APHM
Persatuan Hospital Swasta Malaysia
Association of Private Hospitals of Malaysia

KOD AMALAN

UNTUK HOSPITAL SWASTA DALAM INDUSTRI JAGAAN KESIHATAN

(Menurut Seksyen 23 Akta Perlindungan Data Peribadi 2010)

Disediakan oleh
PERSATUAN HOSPITAL SWASTA MALAYSIA
SELAKU FORUM PENGGUNA DATA
UNTUK HOSPITAL SWASTA

Kandungan

		Muka surat
KOD AMALAN UNTUK HOSPITAL SWASTA		31
1.	Pengenalan	34
2.	Status dan Keterterapan	34
3.	Tafsiran	35
4.	Pelaksanaan Prinsip Perlindungan Data di Persekitaran Hospital Swasta	37
	Gambar rajah menunjukkan aliran data di Hospital Swasta dari pengumpulan awalan DP daripada SD sehingga DP dimusnahkan	37
5.	Hak Subjek Data	52
6.	Isu Spesifik	56
7.	Pekerja	59
8.	Isu Pematuhan Lain	59
9.	Kajian Semula Kod	60
10.	Kesimpulan	60

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

No. Ruj.
CoP_K(a)

PADA menjalankan kuasa yang diberikan oleh Seksyen 23(3) Akta Perlindungan Data Peribadi 2010 (Akta 709), saya dengan ini mendaftarkan Tataamalan bagi Golongan Pengguna Data Kesihatan (subperenggan (a)) dan terpakai kepada semua pengguna data di bawah Golongan tersebut berkuatkuasa serta-merta.

Bertarikh pada: 31 Disember 2020

(MAZMALEK BIN MOHAMAD)
Pesuruhjaya Perlindungan Data Peribadi, Malaysia

1. PENGENALAN

1.1 Kod ini disediakan oleh Persatuan Hospital Swasta Malaysia (Association of Private Hospitals of Malaysia atau "APHM") menurut Seksyen 23(1)(a) Akta Perlindungan Data Peribadi 2010 ("APDP"). APHM telah dilantik sebagai Forum Pengguna Data untuk Hospital Swasta oleh Pesuruhjaya Perlindungan Data Peribadi ("PPDP") menurut Seksyen 21 APDP.

1.2 Kod ini disediakan dengan kerjasama Pesuruhjaya Perlindungan Data Peribadi.

1.3 Kod ini terpakai kepada semua kemudahan jagaan kesihatan swasta yang **berlesen** sebagai **Hospital Swasta** di bawah *Akta Kemudahan & Perkhidmatan Jagaan Kesihatan Swasta 1998,* (**"PHFSA" (Akta 586)**) yang dianggap sebagai "Pengguna Data" bagi tujuan APDP ini.

1.4 Skop Kod

Kod ini bertujuan untuk memastikan pematuhan Prinsip Perlindungan Data seperti yang dinyatakan dalam APDP untuk keadaan unik yang dihadapi oleh Hospital Swasta. Memandangkan APDP hanya menyediakan "Prinsip" untuk pematuhan, Kod ini disasarkan untuk menyediakan beberapa panduan yang jelas kepada pematuhan prinsip yang dinyatakan selagi prinsip ini terpakai untuk Hospital Swasta.

2. STATUS DAN KETERTERAPAN

2.1 Kod ini mengawal selia Pemprosesan Data Peribadi dan Data Peribadi Sensitif daripada Subjek Data di Hospital Swasta.

2.2 Kod ini juga bertujuan untuk memastikan hak Subjek Data berkenaan dengan Data Peribadi seimbang dengan keperluan Hospital Swasta untuk memproses Data Peribadi dalam menyediakan perkhidmatan perubatan dan perkhidmatan yang berkaitan kepada Subjek Data.

2.3 **"Subjek Data"** atau Pihak Berkepentingan di bawah Kod ini akan terdiri daripada:

a. Pesakit yang ingin mendapatkan rawatan perubatan di Hospital Swasta;
b. Petugas Hospital (jururawat, doktor dan kakitangan sokongan);
c. Pakar Perubatan atau Perunding Perubatan;
d. Penyedia Perkhidmatan untuk Hospital Swasta (termasuk kontraktor, vendor dsb.);
e. Orang yang Berkaitan (Waris Terdekat, Penjaga dsb. seperti yang ditetapkan dalam APDP)
f. Pelawat biasa di Hospital Swasta;

2.4 Keperluan Pematuhan

2.4.1 Kod ini tidak bertujuan untuk mengganti APDP. Semua peruntukan dalam APDP akan terus terpakai untuk semua Hospital Swasta (sebagai Pengguna Data) kecuali peruntukan di dalam APDP yang telah diubah suai, dipertingkatkan atau digantikan oleh peruntukan dalam Kod ini.

2.4.2 Subjek Data tidak akan dianggap telah melanggar Kod ini atau APDP jika mereka telah diwajibkan untuk mematuhi mana-mana undang-undang lain yang terpakai yang memberi kesan kepada penjagaan kesihatan am dan khususnya, Hospital Swasta.

2.4.3 Subjek Data juga hendaklah mematuhi mana-mana **Standard APDP** yang ditetapkan oleh Pesuruhjaya PDP dari masa ke semasa yang mengawal selia beberapa Prinsip APDP.

2.5 Kod ini akan berkuat kuasa sebaik sahaja didaftarkan oleh Pesuruhjaya PDP.

2.6 Kod ini telah diderafkan dalam Bahasa Inggeris. Sebarang percanggahan antara versi Bahasa Inggeris Kod ini dengan versi Bahasa Malaysia (atau apa-apa versi terjemahan lain), versi Bahasa Inggeris akan diguna pakai.

2.7 Bagi tujuan untuk mengelakkan keraguan sekiranya terdapat percanggahan antara:
(a) Kod ini;
(b) Standard APDP yang ditetapkan oleh Pesuruhjaya PDP;
(c) Peruntukan dalam APDP;
(d) Garis panduan dan Kod Majlis Perubatan Malaysia (MPM);
(e) Apa-apa Standard lain yang telah ditetapkan oleh Kementerian Kesihatan atau mana-mana agensi kerajaan yang berkaitan;
(f) Apa-apa undang-undang yang spesifik yang memberi kesan kepada mana-mana Prinsip APDP; yang mempunyai kesan secara langsung kepada pemprosesan Data Peribadi oleh Pengguna Data, maka kaedah atau dokumen yang menetapkan standard yang lebih tinggi untuk pematuhan akan diguna pakai.

2.8 Gambar rajah dan contoh di dalam Kod ini hanya bertujuan sebagai panduan sahaja.

2.9 Senarai penzahiran yang dibenarkan kepada pihak ketiga seperti yang dinyatakan dalam **Lampiran A** tidak menyeluruh dan Pengguna Data dikehendaki mematuhi Kod ini dan Prinsip Penzahiran (Seksyen 8 APDP) pada setiap masa.

3. TAFSIRAN

Dalam Kod ini, kecuali konteks telah menjelaskan sebaliknya, perkataan-perkataan yang telah ditafsirkan akan mempunyai makna seperti berikut:

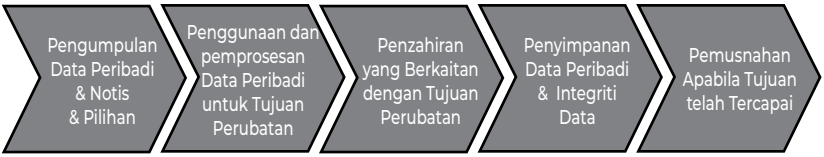
Perkataan	Maksud
Mengumpul	berhubung dengan data peribadi, ertinya perbuatan yang melaluinya data peribadi itu termasuk ke dalam atau berada di bawah kawalan seorang Pengguna Data sama ada pada lawatan pertama atau pada setiap lawatan susulan Subjek Data ke Hospital Swasta
Menzahirkan	berhubung dengan data peribadi, ertinya perbuatan yang melaluinya Data Peribadi itu disediakan kepada pihak ketiga oleh Pengguna Data sebagai sebahagian daripada Tujuan Perubatan dalam rawatan untuk Subjek Data.
Pemproses Data	berhubung dengan data peribadi, ertinya mana-mana orang atau entiti, selain pekerja Pemproses Data yang memproses Data Peribadi itu semata-mata untuk pihak Pengguna Data, dan tidak memproses Data Peribadi untuk tujuan persendiriannya. Sebagai contoh, makmal swasta pihak ketiga, pusat data, perkhidmatan awan dan penyedia storan yang menyediakan perkhidmatan kepada Pengguna Data.

Pengguna Data	ertinya, Hospital Swasta yang memproses Data Peribadi atau mempunyai kawalan ke atas atau memberi kebenaran pemprosesan apa-apa Data Peribadi tetapi tidak termasuk Pemproses Data; Dalam Kod ini, istilah "Pengguna Data" dan "Hospital Swasta" akan digunakan saling bertukar ganti.
Subjek Data	bermaksud, seseorang individu yang menjadi subjek Data Peribadi, dan bagi maksud Kod ini merujuk kepada pesakit, pekerja dsb. yang mana Data Peribadi itu diproses sebagai sebahagian daripada Tujuan Perubatan itu dan tujuan lain yang berkaitan.
Persetujuan yang Nyata	bermaksud, apa-apa permintaan Subjek Data yang diberi dengan sukarela, spesifik, termaklum dan petunjuk yang jelas, melalui kenyataan atau tindakan pengesahan yang jelas, menandakan persetujuan kepada pemprosesan data peribadi berkaitan dengan mereka.
Perkhidmatan Jagaan Kesihatan	seperti yang ditetapkan dalam Akta Kemudahan dan Perkhidmatan Jagaan Kesihatan Swasta 1998 [Akta 586]
Profesional Jagaan Kesihatan	bermaksud, pengamal perubatan, pengamal pergigian, ahli farmasi, ahli psikologi klinikal, jururawat, bidan, pembantu perubatan, ahli fisioterapi, jurupulih pekerjaan dan profesional jagaan kesihatan lain yang berkaitan dan mana-mana orang yang terlibat dalam menyediakan perkhidmatan perubatan, kesihatan, pergigian, farmasi dan apa-apa Perkhidmatan Jagaan Kesihatan lain di bawah bidang kuasa Kementerian Kesihatan yang merupakan pekerja atau dalam kontrak perkhidmatan di Hospital Swasta.
Persetujuan Termaklum	Proses dan bentuk yang digunakan oleh Profesional Jagaan Kesihatan atau Pakar Perubatan untuk menerangkan kepada pesakit/Subjek Data tentang tujuan, manfaat, dan potensi risiko dalam intervensi perubatan atau pembedahan, termasuk ujian klinikal, dan kemudiannya mendapatkan persetujuan pesakit/Subjek Data untuk menerima rawatan atau mengambil bahagian dalam ujian itu.
Peranti Perubatan	Hendaklah mempunyai maksud yang sama seperti yang dinyatakan dalam Akta Peranti Perubatan 2012.
Tujuan Perubatan	termasuk tujuan perubatan pencegahan, diagnosis perubatan, penyelidikan perubatan, rehabilitasi dan peruntukan penjagaan dan rawatan, dan pengurusan perkhidmatan penjagaan kesihatan (dalam erti kata lain, merangkumi pemprosesan menyeluruh Data Peribadi Subjek Data sebagai sebahagian daripada rawatan perubatan yang diberikan kepada Subjek Data)
Pakar atau Perunding Perubatan	pengamal perubatan atau pengamal pergigian di bawah kontrak untuk perkhidmatan dengan Hospital Swasta
Waris Terdekat	bermaksud ahli keluarga terdekat yang masih hidup, termasuk pasangan, anak, ibu bapa dan dalam beberapa kes termasuk adik-beradik seseorang itu.
Hospital Swasta	bermaksud hospital swasta dan pusat perubatan yang berlesen di bawah PHFSA (Akta 586).

Pemprosesan	berkaitan dengan Data Peribadi, ini bermaksud mengumpul, merekod, penggunaan, penzahiran dan menyimpan Data Peribadi termasuk, (a) mengurus, penyesuaian atau pengubahan Data Peribadi; (b) penemuan kembali, perundingan atau penggunaan Data Peribadi; (c) penzahiran Data Peribadi melalui penyiaran, pemindahan, penyebaran atau dengan cara lain yang boleh mendapatkannya; atau (d) penjajaran, penggabungan, pembetulan, pemadaman atau pemusnahan Data Peribadi.
Orang yang Berkaitan	berkaitan dengan Subjek Data, walauapapun yang dinyatakan, bermaksud, (a) dalam kes di mana Subjek Data adalah orang yang dibawah umur 18 tahun, ibu bapa, penjaga atau orang yang mempunyai hak penjagaan ke atas subjek data; (b) dalam kes di mana Subjek Data adalah seorang yang tidak berupaya untuk menangani urusan mereka sendiri, seseorang akan dilantik oleh mahkamah untuk menangani urusan-urusan itu, atau seseorang yang diberi kuasa secara bertulis oleh Subjek Data untuk bertindak bagi pihak Subjek Data.
Peminta	berkaitan dengan permintaan akses data atau permintaan pembetulan data, yang bermaksud Subjek Data atau Orang yang Berkaitan bagi pihak Subjek Data, yang telah mengemukakan permintaan itu.
Data Peribadi Sensitif	bermaksud apa-apa Data Peribadi yang mengandungi maklumat seperti, (a) keadaan kesihatan fizikal atau mental seseorang Subjek Data, (b) pendapat politiknya, (c) pegangan agama atau kepercayaan lain yang seumpamanya, (d) Pelakuan Subjek Data atau apa-apa kesalahan atau dituduh melakukannya
Pihak Ketiga	berkaitan dengan Data Peribadi yang diproses oleh Hospital Swasta, bermaksud mana-mana orang atau entiti yang di luar skop atau kawalan Hospital Swasta yang berkemungkinan menyediakan perkhidmatan untuk Hospital Swasta itu.
Penggunaan	berkaitan dengan Data Peribadi di Hospital Swasta yang bermaksud penggunaan Data Peribadi itu untuk semua Tujuan Perubatan
Kepentingan Vital	bermaksud hal berkaitan dengan nyawa, kematian atau keselamatan Subjek Data.

4) <u>PENERAPAN PRINSIP PERLINDUNGAN DATA DALAM PERSEKITARAN HOSPITAL SWASTA</u>

Berikut ialah gambar rajah yang menunjukkan aliran data di Hospital Swasta dari permulaan pengumpulan Data Peribadi daripada Subjek Data sehingga Data Peribadi dimusnahkan.



4.1 Prinsip Perlindungan Data

APDP menyatakan bahawa pemprosesan Data Peribadi oleh Pengguna Data hendaklah mematuhi Prinsip Perlindungan Data Peribadi yang berikut. Penerapan Prinsip ini akan dilakukan menurut aliran data yang ditunjukkan di atas.:

(a) Prinsip Am (yang melibatkan persetujuan);
(b) Prinsip Notis dan Pilihan;
(c) Prinsip Penzahiran;
(d) Prinsip Keselamatan;
(e) Prinsip Penyimpanan;
(f) Prinsip Integriti Data; dan
(g) Prinsip Akses

Perlu diambil perhatian bahawa ini hanyalah sekadar prinsip, manakala jenis dan kaedah pematuhan untuk Pemprosesan Data Peribadi sesuatu industri terpulang kepada Pengguna Data. **Justeru, tujuan Kod ini adalah untuk menetapkan amalan pematuhan yang unik khusus untuk Hospital Swasta.**

4.2 Prinsip Am – Persetujuan (Seksyen 6 APDP)

4.2.1 Di bawah Prinsip Am, **persetujuan** mesti diperoleh daripada Subjek Data untuk Pemprosesan Data Peribadi di persekitaran Hospital Swasta kecuali Pemprosesan itu melibatkan salah satu keadaan yang dinyatakan dalam Seksyen 6(2) APDP, yang tidak memerlukan persetujuan.

4.2.2 Untuk Data Peribadi Sensitif, Pengguna Data mesti mendapatkan **"Persetujuan Eksplisit"** daripada Subjek Data. **Data Peribadi Sensitif** yang ditakrifkan dalam APDP bermaksud:

(a) Keadaan kesihatan fizikal atau mental Subjek Data;
(b) Pendapat politik Subjek Data;
(c) pegangan agama atau kepercayaan lain yang seumpamanya Subjek Data;
(d) tuduhan pelakuan akan apa-apa kesalahan oleh Subjek Data.

4.2.3 Pengguna Data tidak boleh memproses Data Peribadi kecuali,

(a) Data Peribadi itu diproses untuk tujuan yang sah dan berkaitan secara langsung dengan aktiviti Pengguna Data.
(b) Pemprosesan Data Peribadi itu adalah perlu untuk atau berkait secara langsung dengan tujuan Data Peribadi itu; dan
(c) maklumat Data Peribadi adalah mencukupi dan tidak berlebihan untuk tujuan Data Peribadi itu

Dalam hal ini, Pengguna Data mesti memastikan bahawa semua Borang Hospital Swasta telah disemak untuk mengeluarkan pengumpulan apa-apa maklumat peribadi yang berlebihan dan tidak diperlukan untuk Tujuan Perubatan dan tujuan lain yang berkaitan.

4.2.4 Data Peribadi yang dikumpulkan daripada Subjek Data (Pesakit, Pekerja dan lain-lain) termasuk yang berikut tetapi tidak terhad kepada:

(a) Nama
(b) Alamat
(c) Nombor Kad Pengenalan/Pasport
(d) Tarikh Lahir
(e) Tempat Kelahiran
(f) Jantina
(g) Bangsa
(h) Agama
(i) Pekerjaan
(j) Status Perkahwinan
(k) Kewarganegaraan
(l) Nombor Telefon
(m) Alamat E-mel
(n) Maklumat Waris Terdekat/Penjaga ("Orang yang Berkaitan")
(o) Maklumat Kad Kredit
(p) Kelayakan Pendidikan (untuk pekerja)
(q) Kelayakan Profesional untuk Petugas dan Pakar Perubatan
(r) Rekod Perubatan dan maklumat lain yang berkaitan
(s) Maklumat Biometrik (sepert cap jari)
(t) Profail DNA
(u) Gambar dan Video
(v) Maklumat Doktor Keluarga
(w) Dan lain-lain maklumat yang boleh digunakan untuk mengenal pasti Subjek Data dan menyediakan perkhidmatan penjagaan kesihatan yang diperlukan oleh Pengguna Data.

4.2.5 Dalam keadaan Subjek Data secara sukarela memberi Data Peribadi mereka kepada Pengguna Data untuk tujuan yang dinyatakan, dan dalam Kod ini ialah Tujuan Perubatan, ini akan diterima sebagai Persetujuan Eksplisit untuk Pemprosesan Data Peribadi mereka bagi Tujuan Perubatan dan tujuan yang berkaitan perubatan.

4.2.6 Dalam keadaan Subjek Data tidak berupaya untuk memberi persetujuan (sebagai contoh dia tidak berupaya atau cedera) semasa waktu pendaftaran, persetujuan ini boleh diperoleh sebaik sahaja dia sedar atau daripada Orang yang Berkaitan.

4.2.7 Dalam kes individu bawah umur (seperti seseorang itu di bawah umur lapan belas tahun) atau dalam keadaan Subjek Data tidak berupaya untuk memberi Persetujuannya, maka Persetujuan itu boleh diberikan oleh "Orang yang Berkaitan".

4.2.8 Dalam kes Data Peribadi Orang yang Berkaitan dan pihak lain yang berkaitan yang akan dihubungi sekiranya berlaku kecemasan (di mana Subjek Data kehilangan upaya atau tidak boleh memberi persetujuan), Hospital Swasta akan beranggapan bahawa Subjek Data telah memperolehi Persetujuan daripada mereka untuk Hospital Swasta memproses Data Peribadi mereka bagi tujuan perhubungan.

4.2.9 Apabila Hospital Swasta memproses data pesakit, Persetujuan ini akan dianggap telah diberi untuk "Tujuan Perubatan". Gambaran untuk Aliran data dalam Hospital Swasta ditunjukkan dalam gambar rajah berikut:

4.2.10 Apa-apa pengumpulan dan pemprosesan Data Peribadi daripada pesakit untuk tujuan bukan perubatan akan memerlukan persetujuan tambahan. Jenis persetujuan ini akan diperlukan untuk aktiviti seperti penggunaan Data Peribadi untuk penyelidikan perubatan, ujian perubatan dan aktiviti pemasaran Pengguna Data, yang tidak berkaitan dengan Tujuan Perubatan.

4.2.11 Peraturan PDP memperuntukkan bahawa "persetujuan" mesti diperoleh dalam apa-apa kaedah yang boleh direkodkan dan disenggarakan oleh Pengguna Data seperti:

(a) Menanda tangani borang pendaftaran
(b) Mengklik petak dalam borang mengesahkan persetujuan (Pilih-Bersetuju)
(c) Persetujuan Tersirat (sebagai contoh: persetujuan yang diberikan melalui orang yang diberi kuasa, atau)
(d) Melalui perlakuan atau perbuatan (sebagai contoh: melalui telefon)
(e) Apa-apa dokumen secara bertulis yang lain

4.2.12 Hospital Swasta hendaklah pada setiap masa mendapatkan persetujuan daripada Subjek Data secara "Pilih-Bersetuju" dan bukan menggunakan kaedah "Pilih-Tidak Bersetuju". (Sebagai contoh: Dalam mana-mana borang hospital, Subjek Data akan dikehendaki untuk menandakan petak yang bertulis: "tandakan petak ini jika anda TIDAK mahu menerima bahan promosi").

4.2.13 Data Peribadi dikumpulkan oleh Pengguna Data melalui saluran berikut di persekitaran Hospital Swasta tetapi tidak terhad kepada:

(a) Borang pendaftaran pesakit (pesakit luar atau pesakit dalam);
(b) Borang permohonan pekerjaan (untuk kakitangan, jururawat, doktor dsb.);
(c) Daripada mana-mana pihak ketiga yang berkaitan dengan pesakit seperti ibubapa/penjaga, majikan/bakal majikan, ejen (contoh. ejen pelancongan perubatan), syarikat insurans, kemudahan penjagaan kesihatan yang lain.
(d) Borang prosedur perubatan spesifik (pembedahan dan prosedur lain) yang boleh mengandungi Borang Persetujuan Termaklum;
(e) Borang Kaji Selidik Maklum Balas;
(f) Borang Kemas Kini Maklumat;
(g) Borang Permohonan Penyelidikan Klinikal;
(h) Surat Perjanjian antara Pakar Perubatan dan Pengguna Data;
(i) Borang Permohonan Akses;
(j) Imej yang direkodkan melalui Kamera Litar Tertutup/CCTV atau media elektronik lain;
(k) Maklumat atau dokumen lain yang dikemukakan oleh Subjek Data secara bertulis, melalui telefon, secara elektronik melalui E-mel atau melalui laman sesawang korporat Pengguna Data; dan

(l) Data Peribadi telah diperoleh sebagai sebahagian daripada peranan Pengguna Data selaku Pemproses Data untuk pihak ketiga (iaitu Pengguna Data menyediakan perkhidmatan teleradiologi, kemudahan makmal dsb.)

4.2.14 Berikut ialah contoh-contoh situasi yang merangkumi Tujuan Perubatan yang mana persetujuan boleh diberikan secara eksplisit atau di mana pengecualian boleh diberikan kepada kewajipan persetujuan;

(a) Data Peribadi diberikan oleh Subjek Data secara sukarela dengan mengisi borang pendaftaran pesakit. borang maklum balas, borang kemas kini maklumat dan apa-apa komunikasi seumpamanya kepada Hospital Swasta, dan akan diterima sebagai "persetujuan eksplisit" daripada Subjek Data untuk Pemprosesan Data Peribadinya dengan tujuan mendapatkan rawatan perubatan di Hospital Swasta itu.

(b) Proses rawatan perubatan yang melibatkan pengumpulan dan pemprosesan Data Peribadi boleh merangkumi aktiviti berikut:

i. pemeriksaan oleh Pakar Perubatan atau Perunding Profesional Jagaan Kesihatan;
ii. penyediaan rawatan sebagai pesakit luar atau pesakit dalam;
iii. ujian diagnostik yang sedang dijalankan seperti x-ray, Imbas CT, ultrabunyi, ujian makmal dsb.;
iv. prosedur pembedahan yang sedang dijalankan (di mana Pengguna Data mendapatkan Persetujuan Termaklum yang lebih lanjut untuk pembedahan itu);
v. perbincangan kes antara Pakar Perubatan atau Profesional Jagaan Kesihatan di Hospital Swasta itu atau daripada Hospital lain;
vi. pemerolehan insurans, berurusan dengan pertubuhan penjagaan terurus, majikan atau penjamin pihak ketiga untuk menanggung kos rawatan.
vii. berurusan dengan ejen pemungut hutang dan peguam untuk mendapatkan semula kos-kos perkhidmatan jagaan kesihatan yang telah diberikan kepada Subjek Data;
viii. perundingan susulan; dan
ix. perkongsian lain bagi Data Peribadi yang berkaitan dengan rawatan perubatan Subjek Data itu.

4.3 Prinsip Notis dan Pilihan (Seksyen 7 APDP)

4.3.1 APDP menghendaki Pengguna Data untuk memaklumkan kepada Subjek Data tujuan pengumpulan, penggunaan dan penzahiran Data Peribadi individu itu dan mendapatkan persetujuan mereka yang perlu direkodkan dan disenggarakan melainkan apa-apa pengecualian yang berkaitan dengan Seksyen 6(2) APDP diguna pakai.

4.3.2 Pengguna Data mesti memaklumkan, mendedahkan atau mempamerkan Notis PDP mereka kepada Subjek Data semasa pengumpulan atau sebaik sahaja yang boleh dilaksanakan selepas itu.

4.3.3 Notis PDP mesti mengandungi maklumat berikut:

(a) bahawa Data Peribadi kepada Subjek Data itu sedang diproses oleh atau bagi pihak Pengguna Data dan mengemukakan butiran Data Peribadi itu:

Contoh:
Data Peribadi itu diproses oleh Hospital Swasta atau Pemproses Data yang diberi kuasa oleh pihak Hospital Swasta seperti Pakar perubatan, Makmal Luar dsb.

(b) tujuan Data Peribadi itu dikumpulkan atau akan dikumpulkan dan diproseskan selanjutnya dengan persetujuan Subjek Data. Ini termasuk Tujuan Perubatan dan tujuan yang berkaitan;

Contoh Termasuk:
- Data Peribadi dikumpulkan dan diproses untuk Tujuan Perubatan dan perkhidmatan jagaan kesihatan yang berkaitan
- Untuk mewujudkan dan menguruskan rekod perubatan dan laporan perubatan
- Untuk memudahkan proses pembayaran berkaitan dengan pesakit
- Untuk memulakan tindakan pemulihan hutang terhadap mereka yang gagal membuat pembayaran.
- Untuk melaporkan data peribadi kepada pihak berkuasa yang berkaitan dan/atau pihak ketiga di bawah undang-undang yang dikuatkuasakan berkaitan dengan industri jagaan kesihatan
- Untuk berkongsi data peribadi dengan syarikat pemegangan kumpulan dan syarikat yang berkaitan (mana-mana yang diperlukan) seperti yang dinyatakan dalan Akta Syarikat 2016
- Untuk menjalankan penyelidikan, analisis dan penambahbaikan
- Untuk pemasaran dan pengiklanan produk dan perkhidmatan
- Untuk memudahkan keperluan peribadi pesakit luar negara (sebagai contoh: permohonan visa)
- Untuk mentadbir dan memberikan maklum balas kepada permohonan, pertanyaan, aduan dan isu perundangan
- Untuk memudahkan aktiviti pengurusan sumber manusia yang berkaitan dengan pekerja
- Untuk penyerahan dan pendaftaran borang yang berkaitan, pelesenan dengan pihak berkuasa kawal selia yang berkaitan dan/atau pihak ketiga di bawah mana-mana undang-undang yang dikuatkuasakan berkaitan industri jagaan kesihatan
- Untuk berkongsi data peribadi bagi tujuan kemudahan perbankan, nasihat perundangan dan audit
- Untuk pendidikan dan latihan (dengan menganonimkan Data Peribadi di mana-mana yang boleh)
- Untuk apa-apa tujuan lain yang secara kebetulan atau untuk pelanjutan tujuan-tujuan di atas

(c) Apa-apa maklumat yang tersedia untuk Pengguna Data sebagai sumber Data Peribadi;

(d) Hak Subjek Data untuk meminta akses kepada dan untuk meminta pembetulan Data Peribadi itu;

(e) Maklumat perhubungan Pegawai Pematuhan atau Pegawai Perlindungan Data Hospital Swasta itu untuk apa-apa pertanyaan atau aduan berhubung dengan Data Peribadi itu;
(f) kategori Pihak Ketiga yang mana Pengguna Data mendedahkan atau mungkin dedahkan Data Peribadi itu, (sebagai contoh: vendor pihak ketiga yang menyediakan perkhidmatan kepada Pengguna Data dalam proses menyediakan Perkhidmatan Perubatan, seperti makmal luar, syarikat insurans dsb.);
(g) pilihan dan kaedah yang ditawarkan oleh Pengguna Data kepada Subjek Data dalam mengehadkan pemprosesan Data Peribadi, termasuk Data Peribadi yang berkaitan dengan orang lain yang boleh dikenal pasti daripada Data Peribadi itu;
(h) sama ada pembekalan Data Peribadi oleh Subjek Data adalah wajib atau secara sukarela;
(i) dalam keadaan pembekalan Data Peribadi oleh Subjek Data adalah wajib, kesannya akan diterima oleh Subjek Data jika mereka gagal membekal Data Peribadi itu.

4.3.4 Apabila Notis akan dikeluarkan. Notis PDP itu hendaklah diberikan seberapa segera yang boleh dilaksanakan oleh Pengguna Data:

(a) apabila Subjek Data di minta sejak dari mula oleh Pengguna Data untuk mengemukakan Data Peribadinya;
(b) apabila Data Peribadi untuk Subjek Data itu dikumpulkan buat kali pertama oleh Pengguna Data seperti yang dinyatakan dalam perenggan 3.2.14;
(c) atau dalam apa-apa kes yang lain, sebelum Pengguna Data itu, (i) menggunakan Data Peribadi daripada Subjek Data itu untuk tujuan selain tujuan sebenar Data Peribadi itu dikumpulkan; atau (ii) mendedahkan Data Peribadi itu kepada pihak ketiga.

4.3.5 Kaedah penyampaian Notis PDP. Notis PDP kepada Subjek Data boleh disampaikan melalui satu atau lebih kaedah yang berikut:

(a) Dengan menghantar salinan bercetak ringkasan notis itu kepada Subjek Data semasa pendaftaran pertama sebagai pesakit atau apabila melapor diri sebagai pekerja atau sebagai pakar di Hospital Swasta atau sebaik sahaja selepas itu;
(b) Dengan memaparkan ringkasan notis di tempat utama di Hospital Swasta (sebagai contoh: di papan tanda elektronik dan poster);
(c) Secara lisan menerangkan kepada Subjek Data sebelum mengumpul Data Peribadi di sepanjang proses rawatan di Hospital Swasta;
(d) Secara lisan menerangkan kepada Subjek Data sebelum menjalankan prosedur perubatan khas yang memerlukan persetujuan eksplisit (contoh: untuk pembedahan dan prosedur lain yang tidak terkandung dalam persetujuan am).
(e) Dengan mengarahkan Subjek Data ke Laman Sesawang Pengguna Data.

4.3.6 Notis PDP ini hendaklah diberikan dalam Bahasa Melayu dan Bahasa Inggeris.

4.4 Prinsip Penzahiran (Seksyen 8 APDP)

4.4.1 Penzahiran Data Peribadi milik Subjek Data terhad kepada tujuan dan tujuan yang berkaitan yang telah memperolehi persetujuan asal di bawah Prinsip Notis dan Pilihan.

4.4.2 Tidak ada Data Peribadi yang boleh didedahkan untuk apa-apa tujuan lain kecuali:

(a) Bagi tujuan yang memerlukan penzahiran Data Peribadi semasa pengambilan, yang mana dalam urusan Hospital Swasta, hendaklah merangkumi semua aktiviti berkaitan dengan Tujuan Perubatan; atau

> Contoh: Ini akan melibatkan semua aktiviti-aktiviti berkaitan dengan peruntukan rawatan perubatan, termasuk pemeriksaan, perundingan, diagnostik, ujian makmal, rawatan, pembedahan, pemprosesan pembayaran dsb.

(b) tujuan yang secara langsung berkait dengan tujuan asal;
(c) kepada mana-mana pihak selain pihak ketiga yang dikategorikan sebagai pihak ketiga dalam Lampiran B. Senarai ini akan dikemaskinikan secara berkala oleh Pengguna Data.

4.4.3 Had penzahiran selanjutnya Data Peribadi yang di luar persetujuan yang telah diberikan oleh Subjek Data untuk tujuan asal semasa pengumpulan. Penzahiran seperti ini boleh dilakukan di dalam keadaan seperti berikut:

(a) Subjek Data telah memberikan persetujuan mereka untuk penzahiran itu;
(b) Bagi tujuan mengesan jenayah atau untuk tujuan siasatan:

> Contoh 1: Untuk mengesan kecurian peralatan dan bekalan hospital, Pengguna Data menzahirkan Data Peribadi pekerja atau pesakit kepada penyiasat atau kepada Polis

(c) Diperlukan atau dibenarkan oleh atau di bawah mana-mana undang-undang:

> Contoh: Keadaan di mana Hospital dikehendaki untuk menzahirkan maklumat kepada Kementerian Kesihatan dalam kes penyakit yang wajib dilaporkan.

(d) Pengguna Data telah bertindak dengan keyakinan yang munasabah bahawa mereka berhak di sisi undang-undang untuk menzahirkan Data Peribadi itu kepada orang lain:
(e) Pengguna Data telah bertindak dengan keyakinan yang munasabah bahawa mereka telah mendapat persetujuan daripada Subjek Data, jika Subjek Data telah mengetahui keadaan yang menyebabkan penzahiran itu:
(f) Penzahiran itu diwajarkan sebagai kepentingan awam seperti yang ditentukan oleh Menteri;
(g) Penzahiran yang diizinkan seperti yang diperlukan oleh agensi kerajaan, keperluan undang-undang atau perintah mahkamah.

4.5 Prinsip Keselamatan (Seksyen 9 APDP)

4.5.1 Di bawah Prinsip Keselamatan, Pengguna Data hendaklah mengambil **"langkah-langkah yang praktikal"** untuk melindungi Data Peribadi daripada kehilangan, penyalahgunaan, pengubahsuaian, akses tanpa kebenaran atau tidak sengaja atau penzahiran, pengubahan atau kemusnahan semasa memproses Data Peribadi.

4.5.2 **"Langkah Praktikal"** tidak ditakrifkan dalam APDP, walau bagaimanapun Pengguna Data hendaklah mengambil langkah fizikal dan elektronik yang mencukupi untuk melindungi Data Peribadi. Tahap keselamatan yang diperlukan untuk Data Peribadi yang diproses di persekitaran Hospital Swasta adalah tinggi memandangkan sebahagian besar pemprosesan ini melibatkan Data Peribadi Sensitif.

4.5.3 Langkah fizikal dan elektronik yang perlu diambil oleh Pengguna Data mestilah berdasarkan pada:

(a) Tempat atau lokasi Data Peribadi itu disimpan:

Ini adalah penting khususnya jika Data Peribadi disimpan di luar premis Hospital, seperti Storan Awan, maka protokol komunikasi tersulit selamat mesti dilaksanakan apabila menghantar dan menerima Data Peribadi dari lokasi itu.

(b) Langkah-langkah keselamatan yang telah digabungkan dalam mana-mana kelengkapan tempat Data Peribadi itu disimpan:

1. Keseluruhan Sistem IT di dalam Hospital perlu dilengkapkan dengan tembok api yang mencukupi, anti-virus dan perisian anti-pencerobohan yang lain.
2. Perhatian yang khusus mesti diberikan kepada peranti Diagnostik seperti Imbas CT, Ultrabunyi, X-Ray, pelayan storan dsb, yang menyimpan data pesakit untuk memastikan yang peranti ini mempunyai perlindungan yang mencukupi daripada penzahiran yang tidak disengajakan atau akses yang tidak dibenarkan.
3. Sekali lagi, perhatian yang khusus harus diberikan dalam pemberian kebenaran untuk akses jauh kepada vendor dan penyedia perkhidmatan pihak ketiga yang lain untuk sistem IT hospital (khususnya peranti Diagnostik).

(c) Langkah yang diambil untuk memastikan kebolehpercayaan, integriti dan kecekapan kakitangan di Hospital Swasta yang mempunyai akses kepada Data Peribadi:

1. Hospital perlu memastikan bahawa semua kakitangan hospital telah dilatih secukupnya dalam melindungi keselamatan dan integriti Data Peribadi.
2. Semua kakitangan yang mempunyai akses kepada sistem IT mesti diberi pendidikan tentang kepentingan memastikan keselamatan Data Peribadi terjamin. Hospital perlu memastikan protokol akses dikawal ketat berdasarkan maklumat yang perlu diketahui sahaja.

(d) Langkah yang diambil untuk memastikan pemindahan terkawal Data Peribadi:

1. Pergerakan fizikal Rekod Perubatan di dalam Hospital harus dilakukan dalam keadaan terkawal. Sebagai contoh, Rekod Perubatan hendaklah dibawa dalam karung gelap yang tertutup apabila dipindahkan dari Bilik Rekod Perubatan ke klinik masing-masing.
2. Jika Data Peribadi disimpan di dalam awan, maka pemilihan penyedia perkhidmatan awan dan protokol komunikasi mestilah selamat

4.5.4 Langkah Keselamatan lain yang perlu diambil oleh Pengguna Data untuk melindungi Data Peribadi. Berikut hanyalah standard minimum dan Pengguna Data perlu diberikan kebebasan untuk menggabungkan langkah yang dipertingkatkan untuk melindungi Data Peribadi yang diproses

(a) Proses Pentadbiran diperkukuhkan melalui Dasar APDP:
- (i) Latihan yang kerap dan berterusan dalam perlindungan data untuk semua pekerja, Profesional Jagaan Kesihatan dan mana-mana yang berkaitan untuk Pakar Perubatan;
- (ii) Kaedah mengendalikan Data Peribadi di setiap jabatan di Hospital Swasta dan khususnya di Klinik Pakar;
- (iii) Pergerakan fizikal Data Peribadi di dalam dan di luar Hospital Swasta (harus melibatkan pergerakan Rekod Perubatan dari Bilik Rekod Perubatan dan di seluruh kawasan Hospital Swasta);
- (iv) Protokol Akses untuk menentukan pihak yang mendapat akses kepada Data Peribadi pesakit/ Subjek Data di seluruh Hospital Swasta;
- (v) Akses kepada Data Peribadi pesakit/ Subjek Data oleh Pakar Perubatan yang mempunyai beberapa klinik di hospital yang lain;
- (vi) Dasar yang ketat dalam penggunaan peranti storan mudah alih seperti pemacu USB. Jika perlu, kelulusan mesti diperoleh daripada Ketua Pegawai Maklumat Hospital Swasta itu (Chief Information Officer atau "CIO") atau mana-mana kakitangan Hospital Swasta yang diberi kuasa.

(b) Langkah Elektronik untuk melindungi Data Peribadi:
- (i) Semua komunikasi yang mengandungi Data Peribadi mesti disulitkan;
- (ii) Memasang tembok api yang mencukupi, perisian anti pencerobohan dan takrif virus yang terkini;
- (iii) Semua peranti elektronik mesti dilindungi dengan menggunakan kata laluan (contoh: Komputer Riba, peranti diagnostik, i-pad dsb);
- (iv) Kawalan Akses kepada Sistem Maklumat Hospital (HIS) yang dilengkapi jejak audit;
- (v) Sandaran lengkap untuk semua Data Peribadi yang telah diproses oleh Hospital Swasta di tempat yang jauh daripada premis hospital;
- (vi) Dasar pemulihan bencana dan kesinambungan perniagaan mesti disediakan;
- (vii) Menghadkan penggunaan peranti storan mudah alih untuk memindahkan Data Peribadi dan hanya dibolehkan jika diberikan kebenaran oleh CIO atau pengurusan atasan yang lain.

(c) Langkah Fizikal
- (i) Akses ke pintu bilik tempat Data Peribadi disimpan hendaklah dikawal ketat;
- (ii) Rekod Perubatan Fizikal perlu disimpan di dalam bilik yang terkawal dan akses ke bilik itu dihadkan kepada hanya petugas yang menguruskan Rekod Perubatan sahaja;
- (iii) Pergerakan Rekod Perubatan hendaklah di dalam beg atau kotak yang tertutup;
- (iv) Semua fail perubatan, rekod dan maklumat lain harus disimpan jauh daripada pandangan pesakit dan pihak ketiga yang lain apabila mereka berada di stesen jururawat;
- (v) Menyediakan sistem sandaran data untuk semua data HIS di satu lokasi di luar Hospital Swasta itu sebagai mekanisme pemulihan bencana;
- (vi) Memasang Kamera Litar Tertutup di kawasan yang strategik di Hospital Swasta untuk menghalang pencurian Data Peribadi.

(d) Langkah Tambahan yang perlu diambil oleh Pengguna Data untuk memastikan keselamatan termasuk:
- (i) langkah keselamatan fizikal untuk mencegah akses tanpa kebenaran;
- (ii) proses akses dan kebenaran untuk memastikan hanya pengguna yang sah sahaja mempunyai akses kepada rekod perubatan dan setiap pengguna mempunyai tahap akses yang sewajarnya kepada Rekod Perubatan;
- (iii) penyenggaraan log audit untuk menyokong kesahihan penambahan kepada Rekod Perubatan;
- (iv) perlindungan untuk mana-mana bahagian Rekod Perubatan elektronik daripada dihapuskan;
- (v) format baca sahaja untuk dokumen luar yang disimpan dalam Rekod Perubatan;
- (vi) perlindungan yang mencukupi apabila Rekod Perubatan dizahirkan kepada penyedia penjagaan kesihatan atau pesakit;
- (vii) sandaran yang kerap untuk Rekod Perubatan, sebaik-baiknya setiap hari untuk pesakit dalam;
- (viii) perlindungan virus yang mencukupi untuk memastikan Rekod Perubatan tidak diubah suai atau dimusnahkan oleh faktor luar;
- (ix) rancangan luar jangka untuk pemulihan bencana dan serangan penafian perkhidmatan;
- (x) memastikan tidak ada perkakasan yang mengandungi maklumat pesakit yang boleh dikenal pasti secara peribadi sebelum dimusnahkan dengan sempurnanya;
- (xi) keselamatan yang dipertingkatkan, sebagai contoh, proses penyulitan atau pengesahihan tambahan apabila rangkaian menjadi lebih terdedah seperti peranti tanpa wayar dan capaian jauh, atau di mana kelengkapan yang menyimpan maklumat berada dalam pemacu yang berisiko kehilangan atau kecurian seperti komputer riba, pemacu USB, tablet dan i-Pad dsb.

4.5.5 Pemproses Data

Apabila Data Peribadi diproseskan oleh Pemproses Data bagi pihak Pengguna Data, Pengguna Data hendaklah memastikan bahawa, (i) Pemproses Data memberikan jaminan yang secukupnya berhubung langkah teknikal dan keselamatan organisasi yang mengawal selia pemprosesan itu dan (ii) mengambil langkah sewajarnya untuk memastikan pematuhan langkah-langkah itu.

Contoh Pemproses Data:
a. Pakar Perubatan di Hospital;
b. Pusat Data Sumber Luar;
c. Makmal Luar yang menyediakan perkhidmatan diagnostik;
d. Khidmat Sumber Manusia dari Sumber Luar.

Beberapa langkah berhemat yang boleh diambil oleh Pengguna Data sebelum menggunakan khidmat Pemproses Data termasuk:

(a) Memastikan pemeriksaan pra perjanjian Pemproses Data dilakukan untuk memastikan yang berikut:

(i) Pemproses Data mempunyai dasar dan prosedur yang mencukupi untuk menyimpan dengan selamat Data Peribadi untuk Pengguna Data;
(ii) Mempunyai kawalan akses yang ketat ke atas Data Peribadi milik Pengguna Data itu dengan hanya memberikan akses atas dasar perlu-tahu sahaja;
(iii) Premis Data Peribadi itu selamat daripada apa-apa ancaman siber;
(iv) Mempunyai protokol sandaran bagi memastikan kesinambungan perniagaan untuk Pengguna Data dikekalkan;
(v) Bahawa mereka telah menggabungkan dalam kemudahan mereka semua aspek perlindungan teknikal dan elektronik yang berhemat untuk melindungi Data Peribadi yang diamanahkan kepada mereka;
(vi) Mereka mempunyai pelindungan yang mencukupi khususnya dalam aspek penggunaan, keselamatan, penyimpanan dan pemusnahan Data Peribadi.

(b) Apabila didapati bahawa Pemproses Data telah mematuhi dengan (a) di atas, Pengguna Data itu perlu membuat satu perjanjian rasmi dengan Pemproses Data yang meliputi isu berikut:

(i) peruntukan untuk ketakdedahan yang kukuh;
(ii) mengemukakan aku janji bahawa kemudahan mereka mempunyai anti-virus, tembok api yang terkini dan perisian anti-pencerobohan yang terkemas kini;
(iii) hak untuk mengaudit sistem keselamatan mereka secara tetap;
(iv) hak untuk memeriksa dasar mereka berkaitan dengan pengstoran dan pemprosesan Data Peribadi termasuk hak akses kepada pekerja mereka;
(v) menggabungkan penyulitan dalam semua penyampaian dan penerimaan Data Peribadi;
(vi) fungsi sandaran dan pemulihan dan protokol yang jelas untuk memastikan kesinambungan perniagaan;
(vii) Hak untuk membuat tuntutan ganti rugi atas kerugian yang akibatkan kehilangan Data Peribadi dalam simpanan mereka;
(viii) Kewajipan untuk melaporkan pencerobohan data di pusat kemudahan data Pemproses Data kepada Pengguna Data dalam tempoh satu (1) jam setelah menyedari tentang pencerobohan itu;

4.6 Prinsip Penyimpanan (Seksyen 10 APDP)

4.6.1 APDP menyatakan bahawa Data Peribadi yang telah diproses bagi apa-apa tujuan tidak boleh disimpan lebih lama daripada yang diperlukan bagi memenuhi maksud Data Peribadi itu.

4.6.2 Prinsip penyimpanan ini tidak menetapkan apa-apa tempoh yang tertentu, tetapi untuk Hospital Swasta, hal ini akan ditadbir urus menurut standard Industri Jagaan Kesihatan, PHFSA (Akta 586) dan undang-undang lain yang berkaitan termasuk amalan industri seperti yang dinyatakan dalam Fasal 3.6.5 di bawah.

4.6.3 Di bawah Akta Had Masa 1953, tindakan yang berasaskan kontrak (antara lain) mesti dikemukakan dalam tempoh 6 tahun dari tarikh kausa tindakan itu terakru. Justeru, Pengguna Data boleh meminta untuk menyimpan rekod yang berkaitan dengan kontraknya selama 7 tahun dari tarikh penamatan kontrak itu dan berkemungkinan untuk tempoh yang lebih panjang jika terdapat siasatan atau tindakan undang-undang yang dimulakan dalam tempoh itu.

4.6.4 Peruntukan untuk undang-undang khusus yang lain berhubung penyimpanan Data Peribadi tidak akan memberi kesan kepada prinsip penyimpanan APDP. Tempoh penyimpanan yang dinyatakan dalam Akta-akta ini termasuk: Akta Perkhidmatan Kewangan 2013, Akta Had Masa 1953, Akta Cukai Pendapatan 1967 dsb. hendaklah dipatuhi oleh Pengguna Data;

4.6.5 Tempoh Penyimpanan lazim untuk Hospital Swasta adalah seperti yang ditunjukkan dalam Jadual di bawah. Walau bagaimanapun, tempoh ini mungkin berubah tertakluk kepada undang-undang spesifik, amalan industri atau keperluan pengawalseliaan lain yang ditetapkan.:

No.	Jenis Kegunaan Data Peribadi	Tempoh Penyimpanan
1	Data Peribadi Pesakit	7 tahun untuk dewasa dan 25 tahun untuk yang baru lahir dikira dari tarikh terakhir rawatan mereka
2	Data Peribadi Pekerja	Selama tempoh pekerjaan dan 7 tahun selepasnya
3	Data Peribadi Pelawat	Tidak lebih daripada 3 bulan
4	Data CCTV	30-60 hari kecuali diperlukan sebagai bahan bukti untuk siasatan jenayah
5	Tindakan Undang-Undang (Sivil atau jenayah)	Sehingga penutupan siasatan dan perbicaraan dan apa-apa Rayuan selepasnya
6	Penyimpanan yang diperlukan menurut Undang-Undang	Menyimpan Data Peribadi melebihi tempoh berkaitan dibenarkan seperti yang ditetapkan oleh undang-undang
7	Penyimpanan pada Media Elektronik atau pelayan	Penyimpanan Data Peribadi melebihi tempoh yang dinyatakan dibolehkan jika keselamatan Data Peribadi dapat dipastikan sepanjang tempoh itu. Walau bagaimanapun, Pengguna Data mesti berhati-hati jika menggunakan Data Peribadi yang lama kerana Data Peribadi itu berkemungkinan tidak dikemaskinikan atau tidak tepat untuk pemprosesan yang selanjutnya

8	Penyimpanan Borang fizikal yang mengandungi Data Peribadi setelah dimasukkan secara digital dan ditukarkan kepada format elektronik	Penyimpanan salinan cetak seharusnya untuk tempoh maksimum selama 30 hari kecuali diperlukan untuk tujuan undang-undang, cukai dan tujuan statutori yang lain. Jika salinan cetak ini disimpan, keselamatan salinan ini mestilah dijaga.
9	Data Peribadi Tanpa Nama	Data Peribadi seperti ini boleh disimpan tanpa sekatan selagi data ini TIDAK boleh dikenal pasti sebagai Data Peribadi

4.6.6 Pemusnahan Data Peribadi. Prinsip am menetapkan bahawa Pengguna Data mesti mengambil langkah yang munasabah bagi memastikan Data Peribadi itu dimusnahkan atau dipadamkan secara kekal jika tidak diperlukan lagi untuk tujuan Data Peribadi itu diambil. Hospital Swasta hendaklah mematuhi garis panduan yang dikeluarkan oleh KKM – "Jadual Pelupusan Rekod Perubatan 2016".

4.6.7 ***Pemusnahan*** akan dilaksanakan untuk salinan cetak dokumen yang mengandungi Data Peribadi. Bagi Hospital Swasta pula, hal ini akan merujuk kepada beberapa borang yang digunakan di Hospital itu. (contoh: Pendaftaran, prosedur perubatan, log pelawat dan pengumpulan sementara yang lain bagi Data Peribadi seperti Kurikulum Vitae pekerja). Sebaik sahaja Data Peribadi yang diperoleh melalui borang-borang ini dipindahkan ke dalam pelayan data dan disimpan dalam format elektronik, Data Peribadi ini boleh dipertimbangkan untuk pemusnahan kecuali salinan cetak diperlukan untuk disimpan bagi tujuan spesifik seperti yang dinyatakan sebelum ini.

4.6.8 **Pemadaman kekal** akan dilaksanakan untuk Data Peribadi yang disimpan dalam medium elektronik (seperti pemacu keras dan pemacu USB, Komputer Riba, mesin X-ray, mesin Imbas CT dsb.)

4.6.9 Pemusnahan Data Peribadi dan Data Peribadi Sensitif yang diambil dan diproses di Hospital Swasta memerlukan kaedah khas untuk pemusnahan dan pemadaman yang termasuk;

(a) Pembakaran dokumen dan media elektronik (Data Peribadi dan Data Peribadi Sensitif)
(b) Mencincang dokumen kertas yang mengandungi Data Peribadi yang biasa dan sementara;
(c) Melantik firma pakar untuk mencincang dokumen-dokumen yang mengandungi Data Peribadi/Data Peribadi Sensitif di premis Hospital Swasta dan tidak dipindahkan ke tempat lain
(d) Data Peribadi yang disimpan dalam media elektronik harus dipadamkan dengan menggunakan teknologi terkini seperti penyahgaussan bermagnet;
(e) Pemacu keras lama daripada komputer peribadi harus dimusnahkan secara fizikal atau dihancurkan.

4.6.10 Anonimisasi Data Peribadi

Hospital Swasta selaku Pengguna Data akan dianggap telah berhenti daripada menyimpan Data Peribadi apabila Data Peribadi itu tidak lagi mempunyai kegunaan untuk dihubungkaitkan dengan mana-mana Subjek Data – iaitu Data Peribadi itu telah tidak ada nama. Anonimisasi dalam Data Peribadi ini adalah kaedah yang disyorkan apabila data diperlukan untuk penyelidikan, pendidikan atau untuk kegunaan yang tidak memerlukan maklumat yang boleh dikenal pasti.

4.7 Prinsip Integriti Data (Seksyen 11 APDP)

4.7.1 Pengguna Data hendaklah mengambil langkah yang munasabah bagi memastikan Data Peribadi itu tepat, lengkap, tidak mengelirukan dan sentiasa dikemaskinikan dengan mengambil kira tujuan, termasuk apa-apa tujuan yang terlibat secara langsung yang menyebabkan Data Peribadi itu dikumpul dan diproses selanjutnya.

4.7.2 Berikut akan diambil kira sebagai langkah yang munasabah di Hospital Swasta untuk memastikan Data Peribadi itu tepat, lengkap, tidak mengelirukan dan sentiasa dikemaskinikan.

(a) Membenarkan Subjek Data mengisi sendiri borang permohonan dan borang lain;
(b) Mengumpul Data Peribadi secara muat naik Elektronik (seperti Kad Pengenalan);
(c) Mempunyai prosedur untuk menggalakkan Subjek Data mengemaskinikan Data Peribadi mereka jika terdapat perubahan, sebagai contoh status perkahwinan, alamat, pertukaran agama dsb.
(d) Memastikan bahawa Data Peribadi dikemas kini setiap kali Subjek Data mengunjungi Hospital Swasta.

4.7.3 Prinsip Integriti Data tidak memerlukan Pengguna Data untuk mengesahkan atau menjamin ketepatan atau kesempurnaan Data Peribadi itu tetapi hanya perlu mengambil langkah yang munasabah.

4.7.4 Dalam keadaan yang melibatkan Individu Bawah Umur atau Subjek Data tidak upaya, Pengguna Data itu boleh meminta ahli keluarga atau saudara-mara mengemukakan Data Peribadi pesakit/Subjek Data itu dan untuk mengemas kini maklumat tersebut seperti yang dikehendaki.

4.8 Prinsip Akses (Seksyen 12 & Seksyen 30 APDP)

4.8.1 Subjek Data berhak meminta akses kepada Data Peribadi mereka dan meminta pembetulan dibuat. Dalam hal ini, Pengguna Data hendaklah menyediakan satu Borang Permintaan Akses dalam bentuk fizikal atau dalam talian (satu sampel Borang Permintaan Akses dilampirkan sebagai Lampiran B).

Di bawah Prinsip Akses, Pengguna Data dikehendaki:

(a) memberi akses kepada Subjek Data untuk Data Peribadi mereka yang disimpan oleh Pengguna Data apabila suatu permintaan dan pembayaran fi yang telah ditetapkan atau apa-apa fi yang dibenarkan oleh Pesuruhjaya; dan
(b) Hak untuk membetulkan kesilapan Data Peribadi itu jika Data Peribadi itu tidak tepat, tidak lengkap, mengelirukan atau tidak kemas kini.
(c) Fi yang ditetapkan untuk Permintaan Akses

Hospital yang menerima Permintaan Mengakses Data boleh mengenakan fi untuk setiap Permintaan Akses Data. Fi maksimum yang boleh dikenakan adalah seperti yang dinyatakan dalam Peraturan Perlindungan Data Peribadi (Fi) 2013 seperti yang dinyatakan di bawah:

Butiran	Perihal	Fi Maksimum (RM)
1	Permintaan Akses Data untuk Data Peribadi milik Subjek Data dengan satu salinan	10
2	Permintaan Akses Data untuk Data Peribadi milik Subjek Data tanpa salinan	2
3	Permintaan Akses Data untuk Data Peribadi Sensitif milik Subjek Data dengan satu salinan	30
4	Permintaan Akses Data untuk Data Peribadi Sensitif milik Subjek Data tanpa salinan	5

4.8.2 Semua Pengguna Data harus memastikan hak untuk kebenaran kepada Akses ini dinyatakan dengan jelas dalam Dasar Privasi dan menyediakan juga Borang Permintaan Akses secara dalam talian.

5. HAK SUBJEK DATA

5.1 Hak Akses Peminta untuk Mengakses Data Peribadi (Seksyen 30 APDP)

Peminta boleh membuat permintaaan untuk mengakses data secara bertulis kepada Pengguna Data setelah membayar fi yang ditetapkan untuk maklumat Data Peribadi milik Subjek Data yang sedang diproses oleh atau bagi pihak Pengguna Data itu dengan syarat Peminta;

a. telah mengemukakan kepada Pengguna Data atau Pemproses Data (mana-mana yang berkenaan) borang persetujuan Subjek Data yang memberi kuasa atau melindungi Pengguna Data atau Pemproses Data untuk mengeluarkan/atau membetulkan Data Peribadi milik Subjek Data itu; dan
b. memastikan satu salinan Data Peribadi milik Subjek Data itu akan diberi kepada Subjek Data dalam bentuk yang boleh difahami setelah menerima salinan tersebut daripada Pengguna Data atau Pemproses Data (mana-mana yang berkenaan).

5.2 Hak untuk Mengakses Rekod Perubatan[1]

5.2.1 Rekod Perubatan ialah maklumat yang telah didokumentasikan tentang kesihatan Subjek Data yang direkodkan oleh Profesional Jagaan Kesihatan, sama ada dengan sendiri atau di atas arahan mereka. Rekod ini mengandungi maklumat yang mencukupi untuk mengenal pasti Subjek Data/Pesakit itu, menyokong diagnosis berdasarkan sejarahnya, pemeriksaan dan siasatan fizikal, mewajarkan pengurusan profesional yang diberikan, merekod tindakan dan keputusannya selepas itu, dan memastikan kesinambungan penjagaan yang telah diberikan oleh Profesional Jagaan Kesihatan yang bertugas kepada Subjek Data tersebut.

5.2.2 Rekod Perubatan ialah catatan butiran untuk Profesional Jagaan Kesihatan yang merawat pesakit dan komponen penting kepada penjagaan pesakit. Rekod ini, dalam satu bahagian, mengandungi maklumat tentang pesakit itu, manakala satu bahagian lagi mengandungi pendapat doktor dan pertimbangan klinikal yang menjadi sandaran untuk pengurusan pesakit itu. Berdasarkan konsep ini, Rekod Perubatan telah dianggap sebagai dokumen “sulit” dan maklumat yang terkandung di dalamnya dianggap “peribadi” dalam mematuhi etika hubungan doktor dan pesakit.

[1] *Garis panduan MPM tentang Rekod Perubatan dan Laporan Perubatan*

5.2.3 Telah lama ditetapkan bahawa Rekod Perubatan ialah hak milik Pengguna Data/Hospital Swasta, tetapi Subjek Data mempunyai hak akses kepada maklumat yang terkandung dalam rekod itu. Maklumat peribadi (nama, alamat, data pengenalan, dsb.) yang telah direkodkan oleh Profesional Jagaan Kesihatan ialah milik pesakit.

Subjek Data boleh mendapat akses untuk pelbagai tujuan yang merangkumi keperluan untuk mendapatkan pendapat kedua daripada hospital atau doktor lain, untuk mendapatkan rawatan lanjutan di tempat lain, atau untuk tujuan undang-undang. Dengan persetujuan Subjek Data, hak akses ini diberikan juga kepada ejen, penjaga atau Orang yang Berkenaan yang dilantik oleh Subjek Data itu.

5.2.4 Kandungan Rekod Perubatan Subjek Data/Pesakit

Berikut ialah butiran intelek dan fizikal yang boleh secara keseluruhan atau sebahagiannya dijadikan sebagai kandungan Rekod Perubatan Subjek Data/Pesakit itu:

(i) Maklumat Peribadi Pesakit (diperoleh seperti yang dibincangkan sebelum ini)
(ii) Catatan klinikal doktor (catatan yang ditulis semasa berjumpa dengan pesakit atau selepas itu)
(iii) Rakaman Perbincangan dengan pesakit/Orang yang Berkenaan berhubung penyakit/pengurusan (dengan saksi)/Pita Rakaman boleh digunakan untuk perbincangan seperti ini
(iv) Catatan Rujukan untuk pakar-pakar lain untuk perundingan/ pengurusan bersama
(v) Laporan Makmal & Histopatologi
(vi) Rekod dan laporan pengimejan
(vii) Gambar Klinikal
(viii) Preskripsi Ubat-ubatan
(ix) Laporan Jururawat
(x) Borang Persetujuan, Borang Discaj Dari Hospital Atas Risiko Sendiri
(xi) Catatan Pembedahan/Catatan anestetik
(xii) Rakaman Video
(xiii) Cetakan daripada kelengkapan pemantauan (contoh: elektro kardiogram, elektro ensefalogram)
(xiv) Surat kepada dan daripada profesional jagaan kesihatan yang lain.
(xv) Rakaman perundingan/arahan melalui telefon berkaitan dengan penjagaan pesakit itu

5.2.5 Akses kepada Rekod Perubatan

APDP menetapkan bahawa Subjek Data harus mempunyai akses kepada Data Peribadi mereka yang terkandung dalam Rekod Perubatan yang disenggarakan oleh Pengguna Data. Hak ini juga dinyatakan dalam Garis Panduan Majlis Perubatan Malaysia seperti berikut, dan Subjek Data/Pesakit itu akan:

(a) mempunyai akses kepada rekod yang mempunyai maklumat tentang keadaan perubatan mereka untuk tujuan yang sah dan suci hati;
(b) mengetahui jenis maklumat peribadi yang direkodkan dan diproses;
(c) mengharapkan rekod itu tepat, dan
(d) mengetahui orang yang mempunyai akses kepada maklumat peribadi mereka.

Selain mempunyai hak akses kepada Rekod Perubatan mereka, pesakit juga berhak untuk memaklumkan kepada Profesional Jagaan Kesihatan atau kakitangan Hospital Swasta yang diberi kuasa untuk merawat mereka tentang apa-apa kesilapan fakta dalam maklumat peribadi yang terkandung dalam Rekod Perubatan dan membuat pembetulan padanya. Pesakit/ Subjek Data tidak dibenarkan mengubah apa-apa catatan yang dibuat oleh Profesional Jagaan Kesihatan yang merawat mereka sepanjang tempoh perundingan, diagnosis dan pengurusan kerana kesemuanya dibuat oleh pengamal perubatan berdasarkan pertimbangan klinikal mereka.

Data Peribadi individu lain. Subjek Data tidak mempunyai akses kepada apa-apa maklumat atau identiti individu lain yang terkandung dalam Rekod Perubatan itu. Jika identiti itu sudah diketahui oleh Subjek Data, maka data yang mengandungi maklumat berkaitan pihak ketiga itu boleh didedahkan kepada Subjek Data.

Pengguna Data perlu mempertimbangkan sama ada Data Peribadi mana-mana individu lain boleh diasingkan daripada maklumat Subjek Data yang lain yang akan dizahirkan, sebagai contoh, dengan memadamkan nama individu berkenaan, atau memadamkan butiran pengenalan yang lain sudah memadai untuk menyembunyikan identiti individu itu daripada Subjek Data.

Salinan Rekod Perubatan hanya boleh dibawa keluar daripada penjagaan Hospital dalam keadaan yang terhad, sama ada melalui perintah mahkamah, atau persetujuan bersama antara Pengguna Data dan Subjek Data. Dalam semua keadaan yang menghendaki Rekod Perubatan yang asal dibawa keluar atas Perintah Mahkamah, satu salinan rekod harus disimpan di Hospital itu.

5.2.6 Laporan Perubatan

Laporan Perubatan ialah dokumen yang disediakan oleh doktor yang merawat pesakit/Subjek Data berdasarkan Rekod Perubatan mereka. Pendapat pakar juga boleh dijadikan sebahagian daripada Laporan Perubatan itu.

Pengguna Data hendaklah mengemukakan Laporan Perubatan yang lengkap apabila diminta oleh Subjek Data atau Waris Terdekat dalam kes yang melibatkan kanak-kanak atau individu bawah umur, atau oleh majikan dengan persetujuan spesifik dan jelas daripada Subjek Data/pesakit dalam tempoh yang dinyatakan dalam APDP.

5.2.7 Penafian Penzahiran Rekod Perubatan

Pengguna Data boleh menafikan akses kepada kandungan Rekod Perubatan, jika pada pandangan mereka, diyakini:

(a) Pengguna Data tidak dibekalkan maklumat mencukupi untuk meyakinkan mereka berhubung identiti Peminta;
(b) jika kandungan itu dikeluarkan mungkin akan menyebabkan kemudaratan atau merendahkan Subjek Data, atau mana-mana individu lain, atau
(c) boleh mengakibatkan kemudaratan yang serius kepada kesihatan mental atau fizikal atau membahayakan nyawa pesakit/Subjek Data.

(d) Jika tidak ada persetujuan bertulis daripada pesakit, atau waris terdekat atau penjaga yang sah di sisi undang-undang, untuk mendedahkan kandungan Laporan Perubatan itu kepada pihak ketiga;
(e) Pesakit/Subjek Data sudah meninggal dunia, dan permintaan diterima daripada orang selain waris terdekat.
(f) dan dalam semua keadaan lain yang dinyatakan dalam Seksyen 32 APDP.

5.2.8 Fi semasa yang ditetapkan untuk akses kepada Data Peribadi oleh Subjek Data dikawal selia oleh Pesuruhjaya PDP menurut Peraturan-Peraturan (Fi) PDP 2013 (Lihat Parenggan 3.8.1(c). Subjek Data boleh meminta untuk melihat dokumen dalam Rekod Perubatan atau meminta salinan dibuat untuk bahagian yang berkenaan dalam Rekod Perubatan itu.

5.2.9 Pengguna Data mesti patuh kepada Permintaan Akses dalam tempoh 21 hari tetapi tidak melebihi 35 hari dari tarikh penerimaan permintaan itu, kecuali Pengguna Data boleh dianggap termasuk dalam mana-mana pengecualian dalam Seksyen 32. Walau bagaimanapun, Pengguna Data perlu memaklumkan secara bertulis kepada peminta alasan yang menyebabkan dia tidak boleh mematuhi permintaan akses itu dalam tempoh 21 hari pertama.

5.2.10 Hak untuk membuat pembetulan kepada Data Peribadi boleh dinafikan oleh Pengguna Data jika syarat di bawah Seksyen 36 APDP dipenuhi oleh Pengguna Data.

5.3 Hak Subjek Data untuk menarik balik persetujuan untuk memproses Data Peribadi (Seksyen 38 APDP)

5.3.1 Subjek Data boleh melalui notis bertulis kepada Pengguna Data untuk menarik balik persetujuan mereka untuk memproses Data Peribadi yang mana mereka adalah subjek data.

5.3.2 Pengguna Data selepas menerima notis itu hendaklah memberhentikan pemprosesan Data Peribadi.

5.3.3 Walau bagaimanapun, hak untuk menarik balik persetujuan tidak boleh digunakan untuk rawatan perubatan yang sedang berjalan dan perkhidmatan yang berkaitan dengan rawatan itu, yang memerlukan Data Peribadi pesakit/ Subjek Data itu diproses secara berterusan oleh Pengguna Data di sepanjang tempoh rawatan perubatan yang sedang diberikan kepada Subjek Data.

5.3.4 Jika untuk apa-apa sebab, Subjek Data membuat keputusan untuk menarik balik persetujuan yang telah diberikan untuk Tujuan Perubatan, ini bermakna Pengguna Data perlu memberhentikan pemprosesan Data Peribadi seseorang Subjek Data itu, dan Pengguna Data tidak boleh meneruskan penyediaan rawatan atau perkhidmatan perubatan yang lain kepada Subjek Data yang telah menarik balik persetujuan mereka.

5.3.5 Hak untuk menarik balik persetujuan di Hospital Swasta boleh digunakan dalam keadaan yang terhad seperti:

(a) Pemasaran perkhidmatan Pengguna Data yang lain yang tiada kaitan dengan rawatan:

(b) Penyertaan Subjek Data dalam ujian klinikal (yang memerlukan pemprosesan Data Peribadi);
(c) Pertukaran Data Pesakit dengan pengamal perubatan yang lain;
(d) Mengambil gambar Subjek Data (atau mana-mana bahagian badan mereka) semasa menerima rawatan atau pembedahan; dan
(e) Apa-apa tujuan lain yang tidak berkaitan dengan Tujuan Perubatan.

5.4 Hak untuk menghalang pemprosesan yang mungkin menyebabkan kerosakan atau distres (Seksyen 42 APDP)

5.4.1 Subjek Data boleh, pada bila-bila masa dengan memberi "notis subjek data" secara bertulis kepada Pengguna Data yang memerlukan Pengguna Data itu (a) memberhentikan pemprosesan Data Peribadi atau pemprosesan Data Peribadi untuk tujuan spesifik atau dalam cara yang tertentu; atau (b) tidak memulakan pemprosesan Data Peribadi atau pemprosesan Data Peribadi untuk tujuan spesifik atau dalam cara yang tertentu, apa-apa Data Peribadi di mana dia adalah subjek data, jika berdasarkan sebab-sebab yang dinyatakan oleh mereka:

(a) Pemprosesan Data Peribadi itu atau pemprosesan Data Peribadi untuk tujuan itu menyebabkan atau berkemungkinan akan menyebabkan kerosakan yang cukup besar atau distres yang mendalam kepada mereka atau kepada orang lain; dan
(b) Kerosakan atau distres adalah tidak wajar atau akan menjadi tidak wajar.

5.4.2 Hak dalam 4.3.1 tidak harus digunakan apabila:

(a) Subjek Data telah memberi persetujuan mereka; atau
(b) pemprosesan Data Peribadi itu adalah perlu dalam melindungi Kepentingan Vital Subjek Data itu; dan
(c) sebab lain yang dinyatakan dalam Seksyen 42 APDP.

5.5 Hak untuk menghalang Pemprosesan bagi maksud Pemasaran Langsung (Seksyen 43 APDP)

5.5.1 Subjek Data boleh, pada bila-bila masa melalui notis bertulis kepada Pengguna Data menghendaki Pengguna Data memberhentikan atau tidak memulakan pemprosesan Data Peribadi mereka bagi tujuan Pemasaran Langsung. Jika Pengguna Data mahu menghantar bahan pemasaran kepada pesakit mereka, maka dinasihatkan untuk mendapatkan persetujuan jelas daripada Subjek Data dengan menyatakan maklumat berkenaan kaedah penyampaian yang akan digunakan untuk tujuan pemasaran itu.

5.5.2 "Pemasaran Langsung" bermaksud apa-apa bentuk komunikasi seperti pengiklanan atau bahan pemasaran untuk perkhidmatan Pengguna Data yang ditujukan kepada individu tertentu. Bahan ini merangkumi surat, risalah, SMS, WhatsApp, E-mel dsb.

6. ISU SPESIFIK

6.1 Data Peribadi Sensitif (Seksyen 40 APDP)

6.1.1 APDP menyatakan bahawa Pengguna Data tidak boleh memproses apa-apa Data Peribadi Sensitif seseorang Subjek Data kecuali mengikut, antara lain, syarat berikut:
(a) Subjek Data telah memberikan persetujuan eksplisit untuk pemprosesan Data Peribadi Sensitif itu:

Secara lazimnya apabila Hospital memproses Data Peribadi, Hospital telah mendapat persetujuan eksplisit daripada Subjek Data dengan meminta Subjek Data mengisi beberapa borang sebelum pemprosesan Data Peribadi itu (seperti yang dibincangkan sebelum ini).

(b) Pemprosesan itu adalah perlu (dan persetujuan Subjek Data tidak diperlukan):
   (i) bagi tujuan untuk melindungi Kepentingan Vital Subjek Data atau orang lain, dalam keadaan di mana, (a) persetujuan tidak boleh diberi oleh Subjek Data atau bagi pihak Subjek Data itu; atau (b) Pengguna Data tidak boleh semunasabahnya dijangka untuk mendapat persetujuan daripada Subjek Data;
   (ii) untuk tujuan perubatan dan dijalankan oleh (a) Profesional Jagaan Kesihatan; atau (b) seseorang yang berada dalam kedudukan yang telah diamanahkan dengan tanggungjawab untuk menyimpan rahsia sama seperti yang diperlukan jika seseorang itu adalah professional jagaan kesihatan;

Sebagai contoh
(a) apabila rawatan perubatan diberikan kepada mangsa kemalangan dengan menggunakan maklumat daripada dokumen peribadi seperti Kad Pengenalan;
(b) untuk merawat pesakit psikiatri yang tidak berupaya untuk memberi persetujuan

   (iii) bertujuan untuk, atau berkaitan dengan mendapatkan nasihat untuk
   (iv) prosiding undang-undang;
   (v) untuk tujuan membuktikan atau mempertahankan hak undang-undang;
   (vi) untuk perlaksanaan apa-apa fungsi yang ditauliahkan oleh mana-mana undang-undang bertulis atau dinyatakan dalam mana-mana undang-undang bertulis itu
   (vii) untuk pentadbiran keadilan;

Sebagai contoh
(a) untuk siasatan jenayah, di mana Data Peribadi Sensitif diberikan kepada Polis atau agensi lain;
(b) pembelaan untuk tuntutan yang dibuat terhadap Pengguna Data atau mana-mana Doktor di Hospital, seperti perkongsian Data Peribadi Sensitif dengan Peguam;
(c) perkongsian maklumat Data Peribadi Sensitif dengan Kementerian Kesihatan berkaitan dengan penyakit berjangkit (seperti AIDS), Denggi dsb.

(c) maklumat dalam Data Peribadi telah didedahkan kepada awam disebabkan tindakan secara sengaja Subjek Data.

Sebagai contoh
(a) Subjek Data telah diwawancara dan artikel susulan itu disiarkan dalam akhbar atau majalah atau mengandungi Data Peribadi Sensitif milik Subjek Data itu
(b) Subjek Data memaparkan Data Peribadi Sensitif mereka di saluran media sosial seperti Facebook, Instagram, WeChat dsb.

(d) Lain-lain keadaan seperti yang dinyatakan dalam Seksyen 40 APDP.

6.2 Pakar Perubatan yang bekerja di bawah Kontrak Perkhidmatan

6.2.1 Jika Pakar Perubatan yang bekerja secara kontrak perkhidmatan, semua tanggungjawab yang diberikan kepada pekerja ke atas Data Peribadi akan juga terpakai kepada Pakar Perubatan ini.

6.3 Pakar Perubatan yang diguna khidmat di bawah kontrak untuk perkhidmatan (sebagai Perunding – juga dikelaskan sebagai "Pemproses Data")

6.3.1 Pakar Perubatan mempunyai hubungan yang istimewa dengan Hospital dan pesakit yang ditugaskan kepada mereka walaupun mereka bukan kakitangan, mereka mempunyai akses kepada semua Data Peribadi dan Data Peribadi Sensitif milik pesakit yang telah ditugaskan kepadanya itu yang berada dalam pengawasan Hospital Swasta itu selaku Pengguna Data. Pakar Perubatan itu akan dianggap sebagai Pemproses Data menurut Seksyen 9 (2) APDP untuk semua niat dan tujuan.

6.3.2 Pihak Hospital mesti memastikan terdapat perlindungan kontraktual yang mencukupi dalam perjanjian bertulis yang mentadbir hubungan antara Hospital Swasta dan Pakar Perubatan yang menyatakan bahawa Pakar Perubatan itu harus mematuhi keperluan APDP untuk menyimpan Data Peribadi pesakit/Pengguna Data menurut dasar Hospital, Akta ini, Kod ini dan mana-mana undang-undang, kaedah dan peraturan yang terpakai. Pakar Perubatan perlu dimaklumkan tentang peranan dan tanggungjawab mereka ke atas Data Peribadi pesakit dan Pengguna Data juga hendaklah memastikan latihan mencukupi berhubung APDP diberikan kepada Perunding itu.

6.3.3 Kod ini menyedari kenyataan bahawa Pakar Perubatan lazimnya mempunyai klinik di beberapa Hospital Swasta, justeru, apa-apa akses kepada Data Peribadi pesakit/Subjek Data atau pemprosesan Data Peribadi pesakit/ Subjek Data dari satu Hospital Swasta ke Hospital Swasta yang lain tidak dibenarkan kecuali disetujui oleh pesakit/ Subjek Data.

6.3.4 Pengguna Data harus mempunyai dasar yang kukuh untuk mengawal selia penggunaan peranti elektronik mudah alih oleh Pakar Perubatan kecuali maklumat disulitkan sepenuhnya dan dilindungi kata laluan.

6.4 Pemindahan Data ke Tempat di Luar Malaysia

6.4.1 APDP melarang pemindahan Data Peribadi milik Subjek Data ke suatu tempat di Luar Malaysia kecuali tempat itu telah ditetapkan oleh Menteri sebagai tempat yang selamat untuk memproses Data Peribadi.

6.4.2 Walau apapun dinyatakan di atas, Pengguna Data boleh memindahkan Data Peribadi ke suatu tempat di luar Malaysia jika:

(a) Subjek Data telah memberi persetujuan mereka.

Persetujuan akan diperoleh sejak dari mula semasa pendaftaran pertama pesakit itu (dengan menyediakan persetujuan dalam borang pendaftaran).

(b) Pemindahan itu perlu untuk pelaksanaan kontrak antara Subjek Data dan Pengguna Data.

Contoh:
(a) pemindahan pesakit ke cawangan atau hospital di luar negara untuk rawatan pakar perubatan;
(b) perkongsian Data Peribadi di mana Pengguna Data meminta untuk mendapatkan pendapat kedua daripada perunding luar negara

(c) Pemindahan bertujuan untuk prosiding undang-undang atau untuk mendapatkan nasihat undang-undang:
(d) Pemindahan itu perlu untuk melindungi Kepentingan Vital Subjek Data itu;
(e) Pemindahan itu perlu atas sebab kepentingan awam seperti yang ditentukan oleh Menteri.

7. PEKERJA

7.1 Penerapan APDP ke atas Pekerja

"Pekerja" termasuk Profesional Jagaan Kesihatan, kakitangan pengurusan hospital, petugas perubatan am, kakitangan pentadbiran, kakitangan IT, petugas keselamatan dsb., yang diambil bekerja secara kontrak pekerjaan di Hospital Swasta.

7.1.1 Pengguna Data hendaklah mematuhi semua Prinsip Perlindungan Data dalam APDP apabila berurusan dengan Data Peribadi pekerja:

(a) Prinsip Am – Persetujuan Pekerja hendaklah diperoleh untuk semua tujuan yang berkaitan dengan pekerjaan. Maklumat peribadi waris terdekat dan orang yang perlu dihubungi semasa kecemasan, dianggap telah diperoleh pekerja.
(b) Prinsip Notis & Pilihan – Prinsip ini akan dipatuhi oleh Pengguna Data semasa tawaran dan penerimaan pekerjaan dan Pekerja menandatangani beberapa dasar Hospital dan akuan menyimpan rahsia.
(c) Prinsip Penzahiran – Penzahiran Data Peribadi Pekerja akan melibatkan mana-mana Pihak Ketiga dan tidak terhad kepada syarikat insurans, Pertubuhan Penjagaan Terurus, Peguam, Bank, syarikat pelancongan dan tujuan lain berkaitan pekerjaan.
(d) Prinsip Keselamatan – Semua Data Peribadi akan disimpan dengan sewajarnya daripada akses tanpa kebenaran atau penzahiran atau pemusnahan.
(e) Prinsip Penyimpanan – Lazimnya semua Data Peribadi Pekerja akan disimpan selama 7 tahun selepas penamatan pekerjaan. Semua Data Peribadi (dalam bentuk KV) yang diberikan oleh calon berpotensi dan tidak berjaya harus dilmusnahkan dalam satu tempoh yang munasabah selepas temu duga.
(f) Prinsip Integriti Data – Semua Data Peribadi Pekerja yang telah diproses oleh Pengguna Data akan disimpan dengan tepat dan lengkap. Usaha berkala untuk mengemas kini rekod harus dimulakan oleh dasar Sumber Manusia dan menerusi perkhidmatan intra-net jika tersedia.
(g) Prinsip Akses – Semua pekerja akan diberi akses kepada Data Peribadi mereka yang diproses oleh Pengguna Data dan hak untuk membuat pembetulan dalam Data Peribadi mereka jika Data Peribadi itu tidak lengkap dan tidak dikemas kinikan.

8. ISU PEMATUHAN LAIN

8.1 Kewajipan pematuhan oleh Pengguna Data dalam menjaga keselamatan Data Peribadi Subjek Data adalah seperti berikut:

(a) Mematuhi semua peruntukan APDP kecuali apabila peruntukan dalam Kod ini mengubah suai kewajipan atau hak Pengguna Data atau Subjek Data;
(b) Undang-undang spesifik yang secara khususnya memberi kesan kepada industri jagaan kesihatan dan Hos pital Swasta hendaklah mengatasi peruntukan APDP atau Kod ini.
(c) Pengguna Data hendaklah mempertimbangkan untuk melantik seorang Pegawai Perlindungan Data yang diberi kuasa untuk melaksanakan, menguruskan dan menguatkuasakan peruntukan APDP dan Kod ini di Hospital Swasta yang berkenaan.

8.2 Pemantauan Pematuhan dan Audit Pematuhan Dalaman

(a) Pengguna Data hendaklah membuat satu dasar pemantauan pematuhan bagi memastikan semua jabatan di Hospital Swasta mematuhi Prinsip APDP dan Kod ini.
(b) Satu audit pematuhan dalaman hendaklah dijalankan oleh Pengguna Data sekurang-kurangnya dalam tempoh dua belas (12) bulan untuk memastikan semua dasar dan tatacara berkaitan Data Peribadi dipatuhi sepenuhnya oleh semua petugas Hospital Swasta yang mengendali dan mempunyai akses kepada Data Peribadi di Hospital Swasta.

8.3 Penggunaan Peranti Perubatan

(a) Secara lazimnya di Hospital Swasta, pelbagai Peranti Perubatan digunakan, seperti Mesin X-Ray, Pengimbas CT, Ultrabunyi, MRI dan peranti lain seumpamanya, yang merekodkan dan menyimpan Data Peribadi Pesakit. Peranti Perubatan secara amnya menyimpan satu salinan Data Peribadi selepas memindahkan Data Peribadi ke Sistem Pengurusan Maklumat Hospital (Hospital Information Management System atau HIMS).
(b) Pengguna Data hendaklah menggubal dasar berkaitan Data Peribadi dalam peranti ini supaya Data Peribadi ini dihapuskan secara kekal sebaik sahaja Data Peribadi dan imej dipindahkan ke HIMS.
(c) Pengguna Data juga harus memastikan Data Peribadi dalam peranti ini dihapuskan secara kekal sebelum penyahtauliahan peranti itu atau sebelum penyerahan untuk jualan kepada pihak ketiga.

8.4 Latihan PDP

(a) Pengguna Data harus memastikan latihan kesedaran tetap untuk APDP dijalankan untuk semua kakitangan yang mempunyai akses kepada Data Peribadi di Hospital Swasta. Ini termasuk, doktor, jururawat, perunding, kakitangan pentadbiran dan semua kakitangan sokongan.
(b) Bagi semua pekerja baharu, latihan kesedaran APDP hendaklah diterapkan ke dalam program induksi apabila mereka mula bekerja di Hospital Swasta itu.
(c) Bagi Hospital Swasta yang mempunyai sistem intranet kakitangan, tutorial tetap tentang APDP boleh diterapkan untuk meningkatkan kesedaran secara tetap.

9. KAJIAN SEMULA KOD

(a) Kod ini boleh dikaji semula setiap dua (2) tahun atau bagi tempoh yang lebih panjang seperti yang diperlukan dan diarahkan oleh Pesuruhjaya Perlindungan Data Peribadi.
(b) Kajian semula mungkin diperlukan untuk memasukkan perubahan yang dibuat pada APDP, seperti Peraturan atau undang-undang lain yang mempunyai kesan secara langsung kepada Kod ini.

10. KESIMPULAN

(a) Semua Pengguna Data mesti mematuhi Kod ini selagi kod ini tidak mengubah suai atau menambah Prinsip APDP.
(b) Mana-mana yang diperlukan, dasar dalaman yang mencukupi mesti disediakan untuk memastikan APDP dan Kod ini dipatuhi sepenuhnya.
(c) Dasar-dasar sedia ada harus dikaji semula untuk memastikan pematuhan Kod ini.

LAMPIRAN A
SENARAI PENZAHIRAN YANG DIBENARKAN

Senarai penzahiran yang dibenarkan kepada pihak ketiga untuk Data Peribadi yang diproses oleh Pengguna Data yang merupakan sebuah Hospital Swasta.

Senarai ini tidak lengkap dan boleh ditambah atau dipinda untuk memenuhi "tujuan" dan untuk tujuan-tujuan yang berkaitan secara langsung dengan tujuan utama penzahiran ini.

No	Pihak Ketiga yang terlibat dengan penzahiran oleh Pengguna Data (Hospital)
1	Pakar Perubatan (sebagai Pemproses Data) yang beroperasi di klinik dan merawat Subjek Data di Hospital
2	Syarikat Insurans yang mengurus kewajipan pembayaran bagi pihak Subjek Data
3	Pertubuhan Penjagaan Terurus yang bertindak sebagai pengantara bagi majikan dan Syarikat Insurans dalam proses pembayaran
4	Majikan Subjek Data
5	Ibu bapa dan Waris Terdekat seperti yang dibenarkan oleh Subjek Data
6	Bank, Institusi Kewangan, pengeluar Kad Kredit/Debit untuk pemprosesan pembayaran
7	Ejen Pemungut Hutang untuk menuntut bayaran tertunggak untuk Pengguna Data
8	Peguam Panel yang menguruskan tuntutan terhadap Pengguna Data dan memberi khidmat nasihat kepada Pengguna Data
9	Makmal Swasta dan penyedia perkhidmatan diagnostik yang di luar kawalan persekitaran Hospital Swasta
10	Pusat Data yang menyimpan semua Data Hospital untuk Pengguna Data
11	Ejen, kontraktor dan vendor yang memproses data untuk Pengguna Data
12	Juruaudit dan Akauntan Luar
13	Badan yang Diluluskan untuk mengumpul manfaat pekerja termasuk: • Pertubuhan Keselamatan Sosial (PERKESO) • Zakat • Kumpulan Wang Simpanan Pekerja (KWSP) • Lembaga Tabung Haji • Skim Insurans Pekerja (SIP)
14	Kerajaan Persekutuan dan Agensi Kerajaan dan pertubuhan lain yang berkaitan • Kementerian Kesihatan • Kementerian Sumber Manusia • Kementerian Dalam Negeri • Suruhanjaya Pencegahan Rasuah Malaysia • Lembaga Hasil Dalam Negeri • Jabatan Insolvensi Malaysia • Polis DiRaja Malaysia • Majlis Perubatan Malaysia (MPM) • Majlis Pergigian Malaysia (MDC) • Persatuan Perubatan Malaysia
15	Pihak Berkuasa Tempatan yang berkaitan

LAMPIRAN B

(NAMA HOSPITAL)
AKTA PERLINDUNGAN DATA PERIBADI 2010 BORANG PERMINTAAN AKSES DATA

Maklumat berikut diperlukan bagi membantu kami memberikan maklum balas yang cepat dan tepat kepada Permintaan Akses Data anda menurut Akta Perlindungan Data Peribadi 2010.

Nama Penuh Subjek Data atau Orang yang Berkaitan	
Hubungan Orang yang Berkaitan dengan Subjek Data	
Alamat	
Nombor Telefon Mudah Alih	
Alamat E-mel	

Jika anda pernah menjadi Pesakit di [Hospital Pengguna Data] sila nyatakan Nombor Rekod Perubatan anda

Jika anda sedang atau pernah bekerja di [Hospital Pengguna Data] sila nyatakan Nombor Pekerja dan tempoh pekerjaan anda

Sila nyatakan butiran maklumat yang anda kehendaki daripada [Pengguna Data]:

Pengisytiharan: Saya Subjek Data/Orang yang Berkaitan yang dinyatakan di atas dengan ini meminta, di bawah peruntukan Seksyen 12 dan 30 Akta Perlindungan Data 2010, bahawa [Pengguna Data] membekalkan saya dengan Salinan data peribadi saya yang disimpan seperti yang dinyatakan di atas. Saya memahami bahawa bayaran untuk perkhidmatan ini mungkin dikenakan dan [Pengguna Data] akan menghubungi saya untuk membuat tuntutan bayaran tersebut. Saya juga ambil maklum bahawa pihak Hospital akan memberi maklum balas dalam tempoh yang dinyatakan dalam Akta selepas menerima pembayaran daripada saya dan akan memaklumkan kepada saya tarikh dan waktu untuk hadir sendiri bagi tujuan pengambilan salinan dokumen itu

Tandatangan _____ Tarikh _____

NOTES