering inclusion of another consumer-centric theme – Ethics – as described more fully below. Our

comments around ethics are presented discretely for the sake of focusing thought; however, it is our firm belief that ethics is an essential element, which should be interlaced throughout other values and goals underpinning consumer-centric policy. As a healthcare organization, Highmark Health is dedicated to using data in responsible and transformative ways to advance the healthcare experience for our customers and all of the stakeholder communities we serve. Establishing and maintaining a culture of ethics is a linchpin in guiding our efforts.

We believe 'personal information' should be very clearly defined by NTIA. Presently, there is disparity among federal, state, and international legal and regulatory schemes regarding the types of information subject to protection. In the U.S. sectoral privacy model, information subject to protection tends to be industry-specific, such as healthcare-related (e.g., HIPAA), finance-related (e.g., FCRA), education-related (FERPA), etc. By contrast, in the prevailing European privacy model under the European Union's General Data Protection Regulation (GDPR), information subject to protection is defined by whether it can be linked to a natural person, irrespective of industry. Precisely defining 'personal information' under the proposed framework will be critical for setting federal policy so Sellers can anticipate whether this framework will mimic the current U.S. sectoral privacy approach, or instead pivot toward the more consumer-centric European privacy approach.

I. PRIVACY OUTCOMES[1]

1. Transparency

We agree transparency is a central component to any consumer-centric privacy framework/program. Contemporary privacy policies or notices tend to be written in 'legalese' or are either too dense or too vague to convey meaningful information to end users. Sellers should strive to provide consumers with clear and concise descriptions of their information collection, use, and disclosure practices. Additionally, Sellers should endeavor to regularly update their privacy policies or notices to account for new technologies, methodologies, or other material changes in business direction which affect how consumer information is managed and utilized to make decisions.

This is not to suggest consumers should/must be privy to all of the inner workings of a company, but privacy policies or notices should be representative of collective practices so consumers can make informed choices about providing their information to Sellers. If Sellers hope to earn and maintain consumer trust, they should be keenly transparent as a matter of belief. By requiring privacy policies or notices to contain a uniform set of criteria (similar to the mandatory components of a HIPAA-compliant Authorization), NTIA can move toward achieving this principle.

2. Control

[1] We don't have any particular issue with NTIA's classification of these themes as "privacy outcomes," however, we feel that they might be more appropriately promoted and thought of as core "principles" which drive consumer-centric privacy policy.

We agree consumers should have a qualified right to direct how Sellers collect, use, and disclose information about them – with such a right being largely context-driven and subject to appropriate/necessary limitation. As data subjects, consumers have an inherent stake in exercising some degree of autonomy or control over their information and interactions pertaining to such information. Nevertheless, we admit it is infeasible for individuals to exert dominion over all data which has been collected about them, or all inferences which have been drawn as a result; such a right would be seemingly impossible to effectuate in the complex and inter-connected digital age in which we live. In seeking to strike a balance, offering choice is arguably the most actionable way to empower consumers with a qualified right to ensure their information is subject to control.

By employing techniques such as opt-ins or opt-outs for processes commonly viewed as more sensitive on a sliding scale, such as automated-decision making or other algorithmic-based value judgments, Sellers can offer consumers an opportunity to make an informed decision and exercise structured governance over their information. Choice should be offered in contexts where a reasonable person would expect to have an opportunity to agree or object, and Sellers should endeavor to explore myriad consumer-friendly ways to integrate mechanisms of choice into their products and/or services. We believe offering choice should not simply be a byproduct of a legal requirement, but rather, a byproduct of a culture truly consumer-centric.

We recognize Sellers also have a legitimate interest in needing flexibility to utilize consumer information as necessary to conduct business. Additionally, there are legal requirements imposed upon Sellers to maintain data in a certain manner or for a prescribed timeframe. As alluded to above, consumers should not be able to wholly dictate how Sellers utilize information in the course of engaging in a wide range of business activities, nor should consumers be able to exert limitless command over information if Sellers have independent legal requirements to maintain that information. This comports with HIPAA's right to request a restriction on use/disclosure, which can be denied in circumstances where granting a restriction would render Sellers unable to functionally perform a sanctioned task. By requiring Sellers to allow consumers to exercise reasonable governance over information in contexts where choice is a reasonable expectation, NTIA can move toward achieving this principle.

3. Reasonable Minimization

We agree minimization across the data lifecycle should be promoted as a matter of best practice, if nothing more. The concept of data minimization comports with current legal requirements (e.g., HIPAA's minimum necessary standard) and serves to reduce risk to both consumers and Sellers. If Sellers collect, use, and disclose more information than is minimally necessary to accomplish a defined purpose, their ethos arguably shifts further from consumer-centricity and closer towards corporate agenda. In the event Sellers experience a risk episode such as a data breach or ransomware: the greater the pool of information available to compromise, the greater the potential for negative scope/impact.

We acknowledge attempting to define what constitutes 'minimum necessary' can be arduous and opaque at times, especially as new data consumption pathways are explored. We do not suggest Sellers should holistically flatten their data repositories or processes, but rather review a sampling of their practices in current state and deliberate what might be extraneous, and thereafter develop action plans to implement data minimization moving forward. By establishing some elastic indicators of what data is typically considered minimum necessary – or, alternatively, what data is typically considered more than minimum necessary (e.g., full SSN) – for a particular industry or routine business process, NTIA can move toward achieving this principle.

4. Security

We agree Sellers should employ a wide range of measures designed to safeguard information which is entrusted to them. Security controls should not only provide technical protection, but should also promote a culture of responsibility. We acknowledge no two companies are the same, and those with comparatively greater size/sophistication are often subject to heightened scrutiny or expectation by regulators. This is on par with the HIPAA Security Rule, which mandates 'reasonable' safeguards to account for disparities across different environments. That being said, certain threshold requirements should be established such that consumers can feel confident that their data is being properly handled, whether under the custody of a small start-up Seller or a multi-national Seller.

Security programs should be routinely assessed and enhanced, and open to 3rd party audit or validation in an effort to ensure best practices are being followed and the growing sea of threats is being sufficiently combated. Building robust controls around data should be viewed as a foundational cost of doing business, and promoting responsibility should be built into all security blueprints. By providing resources and guidance to Sellers for creating or maintaining a top-tier security program, NTIA can move toward achieving this principle.

5. Access and Correction

Similar to a right to control, we agree consumers should have a qualified right to access and correct personal information which has been provided to or gathered by Sellers. We do not dispute individuals should generally have structured access to review the set(s) of information pertaining to them and the opportunity to correct any identified inaccuracies or inconsistencies. Nevertheless, there may be times when access would pose a risk of harm to the individual or to a 3rd party (e.g., in the behavioral healthcare setting), or when amending information would be inappropriate (e.g., where the information has been deemed to be accurate and complete). In these instances, there are legitimate reasons for denying access to information or denying requests to correct information – such as protecting individual or public safety, or recognizing/endorsing the judgment of trained professionals. This comports with HIPAA, which provides rights of access and amendment subject to certain constraints. By continuing to mimic this balanced approach, NTIA can move toward achieving this principle.

We do not agree with a right to deletion of information. While we can appreciate the autonomy of individuals, there are legal requirements imposed upon Sellers to maintain information – arguably aimed at protecting individuals – and a right to deletion is contrary to compliance obligations. Sellers also often maintain records for historical/audit/quality improvement purposes, and if a right to deletion were formally codified, this could undercut legitimate interests of Sellers. We are aware the GDPR under the European privacy model does contain a right to erasure, but given the GDPR's nascent existence, there is not much guidance or precedent regarding how this individual right will be interpreted or effectuated; thus, we are not in a position to support it at this time.

6. Risk Management

We agree risk management is a critical discipline for Sellers to practice. Amidst the growing trend of cyber threats, fraudulent schemes, etc., Sellers should invest significant capital in measures designed to detect vulnerabilities at an early stage, and thereafter establish far-reaching mitigation and remediation strategies to avoid or minimize negative consequence to data. Risk management serves to assuage consumers by ensuring them Sellers have taken a comprehensive approach to evaluating concerns, allocating resources accordingly, and practicing preparedness.

Risk Management should be an ongoing function that seeks to stay ahead of new twists and turns on a changing data-fueled landscape. Effective risk management should consider not just external actors and threats, but whether a Seller's own data collection, use, or disclosure activities might lead to harmful effects upon consumers. By providing resources and guidance to Sellers for creating or maintaining an impactful risk management program, NTIA can move toward achieving this principle.

7. Accountability

We agree Sellers should be held accountable for data collection, use, and disclosure activities. Trust and accountability go hand-in-hand: consumers expect accountability in exchange for placing their trust in Sellers. In the aftermath of events like the Facebook/Cambridge Analytica scandal, accountability is a hallmark consumers deserve and demand. In the digital age where data has become an indispensable commodity to many Sellers, enhanced controls are needed to ensure consumers behind the data – or oversight agencies charged with protecting the public – can hold Sellers accountable for activities which undermine trust. We further agree agents/subcontractors of Sellers should also be accountable as downstream entities interacting with consumer information, and it should be incumbent upon Sellers to conduct meaningful due diligence upon their agents/subcontractors prior to providing data to them.

The nexus of accountability comports with HIPAA's requirements regarding flow-down of contractual terms/conditions between business associates and sub-business associates. By establishing a legal agency model and requiring minimum controls are pushed from Sellers to agents/subcontractors such that both entities are accountable for their actions or inactions, NTIA can move toward achieving this principle. The principle of accountability is also a constituent part of data ethics and undergirds responsible data management.

8. Ethics

As referenced above, ethics is a cornerstone for achieving consumer-centric privacy policy. In a data-driven society, Sellers needs to increasingly look within to examine how and why data is used. Data should exist to serve people; collective thought needs to shift away from using data because it is an allowable thing to do, and toward using data because it is the *right* thing to do. Ethical deliberation is an indispensable stride on the path to consumer-centricity, and Highmark Health has committed itself to practicing principled reflection in our efforts to use data in trusted and innovative ways to serve our customers and forge the future of healthcare.

Creating and adhering to a framework for data ethics includes establishing ethical principles which enable not only responsible data access, use, and disclosure, but ensure respect for the person behind the data is maintained at all times. Applying principles of ethics helps to assure decisions rendered are legal as well as just, and also helps to avoid making discriminatory or erroneous inferential decisions.

II. GOALS FOR FEDERAL ACTION

1. Harmonize the regulatory landscape

We agree harmonizing the regulatory landscape is both necessary and long overdue. While the U.S. sectoral privacy model has prevailed to date, and admittedly offers focused protections to consumers, the innate disparity of a sectoral regulatory framework creates uncertainty, inconsistency, and at times, undue burden. Many laws have not been meaningfully updated in decades and are too rigid to support the realities of modernization; they still rest upon consent-based schemes cutting against pro-consumer concepts and modalities, such as interoperable medical record systems. Existing laws have not caught up to reflect the day-to-day workings of a contemporary complex society and they inhibit data use and exchange to the detriment of both consumers and Sellers.

We support comprehensive federal privacy legislation which pre-empts state law, affords broad and uniform rights regardless of industry, location, or other patchwork factors, and makes genuine attempts to align with foreign privacy models in furtherance of recognizing and facilitating an increasingly trans-border consumer existence/experience.

2. Legal clarity while maintaining the flexibility to innovate

We agree legal clarity is desirable for setting objective markers and providing instructive guidance to consumers and Sellers. We also agree having the flexibility to gather and use data in novel ways is crucial to allow Sellers to test and deliver products and/or services which amplify a consumer-centric agenda. The challenge in reconciling these objectives is that bright line standards tend to address historical or current state, but do not always lend themselves well to anticipation or adaptation as society continually evolves.

Our recommendation would be to strive to legislate in a manner that establishes a floor of rules or requirements based upon shared expectation and experience, but leave enough room for Sellers to operate within shades of gray in sincere endeavors to innovate. We are not suggesting Sellers have free rein to use data behind a corporate veil; but overly-legislating would stifle the flexibility needed to foster innovation. By establishing threshold guardrails while still allowing Sellers to explore new edges – guided particularly by transparency, accountability, and ethics – we are hopeful the appropriate balance can be struck to ratify the interests of both consumers and Sellers.

3. Comprehensive application

Just as we support comprehensive federal privacy legislation which is sector-agnostic, we support comprehensive application of the principles herein to shepherd the progression of consumer-centric privacy policy. So long as new technologies, programs, and methodologies are evaluated against a uniform set of consumer-centric values which are equally applied and interpreted by the appropriate oversight agenc(y)(ies), consumers and Sellers can expect balanced outcomes.

4. Employ a risk and outcome-based approach

We agree a risk and outcome-based approach can be an effective way for Sellers to establish a privacy strategy around which to build business processes and culture. By looking to context and expectation to help define the varying degrees of sensitivity of the data, the potential harm and/or benefit to consumers, and risk appetite, Sellers can make informed decisions about proposed uses and which controls to implement. This reflects the reality that not all use cases are equal, and Sellers can make judgments about which use cases may require heightened controls to mitigate heightened risk. Sellers should still be held accountable for their actions or inactions, but taking a balanced approach to privacy strategy based upon a thoughtful weighing of context-driven risks and benefits is quite reasonable and still consumer-focused, in our estimation.

In addition to considerations of risk and benefit, by applying principles of ethics to responsible data governance and data decision-making, we encourage risk/benefit models to also consider the consequences of the data use to the consumer-stakeholder who is the subject of the data. Applying a consequentialist model of data deliberation to hard or complex cases, or those with a high degree of risk to the consumer, forces users to consider the broader range of issues and may further encourage data minimization.

5. Interoperability

We agree interoperability is a key ingredient in breaking down barriers to information exchange and bolstering a framework where data serves people. Any policy aimed at achieving consumer-centricity needs to cultivate a frictionless flow of data, both domestically and across borders. Naturally there may be differences in privacy philosophy between dissimilar entities, but finding ways to bridge gaps and work together toward interoperability is a goal any entity – whether Seller or nation-state – should eagerly embrace.

6. Incentivize privacy research

We agree ongoing research into privacy methodologies and capabilities should be encouraged and incentivized. Exploring ways to augment privacy by design needs to be a continuing effort as new technologies and processes come to market. Incenting Sellers to conduct research and develop consumer-focused solutions helps to ensure they not only play a direct role in their own success, but act as stakeholders in helping to sustain consumer-centric privacy policy.

7. FTC enforcement

While we agree the FTC is certainly capable of protecting consumer privacy rights given its historical role, we would advocate for the creation of a new federal agency charged with oversight and enforcement of the comprehensive federal privacy legislation (and attendant regulations) we alluded to above. The FTC has done a commendable job to date in defending the public against unfair and deceptive acts or practices, but vesting authority in an emergent supervisory body to regulate Sellers' use of data and educate market participants on data management writ large would be appropriate to signify the importance of a new framework and the commitment to ensuring focused action – similar to the conception of the Consumer Financial Protection Bureau in the aftermath of the 2008 financial crisis.

8. Scalability

We agree scalability is of paramount importance; treating disparate Sellers according to the scale of their resources and the scope of their activity is a fair method of regulating. Similar to how Sellers can employ a risk and outcomes-based approach to implementing a privacy program, the appropriate oversight bod(y)(ies) can employ a scale and scope approach to hold Sellers accountable when auditing and enforcing compliance with a consumer-centric privacy framework.

We thank NTIA for the opportunity to provide comments on this very important topic and look forward to working with NTIA in the future. We welcome any additional questions you may have and are open to further discussion. You may contact Jeffrey Brown, Privacy Counsel, at jeffrey.brown@highmarkhealth.org, or Lisa Martinelli, Chief Privacy & Data Ethics Officer, at lisa.martinelli@highmarkhealth.org.

Respectfully,

Jeffrey P. Brown, Esq., CIPP/US
Counsel
Data Ethics, Policy, & Privacy
Highmark Health