Final Report

Team 04

Alabhya Farkiya
Binbin Liu
Hary Krishnan
Yue Xing
Yuhan Zhou

Table of Content

Part One Requirements

S.No	Requirements	HIPAA Rule 1	OECD Framework
1.	The system shall be able to de-identify information based on 164.514(2)(i) before providing it to the advertisement company.	164.514(b)(2)(i)	
2.	The system shall be able to provide only concerned health information to the administrators/auditors.	164.512(a)(i) 164.512(d)	Use Limitation Principle
3.	Every update to the system's purpose of collecting user data, shall be notified to the user via a change in the privacy notice.	§164.520 (b)(3)	Openness Principle
4.	The system should ask for user consent for sharing health information with his family members for the purpose of paying his healthcare.	164.510(b)	
5.	The system shall be able to share confidential health information in times of emergency.	164.512(b)(3)	
6.	The system shall provide the user with a click wrap agreement with a privacy notice that shall describe the user's rights and Giant Beagle's legal duties with respect the use and disclosure of PHI, for completing the signup process. The privacy notice shall state that agreeing to sign up shall assume it to be a written agreement.	§164.520 (a)	
7.	The system shall disclose PHI without the user's written authorization, to a government benefits program for the purpose of deeming beneficiary eligibility	§164.512 (d)(1)	
8.	The system may assign a code which is not derived from the PHI, in order to re-identify the de-identified record of the user, solely to be used by Giant Beagle and not to be disclosed to any other	§164.514 (c)	

	entity for any purpose.		
9.	The system shall ensure the requirement of using limited data, and report any use of the information that is not provided by its data use agreement.	§164.514(e)(1)	
10.	The system shall allow user to terminate the agreement anytime at user's request and store a proof of termination on the system which is considered as a written request.	§164.522(2)	
11.	The system shall give each staff access to PHI based on their assigned job responsibility according to their job description	§ 164.514(d)	
12.	The system shall maintain all HIPAA related records required to be maintained for a minimum of 6 years	§ 164.530(j)(2)	
13.	The system shall inform an individual of the protected health information that it may include in a directory/database.	§ 164.510(a)(2)	Purpose Specification Principle
14.	The system shall use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.	§ 164.512(k)(1)	
15.	The system shall obtain authorization from the patient in writing prior to using PHI for marketing efforts.	§ 164.510(b)	
16.	Risks against the breach of the user's personal health information in the system's database has to be taken care		Security Safeguards Principle

	of, and in the event of such a breach, due recordance of the same should be done to exercise a standard of care to minimize such risks in the future.		
17.	The system shall allow users to sign-up/enroll to HCP from the website.		

Part Three Requirement Matrix

Privacy Laws and Standards	REQ-1	REQ-2	REQ-3	REQ-4	REQ-5	REQ-6	REQ-7	REQ-8	REQ-9	REQ-10	REQ-11	REQ-12	REQ-13	REQ-14	REQ-15	REQ-16
De-identification																
HIPPA §164.514(b)(2)(i)	X															
HIPPA §164.514 (c)								X								
Administrator Access																
HIPPA §164.512(a)(i)		X														
HIPPA §164.512(d)		X														
OECD Use Limitation Principle		X														
HIPPA §164.514(d)											X					
Consent																
HIPPA §164.510(b)				X												
HIPPA §164.514(e)(1)									X							
Confidentiality																
HIPPA §164.512(b)(3)					X											
OECD Openness Principle					X											
Authorization																
HIPPA §164.510(a)(2)													X			
OECD Purpose Specification Principle													X			
HIPPA §164.510(b)															X	
HIPPA §164.512(k)(1)														X		
Privact Notice																
HIPPA §164.520 (a)						X										
HIPPA §164.520 (b)(3)			X													
Disclosure Without Authorization																
HIPPA §164.512 (d)(1)							X									
Agreement Determination																
HIPPA §164.522(2)										X						
Maintenance																
HIPPA §164.530(j)(2)												X				
Security																
OECD Security Safeguards Principle																X