

MR YOUNG

This report provides an analysis of the service from a privacy by design perspective using the process from the book Strategic Privacy by Design

Strategic Privacy Design
Report
APRIL 2019

Prepared in cooperation with
<https://www.dposolutions.co>

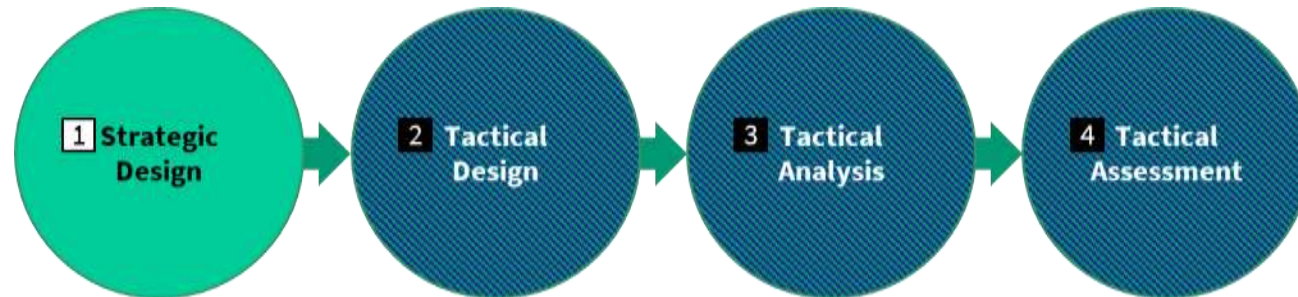


DPOsolutions
Data Protection

© 2019 Enterprivacy Consulting Group
<https://enterprivacy.com>

This Report

This is a **Level 1 Strategic Design** report.



Level 1 Strategic Design

Based on the goals and quality attributes of the product, service or process being reviewed, a strategic design report identifies individuals, threat actors, information and factors contributing to privacy risk. It concludes by identifying strategies to mitigate those risks and where those strategies should be applied.

Level 2 Strategic Gaps and Tactical Design

A tactical design report expands on the strategic design report by identifying strategic gaps between the proffered design and the architecture of the actual product, service or process. For non-deployed strategies, this report indicates the organization's justification and analysis as to why the strategy was not used. For deployed strategies, the report details tactical design recommendations for each strategy.

Level 3 Tactical Analysis

A tactical analysis report identifies gaps between the proposed tactics in the tactical design report and implemented tactics. It looks to see whether other employed tactics sufficiently mitigate risks.

Level 4 Tactical Assessment

A tactical assessment looks at a range of identified tactics implemented by the organization and reviews the sufficiency of the implementation to mitigate risks. Unlike the other reports, this is limited in scope to a predefined set of tactics desiring extra scrutiny.

Contents

This Report	1
Executive Summary	3
Description of Product, Service or Process	5
Goals	5
Quality Attributes.....	6
Implicated At-Risk Individuals	7
Legitimacy, Appropriateness and Adequacy	8
Potential Threat Actors.....	9
Privacy Model.....	10
Minimal Necessary Information	11
Potential Violation Risk Factors	18
Recommended Control Strategies.....	23
Recommended Next Steps.....	34
Step 1 Strategic Decision Making	34
Step 2 Tactical Design.....	34
Step 3 Implementation Technique	34
Appendix A – Hoepman Strategies and Tactics	35

Executive Summary

Enterprivacy Consulting Group (“Enterprivacy”) reviewed the proposed service, Mr Young AI, an innovative chat bot design to assist individuals to locate and use resources to improve their mental well-being. The Users are both the primary beneficiaries of the service and the most at-risk individuals. Three other types of individuals interacting with the service (health providers, Mr Young client employees and Mr Young employees) primarily perform administrative tasks in the system and while risks exist they are not as acute as the risks to users.

In addition to the four at-risk individuals, Enterprivacy identified five goals of the service, five quality attributes that could affect information collection and use, 15 potential threat actors and around 500 opportunities for strategic reduction in privacy risks.

KEY FINDINGS

1. Because Client Employees and Mr Young Employees interact with the service to facilitate their employers’ goals and because of the asymmetric power imbalance between employers and employees, care should be taken in minimize privacy risks to these individuals especially from their employers. Health Providers may be similarly situated though, for this analysis, Enterprivacy did not review the risks of their employer’s as threat actors.
2. Similarly, where Users are employees, students or otherwise affiliated with a Client Organization, heightened consequences could result from those organization’s access to or use of information about Users. Special attention should be made to the controls prevent access to individualized data about Users from Client Organizations and Client Organization Employees.
3. Because the chat bot is computerized, Users may let down their guard and reveal information they wouldn’t share with a potentially judgmental person. The expectation would be that that chat bot wouldn’t share it with others thus Users may suffer heightened consequences from dissemination of information by the chat bot. Note, dissemination risks include dissemination to those who are not in the pool of threat actors. In this case, one significant risk is that the chat bot will

reveal information about one User to another User, even though a User is not considered a threat actor in this model.

4. Finally, because acquaintances of Users may access their phones and information about their interactions with the chat bot, either inadvertently or purposefully, those acquaintances pose a significant privacy risk to the Users.

The key findings here should not detract from the other risks identified or mitigation strategies. Care should be taken to employ strategies to reduce privacy risks in all practical circumstances. In general, front-loading the strategies gives organizations the most benefit. In other words, Architecting the system not to use information reduces the need to Secure information. Securing information away from actors, reduces the need to Supervise their use of the information.



R. Jason Cronk
Principal Privacy and Trust Consultant

Enterprivacy
Consulting
Group

Disclaimer: This analysis is based on public information and information provided by the company on the nature of the provided services. In the event there are system components or functionality that was not identified, this analysis would not cover those risks or possible mitigation strategies. In addition, the risk factors and suggested controls are based on educated guesses and broad categorizations of the threat actors, threats and appropriateness and adequacy of potential controls.

Description of Product, Service or Process

Mr Young is an AI application that runs over one of several messenger applications (Facebook Messenger, Slack, WhatsApp, Teams) to verbally communicate with users, in English or French. Organizations such as businesses, non-profits or educational institutions make the service available to their employees, members or students. The AI application is designed to help individuals deal with anxiety, stress and improve mental health and wellness by connecting them with services and resources that may benefit them. Organizations, including government employers, can develop insights into their workforce (or members/students in the case of insurance programs or schools) to develop broad based programs to improve mental health and wellness. Health professionals provide information about their services to Mr Young, which in turn provides that information determined to be relevant to users.

Resources Reviewed

- <https://www.mryoung.co/>
- <http://quartierinnovationmontreal.com/en/article/mr-young-artificial-intelligence-service-mental-health>
- <https://www.cpacanada.ca/en/news/atwork/2019-01-30-mr-young-mental-health-bot>

Goals

What are the goals of this product, service or process?

- G1** To provide information to users on available relevant mental health services
- G2** To provide users a non-judgmental computerized agent they can discuss their symptoms with
- G3** To provide health providers the ability to inform potential patients about their services
- G4** To provide organizations insight into their employees' well-being ¹
- G5** To provide free self-evaluation tools for anxiety, stress, quality of life (scientifically validated psychometric tests)

¹ "With Mr. Young, managers can gauge the mood within their teams and see what's working and what isn't" - <https://www.cpacanada.ca/en/news/atwork/2019-01-30-mr-young-mental-health-bot>

Quality Attributes

While the goals represent the primary functionality of the product, service or process being developed, the following attributes represent required qualities. They are considered non-functional requirements. In other words, they are requirements but are not strictly necessary to meet the goals. Because some of these quality attributes may have implications on the design and the collection or use of personal information, they are identified here and the implications are explicitly called out. The implications identify the category of information (in bold), the threat actor requiring that information and how that information will be used to meet the required quality attribute. Where the implications may not be obvious, the quality attribute is still included though the implications may be incomplete.

Because many quality attributes increase privacy risks, alternative designs should be considered to reduce these requirements. For instance, many services require the attribute of **accountability** of individuals to discourage fraudulent use of services and punish fraudsters after the fact. However, this often results in **Surveillance** of all users, not just the fraudsters. The question from a designer's perspective, is how do we design the service to prevent fraudulent use (or reduce it to an acceptable level) and not just discourage and punish fraudsters.

	Attribute	Definition	Design and Information Implications
Q1	reliability	Probability that a system will satisfactorily perform the tasks it was designed for	
Q2	usability	The extent to which a product can be used by specific users to accomplish specific goals	
Q3	manageability	Ability to guide or direct system operations	<ul style="list-style-type: none"> ① Identifying to identify Mr Young employees' administration of the service ① Preference to tailor the administrative interface to organizational client employees' liking ① Preference to tailor the administrative interface to Mr Young employees' liking ① Authenticating to authenticate Mr Young employees' access to resources to administer site
Q4	securability	Ability to provide different levels of access to different users according to their security clearance	<ul style="list-style-type: none"> ① Identifying to identify Mr Young employees' administration of the service ① Authenticating to authenticate organizational client employees to access the service ① Authenticating to authenticate Mr Young employees to access the service ① Authenticating to authenticate health providers to access the service
Q5	demonstrability	Ability to prove the system performs in a certain way	<ul style="list-style-type: none"> ① Identifying to identify Mr Young employees' administration of the service

Implicated At-Risk Individuals

The following categories of individuals are at risk of privacy violations in this product, service or process. Subsequent references in the document will always use encircled letters corresponding to the at-risk individuals.

- Ⓐ **Users (Patients)** – Users, such as employees of a client company, interact with the chatbot to seek help and learn about the services that may be available to them.
- Ⓑ **Health Provider** – Trained mental health providers (doctors, nurses, therapists) use the service to provide information about their services made available to potential users/patients. The analysis assumes Health Providers are solo practitioners or small businesses (Doctor's office) and does not discuss the possible differentiation of interests and risks between a Health Provider and Health Provider Employee.
- Ⓒ **Organizational Client Employees** – Employees of organizational clients who manage the service to provide health and wellness to their employees.
- Ⓓ **Mr Young Employees**— Project team and staff of Mr Young who administer the system.

Within these categories of individuals, certain types of individual may have a higher frequency of violations and be more susceptible to consequences as a result of violations.

- **Minors** Ⓐ
- **Crime Victims** Ⓐ
- **Crime Witnesses** Ⓐ
- **Ethnic Minorities** Ⓐ
- **Religious Minorities** Ⓐ
- **LGBT** Ⓐ
- **Mental Health Patients** Ⓐ
- **Victims of Intimate Partner Violence** Ⓐ
- **Victims of Human Trafficking** Ⓐ
- **Wealthy Individuals** ⒶⒷ
- **High Profile Individuals (celebrity/politician)** Ⓐ
- **Employees** ⒶⒷⒸⒹ

Inclusion of these individuals in the population should be considered when deciding the use of certain strategies and tactics and whether not using those strategies or tactics are worth the risks to the affected populations.

Legitimacy, Appropriateness and Adequacy

Legitimacy – Is the application <u>beneficial</u> to the affected populations?			Appropriateness – Is it built with proper technology?	Adequacy - Is the technology built properly?
Ⓐ	Users	The goals of the application are to improve access to resources that help with users' mental health and well-being, so in general, the application benefits users. In determining tradeoffs for specific functionality or activities, care should be taken that adverse consequences don't outweigh the benefits.	<i>The question of appropriateness is addressed in a level 2 Tactical Design report as it reviews the actual or proposed architecture of the product, service or product.</i>	<i>The question of adequacy is addressed in both the level 3 Tactical Analysis and level 4 Tactical Assessment report as it reviews the implementation of the product, service or product.</i>
Ⓑ	Health Providers	Health providers are able to reach patients more effectively, reducing transaction costs for both provider and user/patient in matching them.		
Ⓒ	Organizational Client Employees	There is no direct benefit to client employees, but clients benefit by supporting a healthier workplace. This benefit indirectly affects client employees because they have a healthier workplace, but that's not the reason they are interacting with the service in this context (which is to administer the system). Any collecting of client employee personal information must consider the asymmetric relationship of the (business) client and its employee being instructed to administer the system.		
Ⓓ	Mr Young Employees	There is no direct benefit to Mr Young Employees.		

Potential Threat Actors

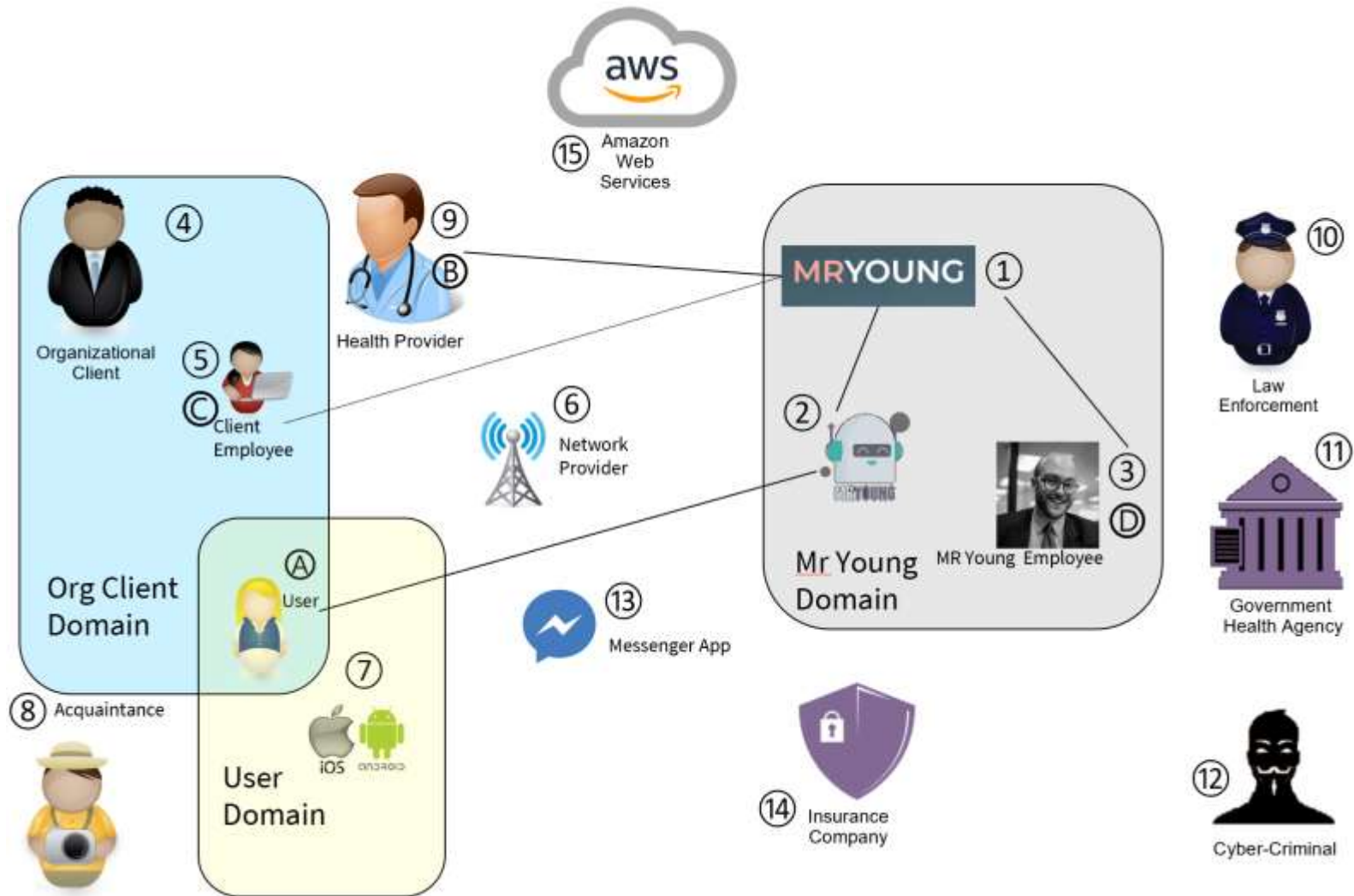
Threat actors are those whose activities could constitute a privacy violation. Potential threat actors for this product, service or process are identified below:

#	Actor	Type	Motives	Resource Level	At Risk Individuals			
					(A)	(B)	(C)	(D)
①	Mr Young Corp	Organization	<i>Money & competitive advantage.</i>	Small to Medium	✓	✓	✓	✓
②	Mr Young AI	AI	<i>Unintended programmatic direction</i>	Small to Medium	✓	✓		
③	Mr Young Employees	Persons	<i>Revenge, money, spite, curiosity, & control.</i>	Solo	✓	✓	✓	✓
④	Organizational Client These are businesses who have hired Mr Young to provide services to their employees, who are the Users ☺	Organization	<i>Money, competitive advantage & control (of employees)</i>	Medium to Multi-National	✓	✓	✓	✓
⑤	Organizational Client Employees These are employees of Mr Young's clients who may administer Mr Young's services.	Persons	<i>Revenge, money, spite, curiosity, & control.</i>	Solo	✓	✓	✓	✓
⑥	Network Providers	Organization	<i>Money & competitive advantage.</i>	Multi-National	✓	✓	✓	✓
⑦	User Mobile Device Provider	Organization	<i>Money & competitive advantage.</i>	FAAMG ²	✓	✓		
⑧	User Acquaintance	Persons	<i>Revenge, money, spite, curiosity, & control.</i>	Solo	✓	✓		
⑨	Medical Provider	Organization	<i>Money & competitive advantage.</i>	Small to Medium	✓	✓		✓
⑩	Law Enforcement	Government	<i>Law enforcement, espionage, control & repression.</i>	Local to Industrialized	✓	✓	✓	✓
⑪	Gov't Health Agency	Government	<i>Law enforcement, espionage, control & repression.</i>	Local to Industrialized	✓	✓		
⑫	Cyber-criminal	Persons	<i>Revenge, money, spite, curiosity, & control.</i>	Amateur to Professional	✓	✓	✓	✓
⑬	Message Platform (Messenger)	Organization	<i>Money & competitive advantage.</i>	FAAMG	✓	✓		
⑭	Insurance company	Organization	<i>Money & competitive advantage.</i>	Large to Mult-National	✓	✓		
⑮	Amazon Web Services	Organization	<i>Money & competitive advantage.</i>	FAAMG	✓	✓	✓	✓

² FAAMG refers to Facebook, Amazon, Apple, Microsoft or Google, who because of their vast resources represent a significant level above most other multi-national companies. Similarly, super-powers are at a resource level of the own for government threat actors.

Privacy Model

Encircled letters correspond to at-risk individuals. Encircled numbers correspond to potential threat actors from the chart above.



Minimal Necessary Information

“N/A” in the purpose means the information is not necessary to support a goal or quality attribute of the service. This does not mean the information doesn’t exist or can’t be inferred, but suggest controls must be put in place to eliminate the information from the system.

One reason for the categorization of information is it alleviates the problem of discussing granularity at this strategic design phase. It’s up to the designers, during tactical implementation, to sufficiently minimize the granularity of information necessary to accomplish a stated goal.

EXAMPLE of Granularity of Information

Goal: To determine if a candidate’s salary requirements exceed a company’s ability/desire to pay.

At-Risk Individual: Candidate






Threat Actor: Recruiter





Information Category: Professional & Preference






While a naïve approach would suggest the recruiter needs to know an actual value (i.e. \$100,000/year), in reality the minimal information necessary is whether the candidate’s requirements exceed the company’s ability or desire to pay. The naïve approach is based on a preconception about the method of calculation necessary: receive candidate’s actual salary requirement and compare it to company’s pay rate. In other words, the developer has preconceived how to do something necessitating more information than actually necessary. Using this method opens the candidate to potential privacy violations, most notably secondary use of information to inform the company during salary negotiations should the company decide to move forward.






One could use several strategies coupled with the naïve approach to reduce the risk of secondary use of information, such as creating a policy against such use and restricting access to salary requirement information to recruiters and not allowing the person doing the salary negotiation access to that information. One might also use a trusted third party to compare the figures. A more sophisticated approach would be to use a secure two party computation to ascertain the comparison information while not revealing the actual figures.¹





¹ See https://en.wikipedia.org/wiki/Secure_two-party_computation


External				
Type	☐ Users	☐ Health Providers	☐ Client Employees	☐ Mr Young Employees
	<i>Encircled numbers refer to the threat actors. G# refers to specific goals (G1 is goal 1). Q# refers to specific quality attributes (Q1 is quality attribute 1)</i>			
 Identifying Information that uniquely or semi-uniquely identifies a specific individual (<i>name, user-name, unique identifier, government issued identification, picture, biometric data</i>) SENSITIVE	② to persist discussion across distinct interactions. workforce usage for G2 ⑬ to facilitate exchange between user and Mr Young AI for G1, G2, G3, G4 and G5	① to authorize them to access service resources to provide information about the services they can provide users/ patients for G3	① to authorize them to access appropriate service resources and gain insights into workforce well-being for G4	① to identify employees' administration of the service Q3, Q4 & Q5
 Ethnicity Information that describes an individual's origins and lineage (<i>race, national or ethnic origin, languages spoken, dialects, accents</i>) SENSITIVE	② to interact with user in their native language for G1, G2 and G5	<i>N/A</i> <i>Note, if offering services to Health Providers in multiple languages this may be implicated</i>	<i>N/A</i> <i>Note, if offering services to Client Employees in multiple languages this may be implicated</i>	<i>N/A</i>
 Sexual Information that describes an individual's sexual life (<i>gender identity, preferences, proclivities, fetishes, history</i>) SENSITIVE	② to provide users resources that may relate to mental health issues around their sexuality for G1, G2 and G5	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>
 Behavioral Information that describes an individual's behavior or activity, on-line or off (<i>browsing behavior, call logs, links clicked, demeanor, attitude</i>)	② to identify traits in users that may help identify helpful resources for them for G1, G2 and G5	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>
 Demographic Information that describes an individual's	② to provide users resources based on resources used by	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>

characteristics shared with others (<i>age ranges, physical traits, income brackets, geographic</i>)	those in similar situations for G1, G2 and G5			
 Medical and Health Information that describes an individual's health, medical conditions or health care (<i>physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions</i>) SENSITIVE	② to engage the user and direct the user to available resources to improve their mental wellbeing based on their medical history and health conditions for G1, G2 and G5	N/A	N/A	N/A
 Physical Characteristic Information that describes an individual's physical characteristics (height, weight, age, hair color, skin tone, tattoos, gender, piercings)	N/A	N/A	N/A	N/A
Internal				
 Knowledge and Belief Information about what a person knows or believes (<i>religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks</i>)	② to help a user deal with how they are feeling (sentiments) for G2	N/A	N/A	N/A
 Preference Information about an individual's preferences or interests (<i>opinions, intentions, interests, favorite foods, colors, likes, dislikes, music</i>)	② to alter advice based on user preferences, such as locations or times for G1, G2 and G5	① to improve service and facilitate better matching with potential patients for G1 & G3	① to tailor the administrative interface to organizational client employees' liking for Q3	① to tailor the administrative interface to Mr Young employees' liking for Q3

 Authenticating Information used to authenticate an individual with something they know (<i>passwords, PIN, mother's maiden name</i>)	② to authenticate users to allow them access to the resources for G1, G2 and G5	① to authenticate health providers to update information about their services for G3 & Q4	① to authenticate organizational client employees to access the service for G4 & Q4	① to authenticate Mr Young employees' access to resources to administer site for Q3 & Q4
Tracking				
 Contact Information that provides a mechanism for contacting an individual (<i>email address, physical address, telephone number</i>)	⑬ to facilitate interaction between user and Mr Young AI for G1, G2 and G5	① to inform health providers about updates and changes for G3	① to inform client employees about changes or updates to client accounts for G4	N/A
 Computer Device Information about a device that an individual uses for personal use, even part-time or with others (<i>IP address, Mac address, browser fingerprint</i>)	N/A	N/A	N/A	N/A
 Location Information about an individual's location (<i>country, GPS coordinates, room number</i>) <div style="background-color: red; color: white; padding: 2px; display: inline-block;">SENSITIVE</div>	② to identify relevant service providers to the user for G1	① to facilitate matching with patients in a defined geographical area for G1	N/A	N/A
Social				
 Professional Information about an individual's educational or professional career (<i>job titles, salary, work history, school attended, employee files, employment history, evaluations, reference interviews, certifications, disciplinary actions</i>)	N/A	① to facilitate appropriate matching with patients based on skill sets and services for G1 & G3 ③ Mr Young Employees may review the service offerings of health providers be allowing them on the	N/A	N/A

		service, which might indicate professional information about those health providers for G3		
 Criminal Information about an individual's criminal activity (<i>convictions, charges, pardons</i>) SENSITIVE	N/A	N/A	N/A	N/A
 Public Life Information about an individual's public life (<i>character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data</i>) SENSITIVE	N/A	N/A Note: will Mr Young be reviewing or collecting reputation-based information on the health providers?	N/A	N/A
 Family Information about an individual's family and relationships (<i>family structure, siblings, offspring, marriages, divorces, relationships</i>)	② to assist user with family related issues (marriage counselor) for G1, G2 and G5	N/A	N/A	N/A
 Social Network Information about an individual's friends or social connections (<i>friends, connections, acquaintances, associations, group membership</i>)	N/A	N/A	N/A	N/A
 Communication Information communicated from or to an individual (<i>telephone recordings, voice mail, email</i>) SENSITIVE	⑬ to facilitate communication between users and Mr Young AI for G1, G2 and G5	① ③ to communicate with health providers about the use of the service (i.e. customer support) for G3	③ to communicate with client employees about the use of the service (i.e. customer support) for G4	N/A

	⑥ to facilitate communication between Users and the messenger service for G1, G2 and G5	⑥ to facilitate communication between health providers and Mr Young for G3	⑥ to facilitate communication between client employees and Mr Young for G4	
Financial				
 Account Information that identifies an individual's financial account (<i>credit card number, bank account</i>) SENSITIVE	N/A	N/A	N/A	N/A
 Ownership Information about things an individual has owned, rented, borrowed, possessed (<i>cars, houses, apartments, personal possessions</i>)	N/A	① ③ May be aware of ownership of business interests of the health provider for G3	N/A	N/A
 Transactional Information about an individual's purchasing, spending or income (<i>purchases, sales, credit, Income, loan records, transactions, taxes, purchases and spending habits</i>)	N/A	N/A	N/A	N/A
 Credit Information about an individual's reputation with regards to money (<i>credit records, credit worthiness, credit standing, credit capacity</i>) SENSITIVE	N/A	N/A	N/A	N/A
Historical				

 Life History Information about an individual's personal history (<i>events that happened in a person's life, either to them or just around them which might have influenced them</i>)	② to assess what resources might help the user (such as services for PTSD from past trauma). The user may reveal historical events that caused them anxiety or stress for G1, G2 and G5	N/A	N/A	N/A
---	---	-----	-----	-----

Potential Violation Risk Factors

Which privacy violations does each threat actor have the opportunity, given the privacy model, and motivation to commit?

















O – The threat actor is given an opportunity through the architecture to engage in an activity that could be this privacy violation.

M – The threat actor has a motive to commit this potential privacy violation.

















C – The consequences to certain individuals may be higher from this threat actor towards certain individuals

While all actors could have some opportunity or motive, the inclusion of them in these charts represents that they cross a subjective threshold which warrants risk mitigation effort.

















A) User – This table identifies risk factors for potential privacy violations by the threat actors against the users.

Collection	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Surveillance watching, listening to, or recording of an individual's activities	OM	OM	O	M	M	OM	OM	MC	M	OM	OM	OM	OM	O	O
 Interrogation questioning or probing for personal information	O	OM	O	M	M		OM	OMC	M	OM	O	OM	OM	O	O
Information Processing	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Aggregation combining of various pieces of personal information	OM	OM	O	OMC	O	OM	OM	OM	OM	OM	OM	OM	OM	O	O
 Identification linking of information to a particular individual	OM	O	OM	OMC	OM	OM	OM	O	O	OM	OM	OM	OM	O	O
 Insecurity carelessness in protecting information from leaks or improper access	OM	O	O	OMC	O	OM	OM	O	OM	OM	OM	OM	OM	O	O
 Secondary Use using personal information for a purpose other than the purpose for which it was collected	OM	OM	OM	OMC	OM	OM	OM	OMC	OM	OM	OM	OM	OM	O	O
 Exclusion failing to let an individual know about the data that others have about her and participate in its handling or use	OM	OM	OM	OMC	OM	OM	OM	OMC	OM	OM	OM	OM	OM	O	O
Information Dissemination	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Breach of Confidentiality breaking a promise to keep a person's information confidential	O	OC	O	O	OM	O	O	OMC	O	O	O	O	O	O	O
 Disclosure revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	O	OC	O	OM	OM	O	O	OMC	O	OM	O	OM	O	O	O
 Exposure revealing an individual's nudity, grief, or bodily functions	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
 Increased Accessibility amplifying the accessibility of personal information	O	OC	O	OM	O	OM	OM	OMC	O	M	M	M	O	O	O
 Blackmail threatening to disclose personal information	O	OC	OM	O	OM	O	O	OMC	O	OM	O	M	O	O	O
 Appropriation using an individual's identity to serve the aims and interests of another	OM	OC	O	O	O	O	O	O	O	O	O	O	O	O	O
 Distortion disseminating false or misleading information about an individual	O	OC	O	O	OM	O	O	OMC	O	OM	O	OM	O	O	O
Invasion	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Intrusion disturbing an individual's tranquility or solitude	M	OM			M	M	O	OC				OM	OM		O
 Decisional Interference intruding into an individual's decision regarding her private affairs	M	OM		M	OM		O	OMC	OM	M	M	OM	OM		O














ⓑ Health Provider - This table identifies risk factors for potential privacy violations by the threat actors against the health providers.

Collection	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Surveillance watching, listening to, or recording of an individual's activities	OM		O			OM				M	M	M			O
 Interrogation questioning or probing for personal information	OM		O							M	M	M			
Information Processing	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Aggregation combining of various pieces of personal information	OM		O			OM				M	M	M			
 Identification linking of information to a particular individual	OM		O			OM				M	M	M			
 Insecurity carelessness in protecting information from leaks or improper access	OM		O			OM									
 Secondary Use using personal information for a purpose other than the purpose for which it was collected	OM		O			OM				M	M	M			
 Exclusion failing to let an individual know about the data that others have about her and participate in its handling or use	OM		O			OM				M	M	M			
Information Dissemination	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Breach of Confidentiality breaking a promise to keep a person's information confidential	OM		OM			OM									
 Disclosure revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	O		O			O									
 Exposure revealing an individual's nudity, grief, or bodily functions	O		O			O									
 Increased Accessibility amplifying the accessibility of personal information	OM		O			O									
 Blackmail threatening to disclose personal information	OM		O			O									
 Appropriation using an individual's identity to serve the aims and interests of another	OM		O			O									
 Distortion disseminating false or misleading information about an individual	O		O			O									
Invasion	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Intrusion disturbing an individual's tranquility or solitude	OM		O			O									O
 Decisional Interference intruding into an individual's decision regarding her private affairs	OM		O			O									

© Organizational Client Employee - This table identifies risk factors for potential privacy violations by the threat actors against the organizational client employees.

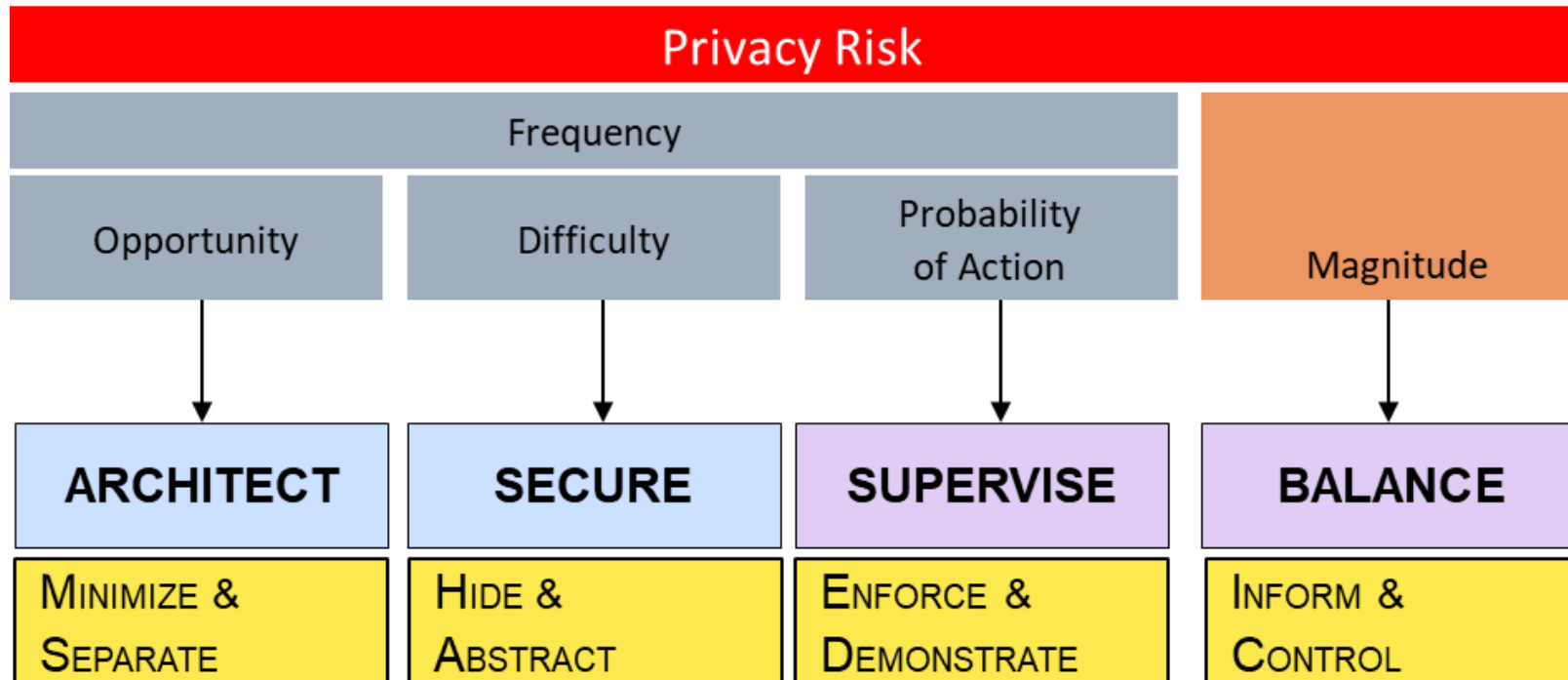
Collection	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Surveillance watching, listening to, or recording of an individual's activities	OM		OM	OMC	OM	OM						M			O
 Interrogation questioning or probing for personal information	OM		OM	OMC	OM	OM						M			
Information Processing	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Aggregation combining of various pieces of personal information	OM		O	O	OM	OM						M			
 Identification linking of information to a particular individual	O		O	O	O	O						M			
 Insecurity carelessness in protecting information from leaks or improper access	OM			OM	OM	OM									
 Secondary Use using personal information for a purpose other than the purpose for which it was collected	O		O	OC	O	O									
 Exclusion failing to let an individual know about the data that others have about her and participate in its handling or use	O		O	OC	O	O									
Information Dissemination	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Breach of Confidentiality breaking a promise to keep a person's information confidential															
 Disclosure revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	O		O	O	O	O									
 Exposure revealing an individual's nudity, grief, or bodily functions															
 Increased Accessibility amplifying the accessibility of personal information	O				O										
 Blackmail threatening to disclose personal information															
 Appropriation using an individual's identity to serve the aims and interests of another															
 Distortion disseminating false or misleading information about an individual	O		O	O	O										
Invasion	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
 Intrusion disturbing an individual's tranquility or solitude	O		O												O
 Decisional Interference intruding into an individual's decision regarding her private affairs	O		O												

© Mr Young Employee - This table identifies risk factors for potential privacy violations by the threat actors against Mr Young's employees.

Collection	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	
 Surveillance watching, listening to, or recording of an individual's activities	OM		OM													0
 Interrogation questioning or probing for personal information	OM		0													
Information Processing	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	
 Aggregation combining of various pieces of personal information	OM		OM													0
 Identification linking of information to a particular individual	OM		OM													0
 Insecurity carelessness in protecting information from leaks or improper access	OM		OM													0
 Secondary Use using personal information for a purpose other than the purpose for which it was collected	OMC		OM													0
 Exclusion failing to let an individual know about the data that others have about her and participate in its handling or use	OMC		OM													0
Information Dissemination	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	
 Breach of Confidentiality breaking a promise to keep a person's information confidential	OM		OM													0
 Disclosure revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	OM		OM													0
 Exposure revealing an individual's nudity, grief, or bodily functions	OM		OM													0
 Increased Accessibility amplifying the accessibility of personal information	OM		OM													0
 Blackmail threatening to disclose personal information	OM		OM													0
 Appropriation using an individual's identity to serve the aims and interests of another	OM		OM													0
 Distortion disseminating false or misleading information about an individual	OM		OM													0
Invasion	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	
 Intrusion disturbing an individual's tranquility or solitude	OM		OM													0
 Decisional Interference intruding into an individual's decision regarding her private affairs	OM		OM													0

Recommended Control Strategies

For each threat actor and potential violation, there are four areas and eight strategies where privacy risks can be mitigated.



For more information on specific tactics available under each strategy, see Appendix A.

ARCHITECT

The ARCHITECT strategies of MINIMIZE and SEPARATE reduce opportunities because they remove access to information or the individual.

- **MINIMIZE** - Limit as much as possible the processing of personal data.
- **SEPARATE** - Separate the processing of personal data as much as possible to prevent correlation.

SECURE

The SECURE strategies of HIDE and ABSTRACT are used to make it more difficult for other threat actors to commit privacy violations.

- **HIDE** - Protect personal data or make it unlinkable or unobservable
- **ABSTRACT** - Limit as much as possible the detail in which personal data is processed.

SUPERVISE

ENFORCE and DEMONSTRATE strategies are enacted by one actor and apply to another.

- **ENFORCE** - Commit to processing personal data in a privacy-friendly way, and enforce this.
- **DEMONSTRATE** - Demonstrate you are processing personal data in a privacy-friendly way.

Supervision comes in two forms. The first is contextual, whereby a policy dictates that an actor stay within a certain boundary of activities. For instance an employee may not use information for personal gain. These often mirror the potential privacy violations. The second dictates what the actor must do with regards to the other strategies. For instance, a company may hire a vendor and they are required to restrict access to certain information from that vendor (HIDE strategy). They must also have a contract with that vendor which requires them to restrict access to personal information to appropriate personnel. In other words, the company must ENFORCE a policy requiring the vendor to HIDE personal information from their employees. These second-tier strategies will be found in that actor's row in the charts.

BALANCE

The BALANCE strategies of INFORM and CONTROL do not reduce the likelihood or frequency of a particular activity but rather reduce its violative nature or effects. For instance, telling (Supply tactic under INFORM) a prospect

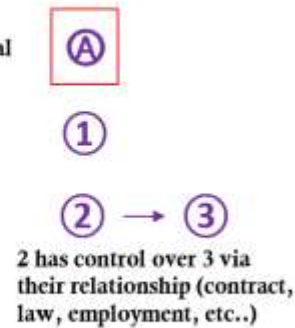
- **INFORM** - Inform data subjects about the processing of their personal data.
- **CONTROL** - Provide data subjects control over the processing of their personal data.

Legend to Maps

Information Map



Relationship Map



Certain assumptions are made about the information flow and relationships. If the actual design doesn't correspond to the mapping then recommended strategies will change.

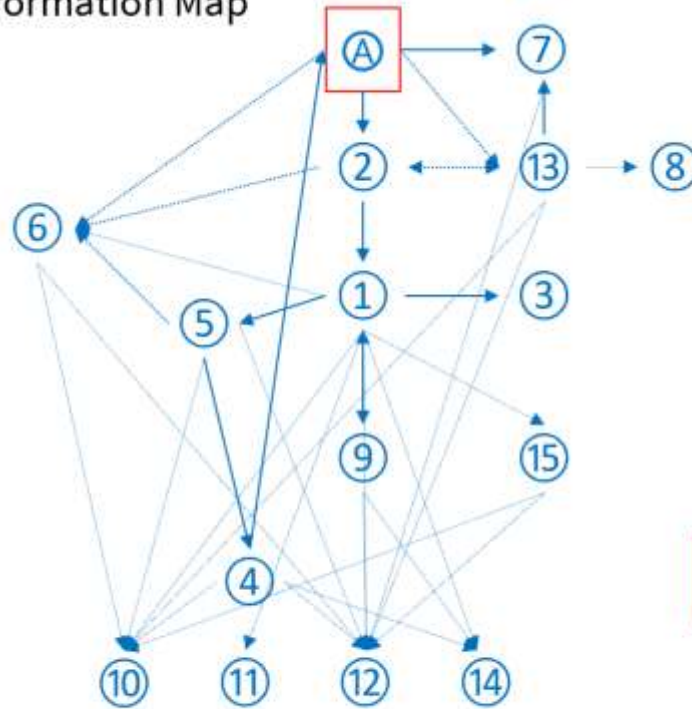
Legend to Recommended Strategies

		Apply To	
		①	②
Implementer	Ⓐ		
	①		

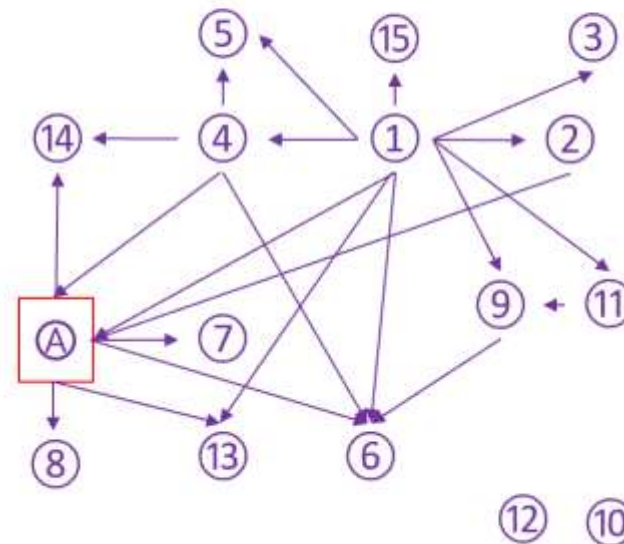
- BALANCE** – ① INFORMS the individual Ⓐ about the risks imposed by the activities ①. ① gives the individual Ⓐ CONTROL over the activities of ①.
- ARCHITECT** – ① MINIMIZES and SEPARATES information from ②
- SECURE** – ① HIDES and ABSTRACTS information unnecessary to ②
- SUPERVISE** – ① ENFORCES policies and DEMONSTRATES compliance by ②
- BALANCE** – ② INFORMS ① about the risk imposed by the activities of ②. ② gives ① CONTROL over the activities of ① all to be passed on to the individual Ⓐ.

Ⓐ User³

Information Map



Relationship Map

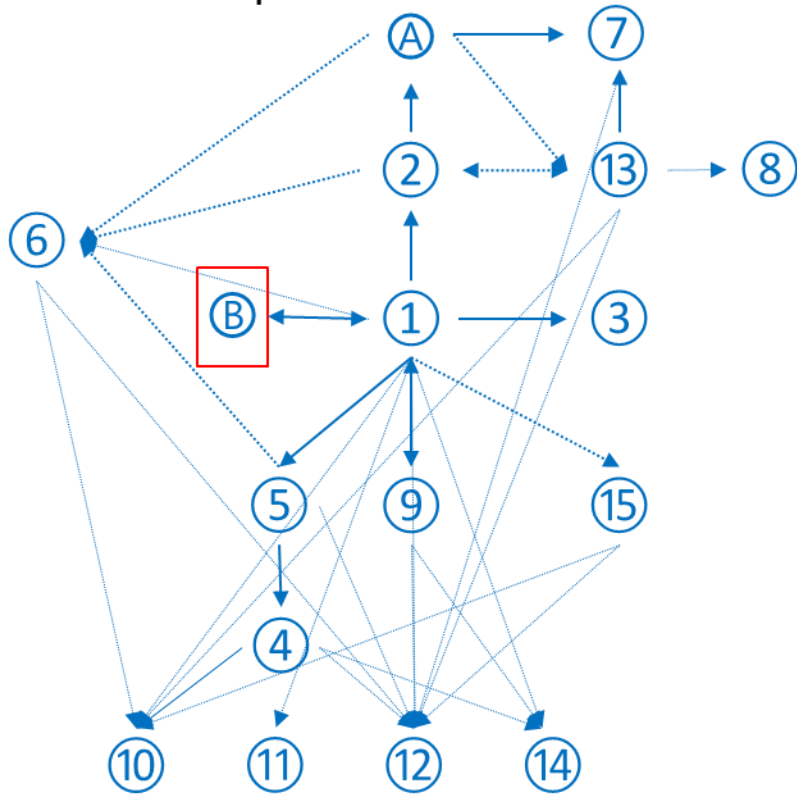


³ The above assumes that the Organizational Client ⑤ doesn't provide information about the User Ⓐ to Mr. Young ①, such as a name. The design requires that authorization codes be given to Users Ⓐ through the Organizational Client ⑤ to facilitate their access to the service.

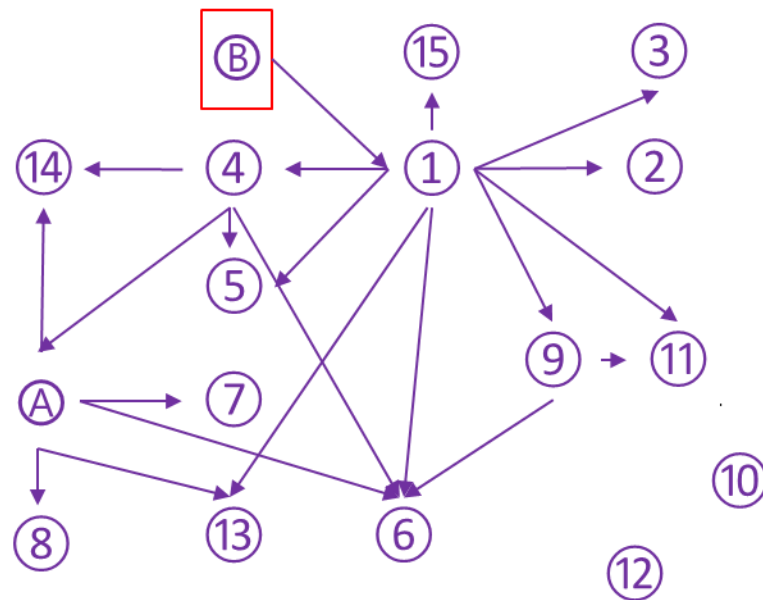
Ⓐ User		Apply To														
		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
Implementer	①															
	②															
	③															
	④															
	⑤															
	⑥															
	⑦															
	⑧															
	⑨															
	⑩															
	⑪															
	⑫															
	⑬															
	⑭															
	⑮															

ⓑ Health Provider

Information Map



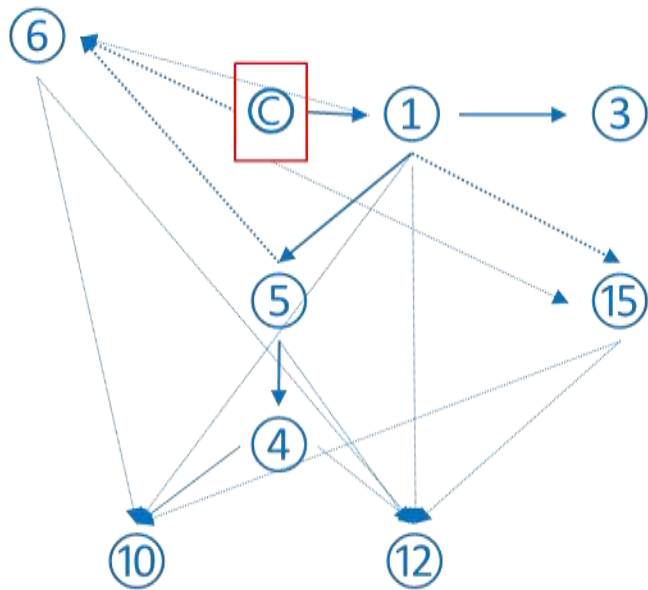
Relationship Map



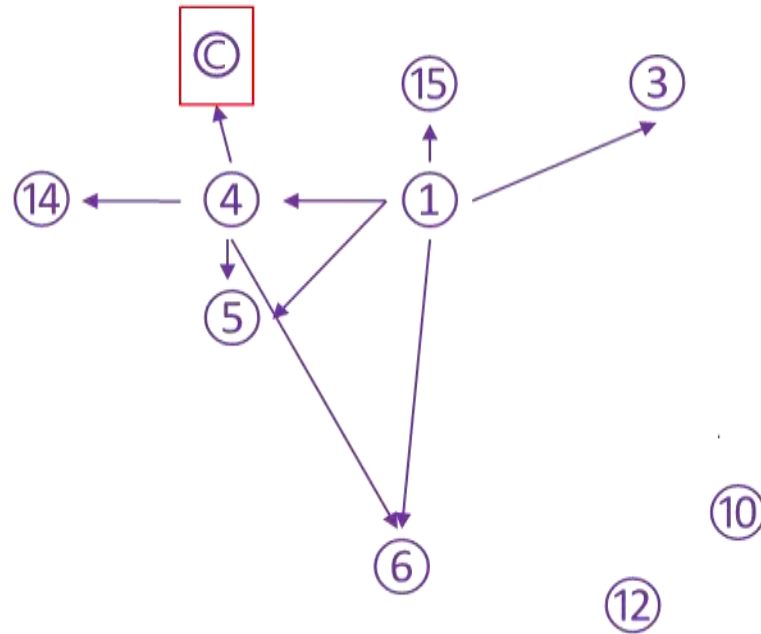
® Health Provider		Apply To														
		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
Implementer	①															
	②															
	③															
	④															
	⑤															
	⑥															
	⑦															
	⑧															
	⑨															
	⑩															
	⑪															
	⑫															
	⑬															
	⑭															
	⑮															

© Client Employee

Information Map

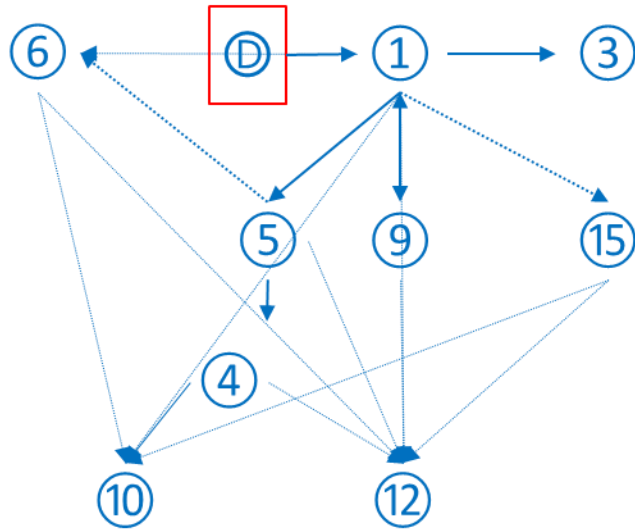


Relationship Map

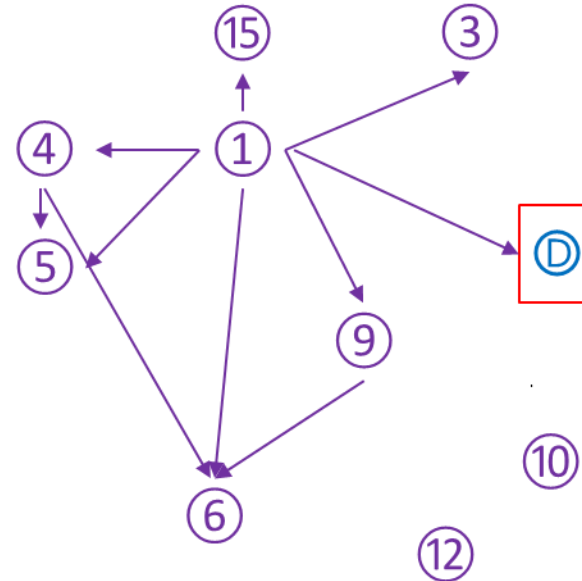


© Client Employee		Apply To														
		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
Implementer	①															
	②															
	③															
	④															
	⑤															
	⑥															
	⑦															
	⑧															
	⑨															
	⑩															
	⑪															
	⑫															
	⑬															
	⑭															
	⑮															

Information Map



Relationship Map





© Mr Young Employees		Apply To														
		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
Implementer	①															
	②															
	③															
	④															
	⑤															
	⑥															
	⑦															
	⑧															
	⑨															
	⑩															
	⑪															
	⑫															
	⑬															
	⑭															
	⑮															

Recommended Next Steps

Step 1 Strategic Decision Making

For each of the recommended strategies in the charts above, a decision should be made whether to employ that strategy or not. This may be done holistically or broken down by information category. For decisions not to employ a particular strategy, the reason for determination should be documented (such as compensating controls, cost justification, market limitations, etc.). This can provide opportunities to reevaluate the determination when circumstances change in the future.

EXAMPLE	Individual	Implementer	Apply To	Strategy	Information	Accept or Reject	Rejection Justification
TA1	PROSPECT	①	②	 ENFORCE	Identifying	Accept	
TA2	PROSPECT	②	①	 INFORM	Identifying	Reject	Risks sufficiently mitigated by ENFORCE strategy. No need to inform prospects because Eventus Employees will not access this information.


Step 2 Tactical Design

For each employed strategy, specific tactic(s) should be identified to achieve that strategy against specific types of information.

EXAMPLE	Individual	Implementer	Apply To	Strategy	Information	Accept or Reject	Tactic
TA1	PROSPECT	①	②	 ENFORCE	Identifying	Accept	Create



Step 3 Implementation Technique

Finally, actual implementation for each tactic should be detailed as the design progresses.



EXAMPLE	Individual	Implementer	Apply To	Strategy	Information	Accept or Reject	Tactic	Implementation
TA1	PROSPECT	①	②	 ENFORCE	Identifying	Accept	Create	A policy promulgated to employees forbids them from identifying prospects of organizational clients. See paragraph 4 of Policy 2018-100A.

Appendix A – Hoepman Strategies and Tactics

Data Oriented Tactics

	STRATEGY	Tactic	Description
 ARCHITECT	MINIMIZE	Exclude	Refrain from processing a data subject's personal data
	MINIMIZE	Select	Decide on a case by case basis to only process relevant personal data
	MINIMIZE	Strip	Remove, partially, unnecessary attributes
	MINIMIZE	Destroy	Remove, completely, personal data as soon as they become unnecessary
	SEPARATE	Distribute	Process personal data (for one task) in physically separate locations
	SEPARATE	Isolate	Process personal data (for different purposes) independently in (logically) separate databases or systems
 SECURE	HIDE	Restrict	Prevent unauthorized access to personal data
	HIDE	Mix	Process personal data randomly within a large enough group to reduce correlation
	HIDE	Obfuscate	Prevent understandability of personal data
	HIDE	Dissociate	Remove the correlation between data subjects and their personal data
	ABSTRACT	Summarize	Summarize detailed information into more abstract attributes
	ABSTRACT	Group	Aggregate data over groups of individuals, instead of processing data of each person separately
	ABSTRACT	Perturb	Add noise or approximate the real value of a data item.

Process Oriented Tactics

	STRATEGY	Tactic	Description
 SUPERVISE	ENFORCE	Create	Decide on a privacy policy that describes how you wish to protect personal data
	ENFORCE	Maintain	Maintain the privacy policy created
	ENFORCE	Uphold	Ensure that policies are adhered to by treating personal data as an asset, and privacy as a goal to incentivize as a critical feature.
	DEMONSTRATE	Audit	Audit the processing of personal data regularly
	DEMONSTRATE	Log	Track all processing of data, and reviewing this information gathered for any risks
	DEMONSTRATE	Report	Analyze collected information on tests, audits, and logs periodically and report to the people responsible
 BALANCE	INFORM	Supply	Inform users which personal data is processed, including policies, processes and potential risks
	INFORM	Notify	Alert data subject whenever their personal data are being used, or breached
	INFORM	Explain	Provide information in a concise and understandable form, and explain why processing is necessary
	CONTROL	Consent	Only process personal data for which explicit, freely-given, and informed consent is received.
	CONTROL	Choose	Allow data subjects to choose which personal data will be processed.
	CONTROL	Update	Provide data subjects with the means to keep their personal data accurate and up to date
	CONTROL	Retract	Honoring the data subject's right to the complete removal of any personal data in a timely fashion.