Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance
(Chapter 486, Laws of Hong Kong)

EC Healthcare's Sharing of Clients' Personal Data Among Its Various Brands Through an Integrated System

Executive Summary

Background

1. The Office of the Privacy Commissioner for Personal Data ("PCPD") received two complaints lodged by citizens on 10 June and 26 August 2021 respectively. Both complaints were made against the brands under EC Healthcare, namely, Primecare Paediatric Wellness Centre ("Primecare"), Dr Reborn, New York Medical Group ("NYMG") and re:HEALTH.

Investigation Case (1)

2. In the first case, which took place in June 2018, Complainant A took her daughter (the "Daughter") to a Primecare[1] clinic at Ocean Centre in Tsim Sha Tsui to consult a doctor (the "Doctor"). Upon registration, Complainant A provided the personal data of herself and the Daughter, and the phone number of the grandmother of the Daughter (the "Grandmother") for contact purpose.

3. In 2020, the Grandmother, who had been using the services provided by Dr Reborn, received a text message from Dr Reborn. The Grandmother noted that the message included the Daughter's name, and hence made inquiries with Dr Reborn. The Grandmother was told that since the

[1] Primecare is a paediatric wellness centre with four clinics. In-house doctors are available in each clinic. The clinic involved in the matter complained of is located on 12/F, Ocean Centre, 5 Canton Road, Tsim Sha Tsui, Kowloon.

Doctor joined Dr Reborn, the personal data of his clients had also been transferred to Dr Reborn.

4. Having learnt about the incident from the Grandmother in 2021, Complainant A lodged a complaint to the PCPD in June.

Investigation Case (2)

5. In another case, in March 2016, Complainant B received chiropractic treatments at an NYMG[2] centre, which was located at Humphreys Avenue in Tsim Sha Tsui at the material time, and he provided his personal data to NYMG.

6. In July 2021, Complainant B contacted a staff of re:HEALTH (the "Staff") by phone to follow up a complaint lodged by a member of his family against re:HEALTH, during which he provided his surname and phone number. Thereafter, the Staff called back Complainant B and addressed him by his full name.

7. Since Complainant B had never been in touch with the Staff, he questioned how the Staff had known his full name. The staff explained that since the complainant had previously used the service of NYMG, which was also under EC Healthcare, and the Staff was able to access the database of all clients of EC Healthcare, the Staff can thus access Complainant B's full name in the computer system. In addition to that, the Staff could tell the date when Complainant B visited NYMG.

8. Dissatisfied with such access by re:HEALTH to his record of medicalvisit(s) with NYMG, Complainant B lodged a complaint with the PCPD.

Investigation

9. Given that the four organisations involved in the matters complained of are all brands under EC Healthcare, and that replies to the preliminary inquiry made with Primecare by the PCPD were provided by EC Healthcare, the PCPD commenced investigations in respect of the two subject complaints against EC Healthcare on 6 August and 11 November

[2] NYMG is a one-stop centre for chiropractic consultations and physiotherapies. In-house doctors are available in each of the 26 pain centres currently in business. The centre involved in the matter complained of is located on 15/F, Humphrey Plaza, 4 Humphreys Avenue, Tsim Sha Tsui, Kowloon.

2021 respectively, in accordance with section 38(a)(i) of the Personal Data (Privacy) Ordinance (the "Ordinance").

10. During the investigation, the PCPD received several written replies from EC Healthcare. The PCPD also visited the office of EC Healthcare at Langham Place in Mong Kok to make inquiries with the representatives of EC Healthcare and obtain from them information pertinent to the cases. Additionally, the PCPD conducted site inspections at branches of two of the brands under EC Healthcare[3].

Findings and Contraventions

Background of EC Healthcare and the Integrated System Adopted by the Group

11. EC Healthcare expanded its business through acquisition and organic growth[4]. There are 39 brands[5] in total under EC Healthcare, which provides one-stop medical and health management services, including but not limited to general, specialist, dental and aesthetic medical cares.

12. Investigations reveal that as at 8 August 2022, 28[6] out of the 39 brands under EC Healthcare have adopted the integrated internal system of EC Healthcare (the "System"), which involved the data of approximately 1.08 million members.

13. The System was developed primarily for enhancing customer service by enabling frontline staff to provide one-stop and holistic medical and healthcare services for customers, respond to customers' inquiries, and handle complaints.

14. In general, customers of the 28 brands are required to fill in the membership form provided by EC Healthcare before using their services[7].

---

[3] See paragraphs 63 to 74 of the investigation report (Chinese version only)

[4] See Annex 1

[5] EC Healthcare holds the majority of shares of its 39 brands. Those brands operate in one of the following three models: (i) EC Healthcare acts solely as an investor. After acquiring the brands, there is no change to the brands' mode of operation (including the collection, use and processing of clients' personal data); (ii) Apart from being an investor, EC Healthcare may also provide various supporting services to the brands acquired, whereas the personal data held by the brands may be stored on EC Healthcare's technology platform; and (iii) EC Healthcare provides one-stop service, incorporates the brands in its membership programme, and applies its Privacy Policy to the brands.

[6] The 28 brands operate under models (ii) and (iii) described in footnote 5. See Annex 2.

[7] Membership enrolment is not required for one-off consumption at some of the healthcare brands, hair care brands and brands for cosmetic retail products.

To register as members, customers are asked to check the box to indicate their consent to the "EC Healthcare Privacy Policy"[8] (the "Privacy Policy"). Upon the completion of registrations, the personal data of the members will be stored in the System.

15. Besides, following the acquisition of various brands by EC Healthcare, the existing clients of such acquired brands (the "Existing Clients Before Acquisitions", including the Daughter and Complainant B) would automatically become members of EC Healthcare, and their personal data would be stored in the System.

The Incidents Involved "Personal Data" Defined under the Ordinance[9]

16. According to the information provided by the complainants and EC Healthcare to this office, when a frontline staff of any brands under EC Healthcare inputs the full phone number of a particular client or member into the System, the System can identify an individual who has registered as a member with that number. Then the staff can see that member's name, membership number and partial telephone number, etc. Moreover, the staff can also learn from the System what brands under EC Healthcare the client patronised and the record of purchases in the past, for example, what vaccinations and medical check-up the client had received.

17. In Case (1), apart from the names of the Daughter and the Grandmother, their membership numbers and partial telephone numbers, the search in the System also returned the diagnosis information of the Daughter in the remarks section. In Case (2), the search in the System returned not only the name, membership number and partial telephone number of Complainant B, but also the name of Complainant B's mother and the information of her insurance, which were shown in the remarks section.

18. The PCPD considers that, taken in its totality, it is practicable to directly or indirectly identify the client concerned from the above information. Therefore, such information constitutes "personal data" under the Ordinance.

---

[8] See Annex 3

[9] Under section 2(1) of the Ordinance, "personal data" is defined as any data relating to a living individual; in a form in which access to or processing of the data is practicable, and from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

EC Healthcare being the "Data User" in the Matters Complained of[10]

19. According to the information provided by EC Healthcare, the System is managed by EC Healthcare, which stores the personal data of clients of the 28 brands in the System and allows access and use by their frontline staff to clients' personal data across those 28 brands in order to achieve their purported purposes of providing the one-stop and holistic medical and healthcare services and improving customer services. Besides, those 28 brands adopt the uniform membership form and Privacy Policy of EC Healthcare in collecting clients' personal data.

20. Based on the above observations, EC Healthcare controls the storage and processing of personal data of clients of those 28 brands and its disclosure, transfer or use among their staff through the System. Thereafter, through the adoption of its uniform membership form and Privacy Policy, EC Healthcare also controls the collection of personal data of clients of those 28 brands.

21. According to the definition of "data user" under section 2(1) of the Ordinance, EC Healthcare is the data user in respect of the personal data of clients of 28 brands in the System.

Sharing, Disclosure and Use of Clients' Personal Data by The System

22. In both complaints, the personal data in question was collected years ago, and records of how such collection took place may not be available. Besides, there is no actual record in Case (1) to prove whether the Daughter's name was included in the text message. Notwithstanding the above, it is revealed from the information obtained during the investigations of both cases, the inquiries and the site visits conducted by the PCPD that the frontline staff of the 28 brands are able to make cross-brand access to and use of clients' personal data in the System. It did not involve unauthorised or accidental access to personal data, as it was indeed an intended arrangement of EC Healthcare for its business operation purposes.

23. As far as Case (1) is concerned, EC Healthcare confirmed that after the staff of Dr Reborn enter the Grandmother's phone number into the

[10] Under section 2(1) of the Ordinance, a "data user", in relation to personal data, means a person who either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

System, the information of both the Daughter and the Grandmother returned. According to the screen captures provided by EC Healthcare, the membership number, name and medical records of the Daughter would also be displayed. As regards Case (2), after the staff of re:HEALTH input Complainant B's phone number, the staff would know that Complainant B was also a member of EC Healthcare and could tell his full name, his consultation records at NYMG, as well as the name and insurance policy information of his mother. However, Complainant B had never provided the aforementioned information to re:HEALTH.

24. Thus, when a frontline staff of the 28 brands adopting the System checks the records of a particular client of its own brand, he/she could also read that client's records of using the services of other brands of EC Healthcare, including the personal data collected by those other brands. In other words, the System is featured with the sharing and transfer of clients' personal data, with the clients' personal data of one brand being disclosed to the staff of other brands for their access and use.

EC Healthcare Failed to Inform Existing Clients Before Acquisitions of the Possible Use of Their Personal Data

25. The Daughter and Complainant B were the Existing Clients Before Acquisitions [11] of Primecare and NYMG respectively prior to their acquisitions by EC Healthcare.

26. After the acquisitions, EC Healthcare stored the personal data of Existing Clients Before Acquisitions (including that of the Daughter and Complainant B) in the System. Hence, frontline staff of other brands under EC Healthcare using the System could access personal data of the relevant clients as well. However, since the acquisitions took place and over the course of the present investigations, EC Healthcare had never informed the Existing Clients Before Acquisitions of the relevant acquisitions by any means, nor provided them with the Privacy Policy of EC Healthcare. As such, Existing Clients Before Acquisitions were not informed that their personal data had been stored in the System and were accessible by the staff of other brands under EC Healthcare, and EC

[11] In June 2018, the Daughter first consulted Primecare, whereas in August 2019, EC Healthcare acquired equity interests of Primecare. On 18 March 2016, Complainant B first consulted NYMG, whereas on 11 November 2016, EC Healthcare acquired equity interests of NYMG.

Healthcare had never sought any consent from the Existing Clients Before Acquisitions in respect of such arrangement.

EC Healthcare Contravened Data Protection Principle 3(1)

27. Data Protection Principles 3(1) and (4) of Schedule 1 to the Ordinance stipulates that personal data, without the express and voluntary consent of the data subject, shall only be used (including disclosure and transfer) for the purpose for which the data was to be used at the time of the collection of the data, or a purpose directly related to that purpose.

28. Based on the information provided by EC Healthcare, Primecare at first collected the Daughter's personal data for the purpose of providing medical services, without explicitly stating the purpose of such collection of the data and the classes of persons to whom the data may be transferred. Meanwhile, upon the collection of Complainant B's personal data, NYMG had only informed Complainant B that the personal data collected would be used in the provision of treatment and dissemination of healthcare newsletters, without mentioning the classes of persons to whom the data may be transferred.

29. Subsequently, after acquiring Primecare and NYMG, EC Healthcare stored the personal data of the clients of these two brands (including those of the two complainants) in the System, and shared parts of their personal data among the 28 brands of EC Healthcare using the System, so that the relevant personal data were accessible by the frontline staff of various brands. As a result, the personal data originally provided by them to a single brand was disclosed and transferred, without their knowledge, to the staff of some other brands. The Privacy Commissioner for Personal Data (the "Commissioner") finds that the above arrangement was plainly inconsistent with the original purpose of collection of the complainants' personal data, and also fell short of their reasonable expectation for personal data privacy.

30. In addition, after acquiring Primecare and NYMG, EC Healthcare failed to obtain consents from the two complainants to the use, disclosure and transfer of their personal data among the various brands within the group, and never informed them by any means that their personal data would be stored in the System. Such practices are disappointing both from the perspective of compliance with legal requirements or that of respecting clients' wills.

31. In the circumstances, the Commissioner is of the opinion that EC Healthcare has contravened the requirements of Data Protection Principle 3(1) on the use (including disclosure and transfer) of personal data.

32. The Commissioner considers that, as an established listed company, EC Healthcare should possess adequate resources and capabilities to formulate comprehensive policies and operation plans (such as carrying out a Privacy Impact Assessment for the System), so as to ensure that the design of the System, and the policies and practices of sharing clients' personal data are in compliance with the requirements under the Ordinance. However, the two complaints reveal that in undertaking mergers and acquisitions for market consolidation, and in collating clients' personal data of its various brands through the System, EC Healthcare disregarded the requirements under the Ordinance on the use (including disclosure and transfer) of personal data and failed to duly consider how the operation of the System may impact clients' personal data privacy. The Commissioner expresses regret at the above shortcomings.

Enforcement Actions

33. The Commissioner is of the opinion that EC Healthcare has contravened Data Protection Principle 3(1) in Schedule 1 to the Ordinance, and hence she has exercised the powers conferred on her by section 50(1) of the Ordinance in serving an Enforcement Notice on EC Healthcare, directing it to take the following remedial actions to remedy and prevent recurrence of the relevant contraventions: -

(i) To cease and prohibit the sharing of clients' personal data among different brands under EC Health and/or the access by staff of any brand under EC Health to clients' personal data of any other brand(s) under EC Health through the System, unless EC Healthcare had explicitly stated such sharing of, and cross-brand access to personal data upon collection of personal data from the relevant clients, or obtained their consent thereafter to the sharing of, and cross-brand access to the data within the System (including any written consent or other forms of express consent);

(ii) In future, before integrating personal data of clients (including clients of the brands to be merged or acquired) into the System for sharing among or cross-brand access by the brands of EC Healthcare, to ensure that the personal data is originally collected, among other purposes, for the purpose of provision by EC Healthcare to its brands for sharing or cross-brand access by staff in the System. Otherwise, prior consent must have been obtained from clients to such use or sharing of their personal data (including written consent or any other forms of express consent);

(iii) In respect of managing clients' personal data of brands acquired through merger or acquisition, to formulate written policies to ensure that the requirements in paragraphs (i) and (ii) above would be properly executed, and to effectively and clearly convey the relevant policies to all staff responsible for or involved in handling the relevant personal data;

(iv) To provide training and formulate guidelines, instruct staff on the permissible use of and access to clients' personal data in the System, specify the access rights to the System assigned to staff of different ranks, ensure that they understand and acknowledge the relevant guidelines on access to clients' personal data of brands under EC Healthcare in the System, and enhance their awareness on personal data privacy protection; and

(v) To provide documentary proof to the Commissioner within three months from the date of the Enforcement Notice, proving that the instructions specified in (i) to (iv) above have been complied with.

Recommendations

34. Section 48(2)(a) of the Ordinance provides that the Commissioner may, after completing an investigation and if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation, any recommendations and other comments arising from the investigation as she thinks fit to make.

35. Before the publication of this investigation report, EC Healthcare has informed the PCPD that they have started working on the improvement measures and policies in relation to the collection and use of personal data within the group. The Commissioner would like to highlight that this investigation involved the personal data of a significant number of citizens. Therefore, apart from serving an Enforcement Notice pursuant to section 50(1) of the Ordinance, she would also like to make the following recommendations through this report to EC Healthcare and other groups which operate multiple brands.

Providing Clients with Clear and Concise Personal Information Collection Statement

36. As public expectation on personal data privacy protection grows, before their personal data would be collected, the public would expect to know the purpose of such collection and the classes of transferees to whom the data may be transferred. Public would also reasonably expect the purposes of use and disclosure of their personal data would be proportionate to the purposes of collection.

37. Data Protection Principle 1(3) in Schedule 1 to the Ordinance provides that on or before a data user collects personal data from a data subject, the data user shall take all practicable steps to inform the data subject whether it is obligatory or voluntary for him to supply the data. The data subject should also be informed of the purpose for which the data is to be used, the classes of transferees of the data, and their rights of access to and correction of personal data.

38. The Commissioner considers that EC Healthcare can make it clearer and more specific in their Privacy Policy to clients that their personal data would be disclosed and transferred to the staff of other brands under EC Healthcare for their access and use, for the purposes set out in the Privacy Policy (such as providing customer services and handling clients' complaints), thus reflecting the actual situation of how personal data of clients would be used in the System[12], and to ensure clients are providing their personal data informedly and voluntarily with knowledge of the relevant situation, in order to comply with the requirements under Data Protection Principle 1(3).

[12] The PCPD notes from the website of EC Healthcare that the Privacy Policy was updated on 7 October 2022.

39. Meanwhile, the Commissioner recommends EC Healthcare to standardize a set of uniform procedures for data collection by all its brands which use the System, ensuring that personal data of clients is stored by the staff in the System with their knowledge, in order to achieve fairness and transparency in the collection and use of the personal data.

Consents must be obtained from customers before using (including disclosing and transferring) their personal data for a new purpose

40. According to Data Protection Principle 3(1) and (4) of Schedule 1 to the Ordinance, organisations shall only use (including disclose and transfer) the personal data of its customers for the purpose for which the personal data was to be used at the time of collection or a directly related purpose. Unless any exemption under Part VIII of the Ordinance applies, organisations must first obtain the voluntary and express consents from their customers if they intend to use the personal data collected from their customers for a new purpose.

Assigning Rights of Access According to the Functions of Staff

41. The Commissioner recommends that, before assigning rights of access to and retrieval of personal data of clients in electronic systems to its staff, organisations must take into account the scope of business and the authorities of the relevant staff, and be prudent in making such arrangement. Besides, access control should form part of the policies on personal data handling, which should be clearly conveyed to relevant staff to prevent disclosure of personal data of clients to staff not authorised to handle such data.

42. The Commissioner recommends EC Healthcare to formulate clear written policies and guidelines on the operations and use of the System, which should cover the review of access rights assigned to staff of different ranks and specific explanations on permissible cross-brand access to records in the System and cautions that should be taken. In particular, it should be expressly provided that, without consent of the client, his/her personal data originally provided to one brand must not be disclosed to another brand.

Carrying Out a Privacy Impact Assessment

43. The Commissioner considers that as the System covers the personal data of various brands and involves a substantial number of clients, EC Healthcare should carry out a Privacy Impact Assessment [13] before launching the System, thoroughly review the initiative from the perspective of personal data privacy protection, carefully deliberate on the potential privacy risks involved, and adequately consider the impacts of the initiative on personal data privacy, so as to prevent any personal data privacy issues from arising.

44. The Commissioner emphasizes that organisations should carry out a Privacy Impact Assessment before the implementation of any plan that involves the handling of a considerable amount of personal data, rather than making retrospective reviews in the aftermath of incidents where personal data privacy problems had arisen. Besides, where there are significant changes in operational practices of an organisation, modifications to the manner of collection or use of personal data, and adoption of new technologies, organisations should consider conducting Privacy Impact Assessments on such plans to alleviate the privacy concerns of the public and stakeholders.

45. The Commissioner recommends that groups operating multiple brands should draw a lesson from this case. In the future, before planning or implementing any projects that involve the handling of a significant amount of personal data, they are strongly advised to carry out a Privacy Impact Assessment to holistically review their impact on and the risks to personal data privacy protection and to adopt adequate measures to address such impacts and risks so as to forestall or minimise the adverse effects, and to ensure that the groups are in compliance with the requirements under the Ordinance on the collection, retention, use and security of personal data.

Implementing Personal Data Privacy Management Programme

46. With the growing public awareness and expectations on personal data privacy protection, the Commissioner encourages organisations to

[13] For details, please refer to the "Privacy Impact Assessments (PIA)" published by the PCPD at: https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

implement a "Personal Data Privacy Management Programme" [14], embrace protection of personal data privacy as part of their corporate governance responsibilities, and adopt a top-down approach in executing open and transparent information policies and standing instructions, so as to signal their determination in exemplifying good corporate governance and gaining trust from their clients.

47. The Commissioner recommends organisations to formulate effective policies and procedures for the protection of personal data and adopt measures to monitor compliance with such policies and procedures on an ongoing basis.

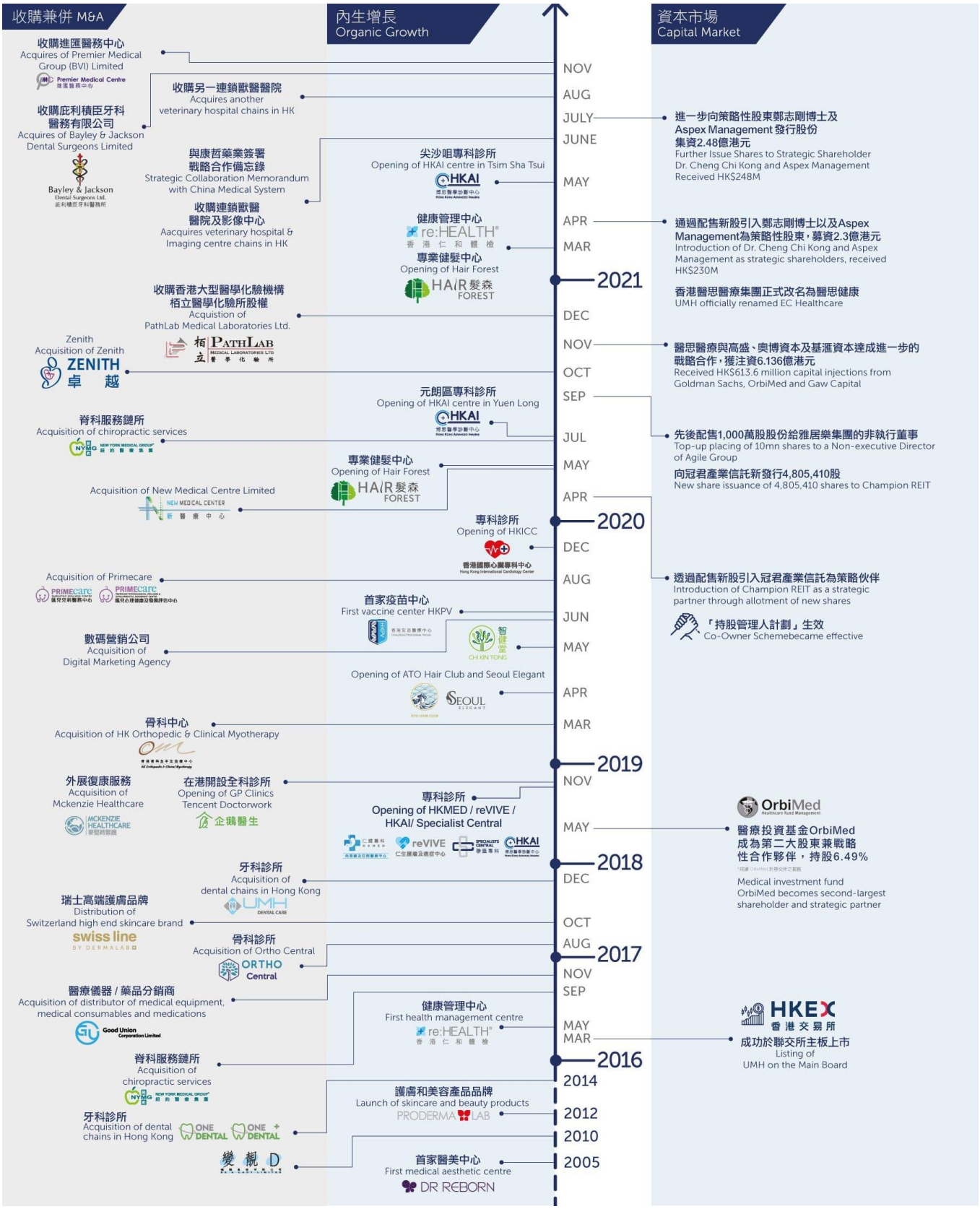
Appointing Data Protection Officer(s)

48. The Commissioner recommends that a Data Protection Officer reporting to the senior management be appointed to oversee compliance with the requirements under the Ordinance and the implementation of the "Personal Data Privacy Management Programme". Meanwhile, organisations should allocate resources to enhance staff awareness of personal data privacy protection, consistently implement personal data protection policies from the top down to the entire organisation, and develop a culture of respect for individual's privacy in relation to personal data.

[14] For details, please refer to "Privacy Management Programme — A Best Practice Guide" published by the PCPD at: https://www.pcpd.org.hk/english/publications/files/PMP_guide_e.pdf

Annex 1：the Milestone of the Development of EC Healthcare

（Extracted from EC Healthcare website on 16 June 2022[15]）



[15] https://www.echealthcare.com/zh/our-company/key-milestone/

Annex 2：28 Brands under EC Healthcare Using the System

1	Centre of Rehabilitation & Exercising Specialist (CORES)
2	Dermagic HK
3	Primecare Paediatrics Wellness Centre
4	Spine Central
5	Swissline
6	New York Medical Group
7	Hong Kong Orthopaedic & Clinical Myotherapy
8	laugh & Shine
9	Seoul Elegant
10	Vivid Eye Centre
11	“未来医生”
12	Āto Hair Club
13	DR REBORN
14	EC Dental Care
15	Hair Forest
16	Hong Kong Advanced Imaging (HKAI)
17	Young Aesthetics
18	reVIVE
19	Hong Kong Medical Endoscopy and Day Surgery Centre (HKMED)
20	Chi Kin Tong
21	AI Medical
22	Specialists Central
23	EC Healthcare Medical Centre
24	EC Specialists Central（PHF No. DP000104）
25	EC Specialists Premium（PHF No. DP000110）
26	re:HEALTH
27	Hong Kong International Cardiology Center (HKICC)
28	Hong Kong Professional Vaccine

Annex 3： “Privacy Policy of EC Healthcare”
Made by EC Healthcare

（Retrieved from EC Healthcare website on 7 September 2022[16]）

EC Healthcare refers to EC Healthcare and its subsidiary and affiliated entities, singly or together (hereinafter referred to as “**we**”, “**us**”, “**our**”, our “**Group**” or “**EC Healthcare**”), presents this “EC Healthcare Privacy Policy (the “**Privacy Policy**”). This Privacy Policy applies to all personally identifiable information that we may obtain from the following parties (whether currently or in the future): (i) data subject; (ii) third parties (data of which is related to products and services (collectively referred to as “**Products and Services**”, and individually as “**Products**” and “**Services**”) that have been indicated to us by interested individuals); and (iii) third parties who provide us with such Products and Services. This Privacy Policy does not apply to any personal data that is/are obtained by us for recruitment or employment related purposes.
fl

1. Methods of collection of personally identifiable information

EC Healthcare may collect your personally identifiable information via the following method(s):

- via the website operated by us, including https://echealthcare.com/ (i.e. the website where you are browsing such Privacy Policy), and other websites owned or controlled by EC Healthcare (collectively referred to as “**Websites**”);
- via software applications provided by us, used on or through computers and mobile devices (collectively referred to as “**Applications**”);
- via social media platforms controlled by us (collectively referred to as “**Social Media Platforms**”);
- via electronic mails that may be linked to this Privacy Policy, sent by us and/or any online or face-to-face communication between you and us;
- via third parties (e.g. authorized licensors, strategic business partners, landlords and franchisers) and other sources (e.g. public databases, marketing partners and relevant third parties)(collectively referred to as the “**Platforms**”)

2. Principles of collection of personally identifiable information

EC Healthcare respects the privacy of all individuals that use our Platforms. We endeavor to ensure that all our collection, transmission, storage and usage of personally identifiable information is carried out in compliance with the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of the Hong Kong Special Administrative Region (“**Hong Kong**”)) (hereinafter referred to as the “**Ordinance**”).

3. Types of personally identifiable information collected

The term “**personally identifiable information**” has the meaning as defined in the Ordinance. It refers to information that can identify you as an individual or associate you with an identifiable individual, including but not limited to your name, gender, age, and identification document number, phone number, fax number, residential address, email address, credit card information, education level, occupation, family income, hobbies and favorite activities, etc. Other information, such as your medical records, medial photos, medical images and medical reports, other product or service preferences, or the number of children; in the event that it is directly associated with any such personally identifiable information, shall be treated as personally identifiable information as subject to this Privacy Policy. You shall not be required to provide any personally identifiable information when you browse or use the Platforms. However, upon registration to use our Products and Services or online content, your personally identifiable information shall be collected by us to enable our provision. You may refuse to provide us with your personally identifiable information, but in this case, we may not be able to provide you with such Products and Services or online content. By providing your personally identifiable information to us, you are consenting to this Privacy Policy.

4. Purpose of collection and use of personally identifiable information (including but not limited to)

- identifying you and any accounts you hold with us
- enabling the provision of Products and Services to you (if you do not prefer to receive any administrative notices and communications, such as changes with respect to any account you hold with our Group or future changes with respect to this Privacy Policy, please write to us at Room 2107-08, 21/F., Office Tower, Langham Place, Mong Kok, Kowloon or send us an email at info@echealthcare.com)
- determining and verifying your eligibility for discounts and promotions on our Products and Services
- processing applications or renewal applications for our business partners’ products and services on your behalf
- processing insurance claims for our business partners’ products and services on your behalf
- processing of payment instructions or collection of amounts outstanding from you in relation to the provision of the Products and Services
- enabling us to store your personally identifiable information so as to prevent you from re-entering it each time you purchase and/or renew a Product or Service
- order processing, billing and fulfilment

[16] https://www.echealthcare.com/zh/our-company/key-milestone/

- direct marketing of our Products and Services (see section headed "**6. Direct Marketing**" below)
- direct marketing of the products and services of our business partners (see section headed "**6. Direct Marketing**" below)
- designing services for you
- conducting research, statistical analysis and behavioral analysis
- customer profiling and analyzing your purchasing preferences
- enabling you to participate in the interactive features of our Services, including identifying your friends or individuals, and sharing and communicating with them your shopping experience, when you choose to do so
- making suggestions and recommendations to you and other users of our Products and Services or goods and services that may interest you or them
- customizing our Platforms and its contents to your particular preferences
- provisioning of customer services
- handling your complaints and account enquiries, and handling any claim, action and/or proceedings against our Group or any party
- fraud prevention and detection
- auditing purposes
- making such disclosures as required by applicable laws, rules and regulations
- any other purposes directly related to the purpose for which the personally identifiable information was originally collected

Any questions, comments, suggestions or information other than personally identifiable information that is sent or posted to any part of our Platforms by you will be considered as voluntarily provided to our Group on a no-confidential and non-proprietary basis. We reserve the right to use, reproduce, disclose, transmit, publish and/or post elsewhere such information freely, including passing it to any associated company for example, in connection with the development and marketing of services and to meet user needs.

We may take your personally identifiable information and make it non-personally identifiable, either by combining it with information about other individuals (aggregating your information with information about other individuals), or by removing characteristics (such as your name) that make the information personally identifiable to you (de-personalising your personally identifiable information). We may use this non-personally identifiable information for, among other purposes, research and analysis to improve our Products and Services.

If you purchase our business partners' products or services including without limitation insurance products, your personally identifiable information will be transferred to that business partner and such information will be used, processed and stored in accordance with that business partner's privacy policy of which is outside our control. Please refer to the relevant privacy policy of our business partner.

If necessary, we may transfer your personally identifiable information to places outside of Hong Kong for carrying out the purposes, or the directly related purposes, for which the personally identifiable information is to be collected. All such transfers will be carried out in compliance with the requirements of the Ordinance.

5. With whom may we share your personally identifiable information as collected?

All personally identifiable information will be kept confidential, but we may disclose such information to third parties where such disclosure is necessary to fulfil one or more of the purposes described in section 4 of this Privacy Policy. A list of classes of persons (who may be located within or outside of Hong Kong) to whom your personally identifiable information may be transferred can be found at the List of Potential Transferees of Personally Identifiable Information as stated below.

From time to time, we may purchase a business or sell or more of our businesses (or portions thereof) and your personally identifiable information may be transferred as part of the purchase or sale. In the event that we purchase a business, the personally identifiable information received with that business would be treated in accordance with this Privacy Policy, if it is practicable and permissible to do so. In the event that we sell a business, we will include provisions in the selling contract requiring the purchaser to treat your personally identifiable information in the same manner required by this Privacy Policy (including any amendments to this Privacy Policy). In light of this protection, your opt-out choices stated in section 6 of this Privacy Policy shall not affect our right to transfer your personally identifiable information to a purchaser in these circumstances.

6. Direct Marketing

From time to time, the Group may use your personally identifiable information to send you news, offers, promotions and joint marketing offers and the Group requires your consent for that purpose. We may contact you by email, in-app notifications, social media, SMS, text/picture/video message, telephone or mail. Your name, email address, telephone number, contact address, social media contact, date of birth, Products and Services portfolio information, transaction patterns and behaviors, browsing records, content viewing habits and personal interests held by the Group may be used by the Group in direct marketing of our Products and Services and products and services offered by our business partners, including without limitation beauty, skincare and cosmetic products and services, which may be of interest to you.

You may decide to "opt in" to, or to "opt out" from, use by us of your personally identifiable information for promotional and marketing purposes. If you prefer not to receive any direct marketing communications from us, you can opt out at any time by updating your preferences through your registered account or an unsubscribed link as provided by us. You can also write to us or send us an email at the addresses as listed in section 4 above. Any such request shall state clearly the relevant personally identifiable information that you would like to opt out for. Upon receipt of the request, we shall cease to use your personally identifiable information for the purpose of direct marketing as soon as possible without extra charges.

7. Use of Cookies

A cookie is a small text file which is placed onto your computer (or other electronic device) when you access the Group's Websites and/or Applications. We use cookies on such Platforms to:

- recognize you whenever you visit the Websites
- obtain information about your preferences, viewing and browsing behaviour, online movements and use of the Internet
- keep track of the items stored in your account and take you through the checkout process
- carry out research and statistical analysis to help improve our Products and Services and to help us better understand our visitor and customer requirements and interests
- target our marketing and advertising campaigns and those of our business partners and advertisers more effectively by providing interest-based advertisements that are personalised to your interests
- make your online experience more efficient and enjoyable
- enable tighter security

The information we obtain from our use of cookies may not contain your personally identifiable information. Although we may obtain information about your computer or other electronic device such as IP address, browser settings, browsing records, and/or other Internet log information, this may not be able to identify you personally. To the extent that non-personally identifiable information is combined with personally identifiable information, we treat the combined information as personally identifiable information for the purposes of this Privacy Policy. In certain circumstances we may collect such personally identifiable information about you, but only where you voluntarily provide it by completing an online form, or where you purchase Products and Services from our Websites and/or Applications.

If you want to disallow the use of cookies, you can do so on your own web browser or electronic device. If you disable cookies, you acknowledge that you may not be able to use some of the functionality of our Websites and/or Applications.

8. Security measures taken to safeguard your personally identifiable information

The security and confidentially of your personally identifiable information is extremely important to us. We have implemented technical, administrative, and all reasonable and practicable measures to protect your personally identifiable information from any unauthorized access and improper use. From time to time, we review our security procedures in order to consider appropriate new technology and methods. Please be aware that despite our best efforts, no security measures are perfect or impenetrable.

9. Retention of your personally identifiable information

We will not keep your personally identifiable information longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the information is or is to be used. This means that, for example, personally identifiable information collected to fulfill your request for Products and Services will be erased, deleted, destroyed or anonymized after their delivery by using technical or other means to render such information unidentifiable or unusable, unless it is necessary to keep such information for other purposes and we have informed you of such other purposes at the time of collection of the personally identifiable information or obtained your consent.

10. Amendment(s) to this Privacy Policy

We may amend this Privacy Policy at any time. If we amend this Privacy Policy to permit material changes in the way we collect, use and/or share your personally identifiable information, we will notify you of such changes by sending you an email at the last email address that you provided to us, and/or by prominently posting notice of such changes on our Website at https://echealthcare.com/. Any such material changes to this Privacy Policy will be effective thirty (30) calendar days following either our dispatch of an email notice to you or our posting of notice of the changes on our Website. Any material changes to this Privacy Policy may affect our use and sharing of personally identifiable information that we collected before our notification to you of the said changes. If you do not wish to permit material changes in our collection, use or sharing of your personally identifiable information collected by us before the effective date of such changes, you must so notify us before that effective date by writing to us or sending an email to us at the addresses listed in section 4 above. Please be advised, however, that, regardless of whether you provide such notice to us, the changes to this Privacy Policy shall apply to any personally identifiable information collected by us on or after the effective date of such changes.

11. Questions and/or comments with respect to this Privacy Policy

If you have any questions or wish to send us any comments, about this Privacy Policy, or wish to complain to us, correct, access a copy of or cease the use of your personally identifiable information, please write to us at the address listed in section 4 above or send us an email at info@echealthcare.com. You may also call us at our Customer Services Enquiry at (+852) 8203 0058 during business hours. In the event that any of your questions, comments, complaints and/or demands relates to and/or involve such illegal or inaccurate information, please understand that we may not be able to process such requests. Nonetheless, we shall follow up within reasonable time upon receipt of your questions, comments, complaints and/or demands.

Our Group reserves the right to charge you a reasonable fee for complying with a data access request as permitted by the Ordinance.

The terms of this Privacy Policy are governed by and interpreted in accordance with the Laws of Hong Kong.

In the event of any discrepancy or inconsistency between the English and Chinese versions of this Privacy Policy, the English version shall prevail.

Date of Last Revision: 02 Feb 2021

List of Potential Transferees of Personally Identifiable Information

Parties to whom personal identifiable information collected by us may be transferred:

1. Governments, law enforcement authorities, courts and tribunals.
2. Legal and other professional advisors, insurers, loss adjustors, rehabilitation service providers.
3. Any third party whom you have authorized to obtain your personally identifiable information from the Group, including without limitation agents, contractors or third party service providers who provide Products and/or Services to us or have any form of business partnership with us.