

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

MILLIMAN, INC., MILLIMAN	)	
SOLUTIONS, LLC, and VIGILYTICS	)	
LLC,	)	
	)	
Plaintiffs,	)	
	)	Civil Action No. 1:21-cv-10865-NMG
vs.	)	
	)	
GRADIENT A.I. CORP., STANFORD A.	)	
SMITH, and SAMUEL CHASE PETTUS,	)	
	)	
Defendants.	)	
	)	

PLAINTIFFS' OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. BACKGROUND	2
A. Solution Provided by the Asserted Patents	2
B. Prosecution Histories	7
III. LEGAL STANDARDS	7
A. Claim Construction	7
B. Indefiniteness	8
IV. THE DISPUTED CLAIM TERMS	9
A. “token”	9
B. “server”	11
C. “encryption server”	12
D. “similarly encrypted”	14
E. “medical information that characterizes a group”	17
F. “absent authorization” terms	19
V. CONCLUSION.....	20

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>3-D Matrix, Inc. v. Menicon Co.</i> , Case No. 14-cv-10205-IT, 2016 WL 111410 (D. Mass. Jan. 11, 2016) (Talwani, J.)	16
<i>Abbott Labs. v. Sandoz, Inc.</i> , 544 F.3d 1341 (Fed. Cir. 2008).....	10
<i>Amax, Inc. v. ACCO Brands Corp.</i> , 282 F.Supp.3d 432 (D. Mass. 2017)	16
<i>BASF Corp. v. Johnson Matthey Inc.</i> , 875 F.3d 1360 (Fed. Cir. 2017).....	8
<i>Bayer Healthcare LLC v. Baxalta Inc.</i> , 989 F.3d 964 (Fed. Cir. 2021).....	8
<i>DuraSystems Barrier Inc. v. Van-Packer Co.</i> , Case No. 1:19-cv-01388, 2021 WL 4037826 (C.D. Ill. Sept. 3, 2021)	16
<i>Hill-Rom Servs., Inc. v. Stryker Corp.</i> , 755 F.3d 1367 (Fed. Cir. 2014).....	18
<i>Koninklijke Philips Elecs. N.V. v. Zoll Medical Corp.</i> , 914 F.Supp.2d 89 (D. Mass. 2012)	16
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	8
<i>Pacing Tech., LLC v. Garmin Int'l, Inc.</i> , 977 F.Supp.2d 1013 (S.D. Cal. 2015).....	12
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (<i>en banc</i>)	7, 8
<i>Summit 6, LLC v. Samsung Elecs. Co.</i> , 802 F.3d 1283 (Fed. Cir. 2015).....	8, 17
<i>Teva Pharm. USA, Inc. v. Sandoz, Inc.</i> , 574 U.S. 318 (2015).....	7
<i>Thorner v. Sony Comput. Ent. Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012).....	8

<i>Verizon Services Corp. v. Vonage Holdings Corp.</i> , 503 F.3d 1295 (Fed. Cir. 2007).....	12
<i>Zapmedia Services, Inc. v. Apple Inc.</i> , Case No. 2:08-cv-104, 2010 WL 8599970 (E.D. Tex. Aug. 19, 2010).....	12

LIST OF EXHIBITS

- Exhibit 1: Declaration of Dr. Aviel D. Rubin
- Exhibit 2: Excerpts from file history of U.S. Patent 9,665,685
- Exhibit 3: Excerpts from file history of U.S. Patent 10,109,375
- Exhibit 4: Excerpts from file history of U.S. Patent 10,886,012
- Exhibit 5: Excerpts from file history of U.S. Patent 9,323,892
- Exhibit 6: Excerpts from Webster's New World Computer Dictionary, 10th ed., Wiley Publishing, Inc., 2003
- Exhibit 7: Excerpts from Dictionary of Computing, 4th ed., Oxford University Press, 1996
- Exhibit 8: Excerpts from Microsoft Computer Dictionary, 5th ed., Microsoft Press, 2002
- Exhibit 9: Excerpts from Merriam-Webster's Collegiate Dictionary, 10th ed., Merriam-Webster, Inc., 1999
- Exhibit 10: Excerpts from The New Oxford American Dictionary, Oxford University Press, 2001
- Exhibit 11: Excerpts from Random House Webster's College Dictionary, Random House, Inc., 1999

I. INTRODUCTION

Plaintiffs Milliman, Inc., Milliman Solutions, LLC and Vigilytics LLC (“Plaintiffs”) submit this Opening Claim Construction Brief setting forth the proper construction of the disputed terms of the “Asserted Patents,” namely U.S. Patent No. 9,118,641 (the “’641 Patent”); U.S. Patent No. 9,323,892 (the “’892 Patent”); U.S. Patent No. 9,665,685 (the “’685 Patent”); U.S. Patent No. 9,965,651 (the “’651 Patent”); U.S. Patent No. 10,109,375 (the “’375 Patent”); and U.S. Patent No. 10,886,012 (1-6, the “’012 Patent”). Dkt. 1-1 to 1.6. The “Asserted Claims” are:¹

’641 Patent:	Claims 7, 8, 9, 12, 13
’892 Patent:	Claims 11, 13, 14, 18
’685 Patent:	Claims 7, 8, 9, 11, 13
’651 Patent:	Claims 7, 8, 9, 11, 13
’375 Patent:	Claims 7, 8, 9, 11, 13
’012 Patent:	Claims 7, 8, 10, 12

The Joint Claim Construction Statement (“JCCS”) identified six terms for construction. Dkt. 98 at Ex. A. Plaintiffs’ constructions should be adopted because they are faithful to the intrinsic evidence, particularly the text of the claims and the Asserted Patents’ specifications. Defendants’ constructions should be rejected because: (i) Defendants proposed “ordinary meaning” constructions for claim terms that have multiple, vastly different, inapplicable ordinary meanings; and (ii) Defendants’ other proposed constructions are inconsistent with the intrinsic evidence.

Plaintiffs’ proposed constructions are supported by a declaration from Prof. Aviel Rubin (hereinafter, “Ex. 1”), a Professor of Computer Science at Johns Hopkins University whose primary research area is computer security, with a focus on security for healthcare IT systems. Ex. 1, ¶¶ 2.1-2.3. Prof. Rubin is knowledgeable about the skill level of a “person having ordinary skill

¹ Plaintiffs reserve the right to identify additional asserted claims as discovery is pending and Defendants have not satisfied their LR 16.6 disclosure obligations. *See e.g.*, Plaintiffs pending Motion to Compel, Dkt. 85.

in the art” (hereinafter, “POSITA”) in the field of the Asserted Patents as of their priority dates. *Id.*, ¶ 4.20. Prof. Rubin’s declaration provides evidence of how a POSITA would interpret the disputed claim terms.

II. BACKGROUND

A. Solution Provided by the Asserted Patents

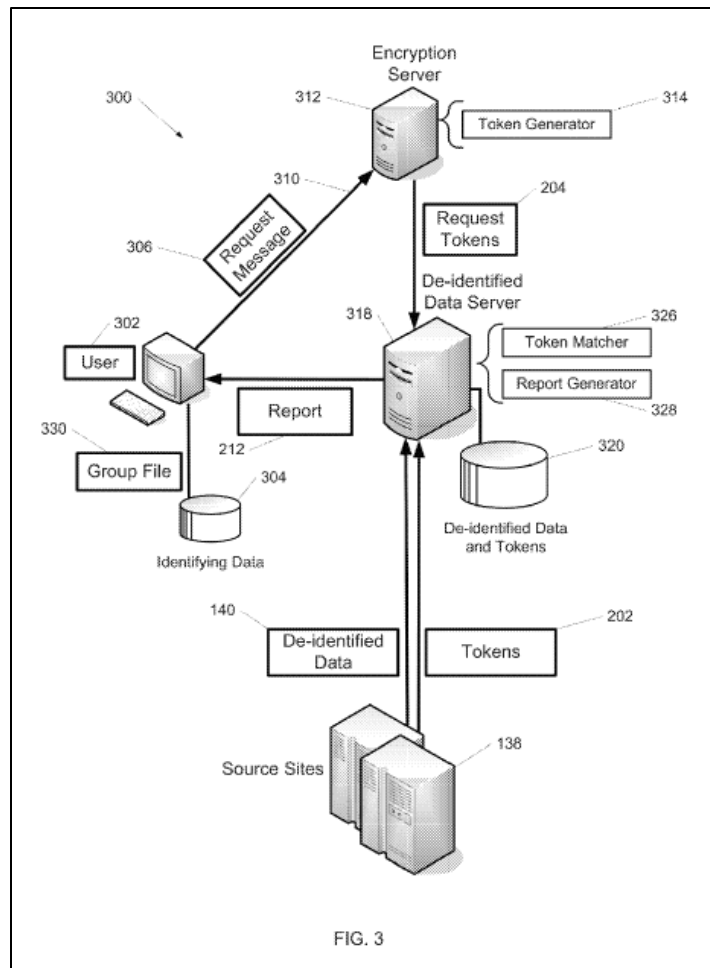
The Asserted Patents explain that health insurers previously lacked sufficient access to protected health information (“PHI”) stored by healthcare providers, such as pharmacies or hospitals, for individuals in small and midsize groups (containing 10-1000 individuals). Ex. 1, ¶ 4.1; ’641 Patent, 1:14-36. PHI for members in these groups, such as “Jack” and his dependents, could be used by health insurers to better understand and assess the risks associated with these groups and to appropriately price premiums for the associated future cost of providing health insurance to the group. Ex. 1, ¶ 4.1; ’641 Patent, 4:4-24. Jack’s PHI was previously inaccessible as a practical matter because “[f]ederal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), protect the disclosure of PHI regarding the health and medical treatment of an individual (e.g., Jack) by prohibiting the health providers, known as source sites possessing Jack’s PHI, from releasing it to third parties without Jack’s permission. Under HIPAA, the source sites can release only irreversibly de-identified data without Jack’s permission.” Ex. 1, ¶ 4.1; ’641 Patent, 3:65-4:3 (reference numbers omitted).

A health insurer “may be interested in the medical history information contained in Jack’s PHI” because “Jack’s employer may like to buy a group health insurance policy for the group made up of Jack and his coworkers” and “the insurer would like to use the medical history from the group to assess the risk of claims and set the group health insurance premium appropriately. Unfortunately, the group may also be too large for the insurance company to practically obtain permission from each person in the group, without which HIPAA prohibits the healthcare

providers from releasing the PHI to the insurer. The de-identified data, which the healthcare providers or other source sites could release without permission, is not useful to the insurer because the insurer has no way to know whether it corresponds to the people in the group. With no way to obtain medical history data for the group, the insurer cannot set the group insurance premium acceptably.” Ex. 1, ¶ 4.1; ’641 Patent, 4:4-24 (reference numbers omitted).

To address this conundrum, the Asserted Patents disclose specific token generation and anonymization approaches to achieve new computer capability: systems able, in response to a request for information regarding a group of individuals who have not authorized PHI disclosure, to provide to third parties, such as insurance companies, irreversibly de-identified healthcare information from which the third party may calculate an insurance premium for the group, while complying with federal privacy regulations, including HIPAA. *See e.g.*, Ex. 1, ¶ 4.2; ’641 Patent, 4:25-30.

In one example, with reference to Figure 3 of the Asserted Patents (reproduced below), a user 302, e.g., an insurer, may request de-identified data that characterizes a group of identified individuals, where the de-identified data may reflect information regarding medical claims, hospital claims, and prescription history (such as the drug categories and drug indications associated with the drugs in the de-identified data). ’641 Patent, 6:6-8; 6:59-62. In this example, the insurer (e.g., user 302) can send a request message 306 to a third party with an “encryption server” 312. Ex. 1, ¶ 4.3; ’641 Patent, 4:32-33.



The request message 306 “uniquely identifies” each individual in the group, ’641 Patent, 5:12-30, such as a group of individuals for which health insurance is sought. The third party, for example, using the “encryption server 312” generates a “request token” 204 for each individual in the group based on the personally identifiable information for each individual in the group. Ex. 1, ¶ 4.4; ’641 Patent, 4:32-35; 5:35-38. The tokens are generated from personally identifiable information of the individuals using “one or more encryption techniques,” such as a hash function. Ex. 1, ¶ 4.5; ’641 Patent, 5:54-67. That way, the personally identifiable information for an individual maps to a hash value, e.g., the token, that is associated with the individual but does not reveal the identity of the individual. Ex. 1, ¶ 4.5.

The encryption server can generate the request token such that the request token is

encrypted similarly to tokens 202 associated with the information to be produced. Ex. 1, ¶ 4.4; '641 Patent, 2:16-18. For example, encryption server 312 may use the same token generator as used to generate the tokens 202 stored with de-identified healthcare data 320 by de-identified data server 318; or the encryption server 312 may use any other means that generates a comparable token from the same personally identifiable information. Ex. 1, ¶ 4.4; '641 Patent, 5:44-67.

In one configuration in the Asserted Patents, the encryption server then sends the generated request tokens to the de-identified data server 318 that stores the de-identified healthcare data 320. '641 Patent, 4:35-37; 5:44-49. The de-identified data server stores irreversibly de-identified healthcare data for many individuals. The de-identified healthcare data can comprise data from source sites 138 such as pharmacies, healthcare professionals and electronic claim clearing houses. *Id.*, 5:45-49. The tokens 202 are associated with the de-identified healthcare data 140 of individuals. The tokens can correspond to persons treated by healthcare providers, none of whom need to have provided authorization to access their PHI, but the tokens do not reveal the identities of the treated individuals. Ex. 1, ¶ 4.6; '641 Patent, 4:25-32, Fig. 2.

The de-identified data server, with a token matcher 326, can find all tokens 202 in the de-identified healthcare data that match the request tokens 204 from the encryption server. Ex. 1, ¶ 4.7; '641 Patent, 4:37-41; 6:1-4. The de-identified healthcare data for the matched tokens can then be processed in a way that leaves it irreversibly de-identified, yet useful for an underwriting assessment of the group. '641 Patent, 4:37-45; 6:8-15. The de-identified data server 318 can retrieve the requested de-identified data for each of the identified individuals in the group, and provide the de-identified data associated with the group of individuals for the matched tokens in a report to the user, without revealing the protected health information of the individuals in the group and without obtaining any authorization from the individual members of the group. *Id.*, 6:62-67.

The report can also include the likelihood that individuals in the group have certain medical conditions that can be determined from the prescriptions for those persons. *Id.*, 8:17-27. The report could also include “health status information based on the prescription drug history information” and “diagnosis codes from medical claims data to assess health status.” *Id.*, 8:27-31. The recipient of the report, e.g., an insurer, can use the report “for making an immediate, informed decision about the insurance related risks” for the group. *Id.*, 8:41-43. However, the recipient of the report, e.g., the insurer which has personally identifiable information about the individuals in the group, does not have access to data associated with specific individuals. Further, “the information in the Report 212 may be processed into metrics that characterize a large group and cannot be used to infer information about individuals.” *Id.*, 4:51-54. “These features of the system maintain the privacy of the protected health information.” *Id.*, 4:59-61 (reference numbers omitted).

The Asserted Patents explain that the above-described process is not performed unless the request includes a minimum number of individuals. The minimum number, which according to the Asserted Patents could be, for example, ten, is “chosen to make it effectively impossible to associate individual group members with individual tokens in the batch of request tokens” *Id.*, 5:40-43. The limit can ensure that it is difficult to infer any association between the particular individuals and the information in the report. *Id.*, 7:11-15. Thus, some embodiments also require that a minimum number of tokens be matched. *Id.*, 7:47-55. In addition, in some embodiments, privacy-preserving rules further protect against identifying any individual member of the group. ’651 Patent, 9:7-20. For example, a privacy-preserving rule may include not allowing the same user to submit more than one request containing substantially the same identifying data during a given time period.

B. Prosecution Histories

The '641 Patent is the first of the Asserted Patents to issue. It issued on August 25, 2015. Its application was filed June 30, 2010 and it claims priority to a provisional application (Serial No. 61/222,428) filed July 1, 2009. The '375 Patent is a continuation of the '641 Patent and the '012 Patent is a continuation of the '375 Patent. The specifications of the '641, '375 and '012 Patents are practically identical.

The '892 Patent issued on April 26, 2016 from an application filed November 18, 2013. The '892 Patent is a continuation-in-part of the '641 Patent and also claims priority to a provisional application (Serial No. 61/729,207) filed November 21, 2012. The '892 Patent (and the continuations thereof, such as the '685 and '651 Patents), adds among other teachings that the de-identified healthcare data could include pre- and post-encounter details of the individuals with healthcare facilities. '892 Patent, 6:11-13. This information might be beneficial to a hospital, for example, to assess risk of re-hospitalization or other medical events. *Id.*, 4:36-46. The '685 is a continuation of the '892 Patent and the '651 Patent is a continuation of the '685 Patent. The specifications of the '892, '685 and '651 Patents are practically identical.

III. LEGAL STANDARDS

A. Claim Construction

The interpretation of a patent claim is a question of law that may involve subsidiary factual findings. *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 331-32 (2015). Claims terms generally are “given their ordinary and customary meaning,” defined as “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (*en banc*). To determine the meaning of claim terms, courts are to consider the intrinsic evidence, which includes the claims themselves, the specification and the file

histories. *Id.*, 1313-14, 1317. The Court may also consider extrinsic evidence, such as dictionaries or expert testimony, which “can be useful to a court for a variety of purposes,” such as “ensur[ing] that the court’s understanding of the technical aspects of the patent is consistent with that of a person of skill in the art.” *Id.*, 1318.

There are two exceptions to using the ordinary and customary meaning: (1) when a patentee sets out a definition and acts as his own lexicographer; and (2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution. *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). “The patentee is free to choose a broad term and expect to obtain the full scope of its plain and ordinary meaning unless the patentee explicitly redefines the term or disavows its full scope” in a “clear and unmistakable” manner. *Id.* at 1367. Courts “do not read limitations from the specification into claims,” even if “the only embodiments, or all of the embodiments, contain a particular limitation.” *Id.* at 1366.

The Federal Circuit has confirmed that courts need not construe limitations consisting of commonly used terms. *See, e.g. Summit 6, LLC v. Samsung Elecs. Co.*, 802 F.3d 1283, 1291 (Fed. Cir. 2015) (“being provided to”); *Bayer Healthcare LLC v. Baxalta Inc.*, 989 F.3d 964, 977–78 (Fed. Cir. 2021) (“random”).

B. Indefiniteness

The definiteness requirement of 35 U.S.C. § 112(b) requires that a patent’s claims, when read in light of the specification and the prosecution history, “inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). This standard “mandates clarity, while recognizing that absolute precision is unattainable.” *Id.* at 910. The party asserting indefiniteness bears the burden of proving indefiniteness by clear and convincing evidence. *BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1365 (Fed. Cir. 2017).

IV. THE DISPUTED CLAIM TERMS

A. “token”

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“token”	’641 Patent, claim 7 ’892 Patent, claim 11 ’685 Patent, claim 7 ’651 Patent, claim 7 ’375 Patent, claim 7 ’012 Patent, claim 7	An identifier associated with an individual that does not reveal the identity of the individual.	Ordinary meaning

Plaintiffs’ construction should be adopted because it is faithful to the intrinsic evidence. Defendant’s position should be rejected because “token” has divergent ordinary meanings, some of which are inconsistent with the tokens described in the Asserted Patents. For this reason, adopting an “ordinary meaning” construction proposed by Defendants is likely to confuse factfinders.

The claims explicitly state that a “token” is associated with an individual yet does not reveal the identity of the individual. Claim 7 of the ’641 Patent states that a token is produced “for each individual in a group...,” thereby linking tokens to individuals. Claim 7 further states that “the identity of the individuals in the group is unattainable from the tokens...” *See also* ’892 Patent, claim 11 (similar). This means that the token does not reveal the identity of the individual; the identity of the individual is “unattainable” from the token.

The other intrinsic evidence confirms that a token is data associated with an individual that does not reveal the identity of the individual. The patents’ specifications explicitly state that the tokens “correspond to persons” and “uniquely identify each person in the group.” ’641 Patent, 4:30-31, 7:20-21; ’892 Patent, 4:65-66, 8:15-16. Each token is data associated with a particular individual because it is generated from personally identifiable information about the individual. ’641 Patent, 1:52-54 (producing a token “for each individual may include encrypting respective

data that identifies each individual”); 5:35-38 (a token is generated for an individual “by applying a token generator 314 that encrypts the personally identifiable information of each group member”); 5:50-53 (token generated from “personally identifiable information”); 5:60-61 (similar); 7:15-18 (tokens are produced “from the identifying data of each person”). For example, the patents explain that a social security number could be the personally identifiable information and that a hash function could be used to generate the tokens. ’641 Patent, 5:25, 5:66-67. A person skilled in the art of the Asserted Patents would know that a hash function could generate a value (called a “token” in the Asserted Patents) from an individual’s personally identifiable information (e.g., social security number) such that the value would be associated with the individual without revealing the person’s identity. Ex. 1, ¶ 5.2. Indeed, the essence of the Asserted Patents is that the tokens have to correspond to individuals in order to perform the matching of the tokens to the individuals corresponding to the de-identified healthcare data. Ex. 1, ¶ 5.3. To that end, this Court, in its Memorandum and Order denying Defendants’ motion to dismiss, already recognized that a token “corresponds to” an individual and that “the identity of an individual is not ascertainable from the corresponding token.” Dkt. 43 (March 11, 2022) at 3.²

In contrast, the Court should reject Defendant’s “ordinary meaning” construction because “token” has multiple ordinary meanings, including one that includes a tangible object, such as a coin. Ex. 1, ¶ 5.6; Ex. 9 at 1240; Ex. 10 at 1781; Ex. 11 at 1371. If an “ordinary meaning” construction were adopted, the factfinder may be confused as to whether the claims require tangible tokens. “‘Claim construction’ is for the purpose of explaining and defining terms in the

² The file histories’ only meaningful disclosure on the construction of the term is that in the ’685, ’375 and ’012 Patent file histories, the patent applicant confirmed that a “unique token” is “for each individual included in the group” (Ex. 2 at Mil_0001301-02; Ex. 3 at Mil_0001741 and 0001823; Ex. 4 at Mil_0002078), which supports Plaintiffs’ construction.

claims” *Abbott Labs. v. Sandoz, Inc.*, 544 F.3d 1341, 1360 (Fed. Cir. 2008). Nor does that “ordinary meaning” comport with the patent’s requirements that the tokens be associated with specific individuals without revealing those individuals’ identities.

B. “server”

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“server”	’641 Patent, claim 7 ’892 Patent, claim 11 ’375 Patent, claim 7 ’012 Patent, claim 7	A computer, with a processor and a memory, on a network that provides information in response to requests from another computer.	Ordinary meaning

The Court should adopt Plaintiffs’ proposed construction of this term, which is consistent with the patents’ intrinsic record, and reject Defendant’s “ordinary meaning” which could include definitions wholly inapplicable to this invention.

Intrinsic evidence supports Plaintiffs’ construction. The text of the claims shows that a server includes a processor and memory. Claim 7 of the ’641 Patent explicitly states that the claimed encryption server has “a processor and a memory.” Claim 11 of the ’892 Patent similarly clarifies that the claimed “encryption server” is a “*hardware* encryption server.” The “hardware” refers to a processor and a memory. Ex. 1, ¶ 5.15. Correspondingly, the specifications explain that the servers used in the token matching process, particularly the “encryption server” and the “de-identified data server,” are “computer systems” and that computer systems include a processor and memory. ’641 Patent, 8:50-56. The file histories also explain that a server has a processor. Ex. 3 at Mil_0001741 and 0001744.

Extrinsic evidence confirms that “server” is a known term in computer science, and its meaning in computer science comports with Plaintiffs’ proposed construction. In computer science, “server” means a “system on a network that provides a server to other systems connected

to the network.” Ex. 1, ¶ 5.10 (quoting, Ex. 7, The Dictionary of Computing, Oxford Univ. Press, 4th ed., 1996). Consistent with this intrinsic and extrinsic evidence, Plaintiffs’ construction should be adopted to make explicit that the “server” is a hardware device that comprises a processor and a memory.

Other courts have defined “server” similarly. In *CellTrust Corp. v. ionLake, LLC*, the court construed “server” to mean “a networked computer that manages access to a computer resource or server.” -- F.Supp.3d --, Case No. 19-cv-2855, 2022 WL 4018042, *8 (D. Minn. Sept. 2, 2022). In *Verizon Services Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1303-1305 (Fed. Cir. 2007), the Federal Circuit upheld a district court construction of “server” as “a computer system, such as one or more computers and/or devices, that provides services to other computer systems over a network.” See also *Pacing Tech., LLC v. Garmin Int’l, Inc.*, 977 F.Supp.2d 1013, 1025 (S.D. Cal. 2015) (“computer dedicated to run one or more services”); *Zapmedia Services, Inc. v. Apple Inc.*, Case No. 2:08-cv-104, 2010 WL 8599970, *3 (E.D. Tex. Aug. 19, 2010) (“one or more computers or devices on a network, with each computer or device having user account(s), server database application(s), and server application(s)”). These constructions support Plaintiffs’ construction.

Finally, Defendant’s “ordinary meaning” approach is inappropriate because “server” has meanings wholly unrelated to computers. Ex. 1, ¶ 5.18; Ex. 9 at 1070; Ex. 10 at 1558 Ex. 11 at 1199.

C. “encryption server”

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“encryption server”	’641 Patent, claim 7 ’375 Patent, claim 7 ’892 Patent, claim 11	A “server” that produces “tokens” in response a request. ³	Ordinary meaning

³ Plaintiffs propose a slight modification of their position set forth in the JCCS, which is warranted and supported by the intrinsic evidence.

All of the relevant evidence confirms that an “encryption server” as used in the Asserted Patents is a server that produces tokens in response to a request. The intrinsic evidence, including the claims themselves, fully support Plaintiffs’ construction. For example, Claim 7 of the ’641 Patent states that the “encryption server” is for “producing a token for each individual included in a group,” where the group is “composed of multiple individuals identified in a request [singular] for healthcare information that characterizes the group,” and where “the identity of the individuals in the group is unattainable [e.g., encrypted] from the tokens” ’641 Patent, 11:9-14. Likewise, Claim 11 of the ’892 Patent describes the “encryption server” in almost an identical way. ’892 Patent, 12:54-60. Thus, the text of the claims supports Plaintiffs’ proposed construction that the encryption server “produced tokens in response to a request.”

The claims’ characterization of an “encryption server” is also consistent with the specifications and file histories. The ’641 Patent explains that the “encryption server” is for “producing a request token of each individual included in a group identified in a request for information that characterizes the group.” ’641 Patent, 2:1-4. In response to receiving the request from the user, the encryption server “creates a unique token, or identifier, for each person in the message,” i.e., the request. *Id.*, 5:31-36. The encryption server creates the token “by applying a token generator 314 that encrypts the personally identifiable information of each group member” in the request message. *Id.*, 5:36-38. The file histories similarly confirm that an “encryption server” is for producing tokens for individuals in the group. Ex. 3 at Mil_0001741 and 0001823. Based on the intrinsic evidence, a POSITA would understand that an “encryption server” as used in the Asserted Patents is a “server” that produces “tokens” in response to a request. Ex. 1, ¶ 5.22.

This Court, in its denial of Defendants’ motion to dismiss the complaint, also characterized the “encryption server” in a manner consistent with Plaintiffs’ construction, stating that the

“encryption server produces encrypted tokens A, B, C, D in response to a request for protected healthcare information of a group consisting of individuals W, X, Y and Z.” Dkt. 43 at 3. The Court’s characterization and understanding of the “encryption server” confirms the appropriateness of Plaintiffs’ construction.

“Encryption server” does not have a well-understood meaning in the computer science field, but from the individual words themselves, a POSITA would understand that an “encryption server” is a server that performs some sort of encryption. Ex. 1, ¶ 5.24. However, the Asserted Patents explain that a hash function can be an encryption technique according to the Asserted Patents. ’641 Patent, 5:65-67. Because encryption is often considered by a POSITA to be reversible (with corresponding decryption), but whereas a POSITA would consider a hash function to be practically irreversible, an “ordinary meaning” construction of “encryption server” might not capture that a hash function could be an encryption technique according to the Asserted Patents. Ex. 1, ¶ 5.24. Therefore, Defendant’s proposed “ordinary meaning” construction should not be adopted.

D. “similarly encrypted”

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“similarly encrypted”	’641 Patent, claim 7 ’892 Patent, claim 14 ’685 Patent, claim 11 ’651 Patent, claim 11 ’375 Patent, claim 11 ’012 Patent, claim 10	Generated such that tokens generated from corresponding information can be compared to one another to detect a match.	Indefinite

In the Asserted Claims, the tokens for individuals in the request and the tokens in the de-identified healthcare data are “similarly encrypted.” *See e.g.*, ’641 Patent, claim 7 (“wherein the produced **tokens** and the **tokens** in the set of de-identified data are similarly encrypted...”); ’892 Patent, claim 14 (“the **tokens** associated with the set of medical information and the produced

token for each individual in the group are similarly encrypted...”). The tokens are “similarly encrypted” so that a match between tokens can be found. *See e.g.*, ’685 Patent, claim 7 (“comparing the request tokens to tokens associated with the de-identified medical data to find matching tokens”); ’651 Patent, claim 7 (similar); ’375 Patent, claim 7 (“the data server is configured to compare the request tokens to tokens associated with healthcare data that includes de-identified information to find matching tokens”); ’641 Patent, 6:1-4 (“A token matcher 326 ... performs a look-up in the de-identified database 320 to find all tokens in the database that match the tokens sent from the encryption server ...”); *id.*, 7:42-44 (“Upon receiving a request token, de-identified data and a token, operations include determining whether the request token matches the token.”). For a given individual, the tokens from both the encryption server and the de-identified data server will match, according to the Asserted Patents, because the tokens are generated in a like way from the same personally identifiable information of the individual. ’641 Patent, 5:49-53 (“Each token obtained from the source sites 138 may have been created using the same token generator 314 used by the encryption server 312, or using any other means that generates the identical token for the same personally identifiable information.”).

This intrinsic evidence supports Plaintiffs’ construction that two tokens, generated from corresponding information (e.g., personally identifiable information of an individual), are “similarly encrypted” when then two tokens can be compared to detect a match. Ex. 1, ¶¶ 5.26-5.27. For example, the ’641 Patent’s specification explains “The data server may be configured to **compare** the request tokens to tokens associated with the information to be produced . . . [and t]he data server may be configured to determine if the comparison provides at least a minimum number of matches.” ’641 Patent at 2:15-21; *see also id.* at 1:54-56 (“Producing information that characterizes the group may include comparing the request tokens to tokens associated with the

information to be produced.”); 6:1-4 (“A token matcher 326, executed by the de-identified data server 318, performs a look-up in the de-identified database 320 to find all tokens in the database that match the tokens sent from the encryption server 312.”); 7:38-55 (describing operation of Fig. 3’s data server’s “token matcher” including “determining 606 whether the request token matches the token. . . . If such a minimum number of matches has not occurred in comparing the request tokens and the tokens, action may be taken (e.g., pause or restart processing) until the predefined number of matches has been detected . . .”). Indeed, the ability to match tokens is a fundamental aspect of the processes described in the Asserted Patents. Ex. 1, ¶ 5.3.

Defendant asserts that the term is indefinite. Courts have recognized several reasons for deferring ruling on indefiniteness at the claim construction stage. These reasons include: (i) while indefiniteness is a question of law to which general principals of claim construction apply, indefiniteness is an invalidity defense that must be proven by clear and convincing evidence; and (ii) while claim construction gives meaning to claim terms, indefiniteness invalidates the claims entirely. *See DuraSystems Barrier Inc. v. Van-Packer Co.*, Case No. 1:19-cv-01388, 2021 WL 4037826, *6-7 *(C.D. Ill. Sept. 3, 2021). This Court previously recognized that indefiniteness issues tend to involve battles of experts and factual disputes, making them more appropriate for later adjudication. *See Koninklijke Philips Elecs. N.V. v. Zoll Medical Corp.*, 914 F.Supp.2d 89, 100-101 (D. Mass. 2012); *Amax, Inc. v. ACCO Brands Corp.*, 282 F.Supp.3d 432, 441-442 (D. Mass. 2017); *see also 3-D Matrix, Inc. v. Menicon Co.*, Case No. 14-cv-10205-IT, 2016 WL 111410, *13 (D. Mass. Jan. 11, 2016) (Talwani, J.). In any event, Prof. Rubin’s testimony shows that “similarly encrypted” is not indefinite in the context of the Asserted Patents. Ex. 1, ¶ 5.30. Thus, the Court should not adopt Defendant’s position that the claim term is indefinite under § 112(b).

E. “medical information that characterizes a group”

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“medical information that characterizes a group”	’892 Patent, claim 11 ’685 Patent, claim 7	Ordinary meaning	Information characterizing health status of the group as a whole

Courts need not construe limitations consisting of commonly used terms. *See, e.g. Summit 6, LLC v. Samsung Elecs. Co.*, 802 F.3d 1283, 1291 (Fed. Cir. 2015). This is the case here. All of the words individually in the phrase “medical information that characterizes a group” are well understood and do not have specialized meanings in the field of computer science. The file histories confirm that no construction is necessary. In the ’892 Patent’s prosecution history, the applicant was able to easily point out to the examiner distinctions between the claimed “medical information that characterizes a group” and other information that might obliquely concern the topic of medicine. Specifically, when the examiner cited prior art relating to medical websites with medical information, the applicant distinguished that prior art from the claimed “medical information that characterizes a group” by explaining that “[d]elivery of a body of knowledge such as web sites visited by other patients is not medical information that characterizes a group of multiple individuals” Ex. 5 at Mil_0001027-1028. The examiner accepted that argument on its face, without any further explanation needed, confirming that this term needs no construction.

Defendant’s proposed construction should be rejected because it is inconsistent with the claim language and the patents’ specifications. The claim term recites “medical information,” yet Defendant’s construction replaces that phrase with a different concept, “health status.” “Medical information” and “health status” are not coterminous. “Medical information” can include information collected from healthcare professionals, such as procedures performed, prescriptions, or disabilities. Ex. 1, ¶ 5.33. Not all of this information necessarily includes a person’s “health

status,” i.e., whether the person has poor (or great) health. A person has a health status regardless of whether she ever sees a healthcare professional, while a person’s medical information—e.g., history of physician visits--may not include her health status. For that reason, Defendant’s construction is inconsistent with the claims’ plain language.

Nor is there justification in the patents’ specifications for limiting “medical information” to “health status.” While the Asserted Patents’ specifications teach that the report prepared following matching of the tokens may include a health status for the group (*see* ’892 Patent, 7:3), the Asserted Patents also disclose that the report can include information other than health status, such as medication utilization metrics (’892 Patent, 5:10-11) and diagnostic codes (*id.*, 9:44-45). Thus, not all embodiments report health status information. Consequently, it is improper to read “health status” into the claims to limit the scope of “medical information.” *See e.g., Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371–72 (Fed. Cir. 2014).

Defendant’s construction is also improper because it includes the phrase “as a whole.” The claims do not include that language, and it is not required by the specifications or any other intrinsic evidence. The Asserted Patents teach that not all of the request tokens for individuals in the group may match a corresponding token in the de-identified healthcare data. ’641 Patent, 8:8-10. Also, the final report from the matching process may indicate only that a subset of the individuals in the request take a certain medication and/or are likely to have a certain medical condition. ’641 Patent, 8:17-27 (“the requested de-identified data would include the likelihood that anonymous individuals associated with the request tokens ... have each of the conditions indicated by the prescribed drug”). Thus, the report can be formed based on a subset of the individuals in the group and, therefore, not necessarily for the group “as a whole.” Ex. 1, ¶¶ 5.36-5.37.

F. “absent authorization” terms

Term	Claims	Plaintiffs’ Construction	Defendant’s Construction
“absent authorization from the individuals in the group” / “absent authorization from individuals in the group” / “absent authorization from the group” / “without the individuals in the group having authorized production of such medical information” / “has been produced without the individuals in the group having authorized production of such healthcare information that characterizes the group”	’641 Patent, claim 7 ’892 Patent, claim 11 ’685 Patent, claim 7 ’651 Patent, claim 7 ’375 Patent, claim 7 ’012 Patent, claim 7	Ordinary meaning	Authorization was not given to produce the (healthcare/medical) information in response to the request

These terms use the word “authorization” and state that the authorization is “absent” or “without” having been given. A POSITA would know what these various “authorization” claim terms mean without an express construction because they are comprised of common English words that do not have specialized technical meaning. Ex. 1, ¶ 5.41.

To the extent a construction is needed, Defendant’s construction should be rejected because it conflicts with the intrinsic evidence in two main respects. *First*, Defendant’s construction drops from the meaning that the authorization has to be “absent,” or that the medical information is produced “without” authorization, “*from the individuals in the group*” This requirement is in the claims, yet missing in Defendant’s construction. See ’641 Patent, claim 7 (“absent authorization at any time *from the individuals in the group* of individuals” and “the produced healthcare information ... has been produced *without the individuals in the group having authorized* production of such healthcare information”); ’892 Patent, claim 11 (“absent authorization *from individuals in the group* of individuals”); ’685 Patent, claim 7 (“producing the

requested medical information ... *without the individuals in the group having authorized production* of such medical information that characterizes the group” and “providing the produced medical information ... absent authorization *from the individuals in the group of individuals* identified in the request containing identifying data”). By dropping the requirement that the authorization is from the individuals in the group request, Defendant inappropriately alters the meaning of the claims. For example, Defendant’s proposed construction allows for the authorization to be absent from somebody, or some party, that is not an individual in the group. This proposed construction is inconsistent with the intrinsic evidence.

Second, by adding the “in response to the request” language at the end of its proposed construction, Defendant’s proposed construction implies a causal connection between the request and the authorization, i.e., authorization is sought, under Defendant’s proposed construction, “in response to the request” for the healthcare/medical information. This makes Defendant’s construction wholly inconsistent with the intrinsic evidence. In the Asserted Patents, the authorization to produce the healthcare/medical information is not made in response to the request for the healthcare/medical information. To the contrary, the request for the healthcare/medical information that characterizes the group initiates a process that generates the healthcare/information without the need to obtain the individuals’ authorization for any step or aspect of the invention, including no authorization for producing or reporting the healthcare/medical information, no authorization for accessing the healthcare/medical information, and no authorization for generating tokens that represent the individuals’ identities. *See e.g.*, ’641 Patent, 4:32-61, 7:1-21. Accordingly, the Court should reject Defendant’s proposed construction which limits this term in a way that is inconsistent with the intrinsic evidence.

V. CONCLUSION

Plaintiffs respectfully request that the Court adopt Plaintiffs’ proposed constructions.

Dated: October 20, 2022

Respectfully submitted,

/s/ Christopher Centurelli
Christopher Centurelli (BBO #640974)
christopher.centurelli@klgates.com
John L. Gavin (BBO #705385)
john.gavin@klgates.com
K&L GATES LLP
State Street Financial Center
One Lincoln Street
Boston, MA 02111
Telephone: (617) 261-3100
Facsimile: (617) 261-3175

and

Patrick J. McElhinny (*pro hac vice*)
patrick.mcelhinny@klgates.com
Mark G. Knedeisen (*pro hac vice*)
mark.knadeisen@klgates.com
Anna Shabalov (*pro hac vice*)
anna.shabalov@klgates.com
K&L Gates LLP
K&L Gates Center
210 Sixth Avenue
Pittsburgh, Pennsylvania 15222
Telephone: (412) 355-6500
Facsimile: (412) 355-6501

*Attorneys for Milliman, Inc. and Milliman
Solutions, LLC*

and

Christopher Dillon (BBO #640896)
dillon@fr.com
Fish & Richardson P.C.
One Marina Park Drive
Boston, MA 02210
Telephone: (617) 542-5070

and

Noah C. Graubart (*pro hac vice*)
graubart@fr.com
Joseph R. Dorris (*pro hac vice*)

dorris@fr.com
Fish & Richardson P.C.
1180 Peachtree Street NE
21st Floor
Atlanta, GA 30309
Telephone: (404) 892-5005

Attorneys for Vigilytics LLC

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Christopher Centurelli