From: Peter Acton <pacton@athenahealth.com>
Sent: Thursday, October 24, 2019 4:24 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Karinna Allen <kaallen@athenahealth.com>; Michael Samarel <msamarel@athenahealth.com>; Andrea Bilbija <abilbija@athenahealth.com>; Taylor Lehmann <tlehmann@athenahealth.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Attached are athenahealth, Inc.'s comments to the NIST Privacy Framework Preliminary Draft. Please contact me if you have any questions.

Thank you.

Peter Acton

Chief Compliance Officer

311 Arsenal Street | Watertown, MA 02472

o: 617.402.6182

c: 978.463.3198

NIST Privacy Framework: Preliminary Draft Comments
Organization Name: athenahealth, Inc.
Submitted electronically by: Peter Acton, pacton@athenahealth.com

Comment #	Page #	Line # / Row #	Section	Comment	Suggested Change	Type of Change
1	23	R30	GV.PP-P5	The athenahealth, Inc. (Athena) platform, service offerings, and contractual relationships with provider customers grant access to consumer and patient data; however, Athena has no direct relationship or interaction with those patients. The only means by which to communicate (and honor) patient preferences with respect to management of their data is through the provider/customers, and for Athena to assume those responsibilities directly is not practical. Moreover, data entered into a customer's instance of the Athena solution is, by contract, owned by the respective customer and there are explicit restrictions and limitations on what Athena can do to (or with) that data absent direction and authorization from the customer. That is, Athena is contractually prohibited in certain situations from taking directions from patients with respect to the handling of that patient data unless independently authorized by the customer. The current draft of the framework is not structured in a way that clearly accounts for these distinctions, and how Athena should define/consider "data ownership" in the context of NIST as compared to that of its existing contractual relationships.	We suggest clarification on how "data ownership," as defined, impacts compliance by a data processor within the NIST framework while simultaneously permitting compliance with contractual obligations to data owners.	General
	23	R31	GV.PP-P6			
	24	R45	GV.MT-P7			
	24	R48	CT.PO-P3			
	26	R66	CM.AW-P1			
2	10; 14	339; 486	2.1; 3.3	As an entity operating in the healthcare industry, much of the data collected by Athena is subject to regulatory requirements that dictate how that data should be secured and protected (e.g., PHI). With respect to the Identification-P component of the NIST framework, organizations like Athena need to be able to categorize their data in a way that separates higher risk data (i.e., regulated data) from other data types. This type of data categorization will likely drive the analysis of additional privacy framework factors (e.g., the identification of problematic data actions will vary based on whether the data in question is highly regulated, such as health data, or is less regulated, such as marketing data). We would expect that such categorization be permissible, and that it can be driven by the regulatory environment.	We would suggest more explicit language that acknowledges and accounts for the need for data categorization based on regulatory requirements. This would inherently allow businesses to account for higher risk data elements (e.g., health data).	Editorial
	21	R1	ID.IM-P1			
	21	R4	ID.IM-P4			
	21	R5	ID.IM-P5			
	22	R12	ID.RA-P1			
3	25	R60	CT.DP-P3	Requiring that data is processed to limit the identification of inferences about individuals' behavior or activities is unduly restrictive for the majority of data categories. Such practices are commonplace for advertising across industries. While it makes sense to have a clear methodology surrounding appropriate management of data and consumer transparency, including acknowledgement of behavioral advertising practices, to substantially limit a company's ability to form meaningful inferences about their consumer base can negatively impact a company's business, including its ability to interact with consumers to their benefit. For example, one of the main purposes of the several population health initiatives by the government within the healthcare industry is to utilize data to make assumptions that improve the health profiles of a broad community base. As drafted, section CT.DP-P3 would restrict the potential effectiveness of such initiatives.	We would suggest that such limitations on inferences, should they exist in the framework, be focused on higher risk data categorizations, such as PHI, and inferences made related to marketing activities specifically. Such a change aligns with the current regulatory environment and would not unnecessarily limit standard business practices. We would further suggest that NIST consider a focus on requiring entities to be transparent to their consumer base about inferences they may make, and any behavioral advertising practices the entity engages in, rather than forcing entities to restrict the formulation of inferences entirely.	Editorial
4	25	R63	CT.DP-P6	Athena would request clarity surrounding how an entity would be expected to limit data processing to only that which is relevant and necessary for the service to meet its mission and/or business objectives. Assuming that this can be determined by the entity, we expect that such objectives will be crafted broadly causing section CT.DP-P6 to have no meaningful impact. The section also provides no clear guidance for entities like Athena that receive and process data on behalf of customers and cannot make determinations as to what underlying data is or is not relevant for those customers to meet their business objectives.	Suggested change is included in our comment.	Editorial
5	26	R69	CM.AW-P4	For the Data Processing Awareness category, Athena would request additional clarity around the definition of a data disclosure as included in section CM.AW-P4 of the proposed framework. If a disclosure is equivalent to every "touch", tracking will become unduly burdensome and ultimately not meaningful to the consumer. We would request the same clarity around the definition data provenance in section CM.AW-P6 of the proposed framework.	Suggested change is included in our comment.	Editorial

NIST Privacy Framework: Preliminary Draft Comments
Organization Name: athenahealth, Inc.
Submitted electronically by: Peter Acton, pacton@athenahealth.com

	26	R71	CM.AW-P6	Would NIST consider that to be the entity that provided Athena the data, or require a broader lookback window?		
6	22	R13	ID.RA-P2	Athena would request additional clarity on what "evaluation bias" is meant to include.	Suggested change is included in our comment.	General
7	28	R108	PR.PT-P2	Athena would request additional clarity on what is meant by "principle of least functionality."	Suggested change is included in our comment.	General