

BAB IV HASIL DAN PEMBAHASAN

A. Gambaran Puskesmas Gamping 1

Puskesmas Gamping I, yang bertanggung jawab atas pembangunan layanan kesehatan di wilayah kerjanya. Alamatnya adalah Jl. Delingsari, Ambarketawang, Gamping, Patukan, Ambarketawang, Kabupaten Sleman, Daerah Istimewa Yogyakarta. Lokasinya berada di Kecamatan Gamping. Pusat Kesehatan Gamping I memiliki dua lantai untuk layanan. Di lantai 1 terdapat ruang pendaftaran, ruang kasir, ruang tunggu, ruang BP umum, ruang BP tindakan, ruang BP gigi, apotek, ruang BP KIA, imunisasi, ruang KB, gizi, TB, ruang laboratorium, gudang obat, dapur, dan toilet. Di lantai 2 terdapat ruang kepala puskesmas, aula, ruang Tata Usaha (TU), ruang Unit Kesehatan Masyarakat (UKM).

Untuk mencapai Indonesia Sehat, Puskesmas Gamping memiliki visi dan misi sebagai berikut:

1. Visi Puskesmas Gamping I
“Terwujudnya Pelayanan Puskesmas yang Berkualitas, Terjangkau dan Berdaya Saing Munuju Masyarakat Sleman yang berbudaya Hidup Bersih dan Sehat”.
2. Misi Puskesmas Gamping I
 - a. Meningkatkan tata kelola Puskesmas yang baik dengan dukungan teknologi untuk meningkatkan kualitas pelayanan kepada Masyarakat.
 - b. Menyelenggarakan pelayanan kesehatan di tingkat pertama yang bermutu dan terjangkau dengan penyediaan sarana prasarana sesuai standar.
 - c. Mendorong kemandirian masyarakat untuk berperan aktif dalam upaya peningkatan derajat Kesehatan Masyarakat.

B. Gambaran Aplikasi *Primary care* di Puskesmas Gamping I

Aplikasi *primary care* diperkenalkan pertama kali oleh BPJS pada tahun 2014 dan mulai digunakan di puskesmas Gamping I tahun 2015, aplikasi ini tidak dibuat oleh vendor atau IT Internal Puskesmas Gamping I tetapi di buat langsung oleh pusat BPJS. Aplikasi *primary care* digunakan di Puskesmas Gamping I untuk

mempermudah petugas mengakses data dari server BPJS. Fungsinya meliputi input data pasien, pendaftaran pasien baru, catatan kunjungan pasien, basis data diagnosa penyakit beserta kode, informasi pelayanan obat, data penunjang diagnosa, dan proses rujukan. Setiap petugas yang akan menggunakan aplikasi *primary care* harus mengisi *user* dan *password* untuk bisa menggunakannya, untuk keamanan data – data rekam medis pasien pada aplikasi *primary care*. Keuntungan petugas menggunakan aplikasi *primary care* seperti berikut:

1. Proses pendaftaran pasien menjadi lebih mudah dan cepat
 - a. Pasien dapat mendaftar online melalui aplikasi, sehingga mengurangi antrian di faskes.
 - b. Petugas dapat langsung mengakses data pasien, termasuk riwayat kesehatan, sehingga proses pendaftaran lebih cepat dan akurat.
2. Memudahkan diagnosa pasien
 - a. Aplikasi *Pcare* menyediakan akses ke data riwayat kesehatan pasien yang terintegrasi, sehingga petugas dapat lebih mudah mengdiagnosa penyakit pasien.
 - b. Tersedia fitur skrining kesehatan yang dapat membantu petugas dalam mendiagnosis penyakit pasien.
3. Mempermudah proses rujukan pasien
 - a. Petugas dapat mudah merujuk pasien ke faskes lain melalui aplikasi *Pcare*.
 - b. Aplikasi *Pcare* menyediakan informasi faskes rujukan yang lengkap, termasuk alamat, jam buka, dan kontak.
4. Mempermudah proses klaim
 - a. Petugas dapat mengajukan klaim secara online melalui aplikasi *Pcare*
 - b. Aplikasi *Pcare* menyediakan panduan dan informasi yang lengkap tentang proses klaim.
5. Meningkatkan kualitas pelayanan
 - a. Penggunaan aplikasi *Pcare* dapat membantu meningkatkan kualitas pelayanan di faskes, karena petugas dapat memberikan pelayanan yang lebih cepat, akurat, dan efisien.

- b. Data yang tersedia di aplikasi *Pcare* dapat membantu petugas dalam mengambil keputusan yang tepat terkait dengan pengobatan pasien.

C. Hasil

Hasil dari penelitian ini adalah terkait keamanan data rekam medis pada aplikasi *primary care* di puskesmas Gamping I, menggunakan metode kualitatif deskriptif yang mengambil pada suatu komponen *model CIAAN* yang memperluas dari *triad CIA* meliputi aspek *privacy*, aspek *integrity*, aspek *authentication*, aspek *Availability*, dan aspek *non-repudation*.

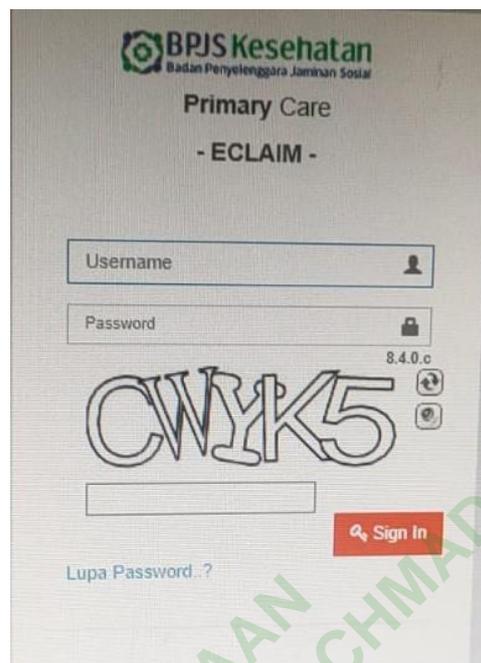
Bedasarkan hasil wawancara penulis menyusun sebuah kerangka sebagai acuan dari pedoman dalam melakukan *coding*. Dengan pedoman ini, penulis kemudian kembali membaca transkrip wawancara, melakukan *coding*, dan melakukan pemilihan data yang relevan dengan pokok pembicaraan untuk menunjukkan hubungan antara bagian – bagian yang diteliti. Karakteristik informan dalam penelitian ini adalah sebagai berikut.

Tabel 3 Karakteristik Informan

Kode informan	Jabatan	Pendidikan	Jenis kelamin	Lama kerja
IU 1	Petugas rekam medis	D3 Rekam medis	Perempuan	2 tahun
IU 2	Perawat poli umum	S1 keperawatan	Perempuan	5 tahun
IU 3	Petugas rekam medis	D3 Rekam Medis	Laki-laki	5 tahun
IU 4	Dokter poli umum	S1 Profesi	Perempuan	5 tahun
TS 1	Kepala puskesmas	S1 kedokteran	Laki laki	6 bulan

1. Aspek *Privacy*.

Pada halaman awal aplikasi *primary care* di puskesmas Gamping I menunjukkan aspek *privacy* setiap pengguna harus mempunyai *user* dan *password* yang sudah di daftarkan ke pusat BPJS yang membuat informasi terlindungi dari pihak pihak yang tidak punya hak untuk mengakses informasi. Hal tersebut dapat dilihat dari pernyataan responden dan halaman awal aplikasi *primary care* berikut:



Gambar 3 Halaman awal aplikasi *primary care* di puskesmas Gamping

Gambar 3 menunjukkan halaman awal pada aplikasi *primary care* di puskesmas Gamping I yang terdiri dari tiga isian, yaitu *username*, *password*, dan pengisian kode verifikasi. *Username*: diisi nama *user* masing- masing yang telah dibuat, *password* merupakan perpaduan alfanumerik dan angka, dan pengisian kode verifikasi diisi sama seperti gambar yang muncul.

Kotak 1

“petugas di Puskesmas yang sudah punya *user* dan *password*, petugas pendaftaran, perawat, dokter, psikolog, terapis bisa, udah itu aja” (IU 3,4)
 “Dokter, perawat tapi perawat juga gasemuanya gunain tapi dia punya *user* dan *password* nya.” (IU 1)

Dari hasil wawancara diketahui bahwa keamanan data rekam medis pada aplikasi *primary care* di puskesmas Gamping 1 dengan Aspek *Privacy* belum berjalan dengan baik, karena masih ada beberapa petugas yang mengetahui *username* dan *password* milik petugas lainnya digunakan untuk menginputkan data. Setiap petugas memiliki *user* dan *password* yang berbeda hal tersebut membuat petugas yang tidak memiliki akses untuk menggunakan aplikasi *primary care* tidak dapat masuk ke sistem yang berdampak pada keamanan data pasien. Untuk setiap petugas yang belum mempunyai *user* dan

password harus mendaftarkan diri terlebih dahulu ke BPJS dengan mengisi form yang disediakan oleh BPJS, setelah mengisi form petugas mengirimkannya ke email BPJS Kesehatan untuk dibuatkan *username* dan *password* nya. *Username* dan *password* dapat diubah sendiri oleh petugas tetapi harus ada konfirmasi terlebih dahulu kepada pusat. Hal tersebut dapat dilihat dari responden berikut.

Kotak 2

“Kita bersurat ke bpjs, terus nanti dikirim ke email bpjs, kalau udah dapet balesannya nanti ada *user password* nya.” (IU 3)

“Biasanya kita isi form yang disediakan oleh bpjs terus nanti ada dua form nanti form itu di scan lalu dikirimkan lewat email dan petugas bpjs yang membikin *user* dan *password*” (IU 1)

Hal tersebut juga disampaikan oleh informan triangulasi sumber yang menyatakan bahwa dalam pembuatan *username* dan *password*, harus mengisi terlebih dahulu form yang sudah disediakan oleh BPJS Kesehatan dan berikut adalah kutipan wawancaranya:

Kotak 3

“Nanti bpjs biasanya kasih form terus petugas ngisi form nya, setelah itu ya dikirim lewat email masing masing, nanti tinggal liat balesannya aja si de kalau sudah di balas pasti bisa buka *username* dan *password* nya” (TS 1)

Dari penjelasan di atas dapat diketahui setiap petugas yang mempunyai *username* dan *password* harus mendaftarkan diri terlebih dulu untuk mendapatkan *username* dan *password* tersebut. Caranya dengan mengisi terlebih dahulu beberapa formulir yang telah disediakan oleh pihak BPJS Kesehatan untuk mendaftarkan diri lalu setelah itu, petugas mengirimkannya melalui email masing – masing dan setelah dikonfirmasi akan mendapatkan balasan dari pihak BPJS Kesehatan mengenai *username* dan *password* ke email masing-masing.

Setiap petugas mempunyai *username* dengan awalan menggunakan 12020101-nama pengguna angka tersebut merupakan tanda sebagai kode puskesmas Gamping dan *password* yang berbeda setiap pengguna, untuk

password akan dilakukan skala pergantian setiap 3 bulan sekali dari pihak BPJS pergantian *password* ini akan otomatis akan *log off* dan terdapat pemberitahuan untuk mengganti *password*. Hal tersebut dapat dilihat dari responden berikut

Kotak 4

“User Bpjs gamping itu ada kodenya 12020101. Terus baru nama penggunaanya tapi nanti kalau *password* nya bebas” (IU 3)
 “Nanti tiap 3 bulan off sendiri jadi nanti tiap 3 bulan mau gamau kita harus perbarui *password* nya jadi kalua nanti *password* yang sekarang mau ganti gabisa langsung harus 2x samapai 3x ganti dlu” (IU 3)

Hal tersebut juga disampaikan oleh informan triangulasi sumber yang menyatakan bahwa bentuk *username* dan *password* di puskesmas Gamping I ini memiliki kode awal yang hanya dipakai oleh puskesmas Gamping I yaitu 12020101- nama pengguna, lalu untuk *password* nya tetap berbeda setiap pengguna. *Password* mempunyai jangka waktu perubahan berkala dilakukan setiap 3 bulan sekali yang akan otomatis mati tidak bisa digunakan oleh pengguna dan harus diganti dengan *password* yang baru untuk keamanan data pasien. Aplikasi primary juga otomatis keluar ke menu *login* jika aplikasi tidak digunakan kurang lebih 10 menit oleh petugas. berikut adalah kutipan wawancaranya informan triangulasi sumber:

Kotak 5

“Untuk *usern*nya bebas tapi setiap petugas punya beda *user* tetapi puskes gamping itu kode awal nya 12020101 baru namanya dan *password* nya berbeda-beda” (TS 1)
 “Setiap 3 bulan sekali pasti ada perubahan dari pusat nya, pasti otomatis off sendiri dan ya berarti tandanya harus ganti *password* atau memperbarui *password* nya agar tidak sama dengan yang sebelum nya agar tidak ada yang tahu juga yang lain nya” (TS 1)

Dari penjelasan diatas dapat diketahui setiap petugas yang mempunyai *username* dan *password* harus mengganti *password* yang berbeda dalam jangka waktu 3 bulan untuk keamanan lebih terjaga dan tidak sembarangan orang dapat mengakses aplikasi *primary care* dengan mudah. Tetapi pada saat petugas login tidak ada verifikasi ke Email maupun WA untuk memastikan bahwa itu memiliki

asli dari *user* dan *password*, oleh karena itu siapa saja mudah menggunakan *user* dan *password* milik petugas lain.

2. Aspek *Integrity*

Pengguna menilai dapat dengan mudah untuk mengubah data yang terdapat kesalahan tetapi tidak bisa mengetahui siapa yang mengubah nya. Hal tersebut dapat dilihat dari pernyataan responden berikut;

Kotak 6

“Nanti ada tombol edit disini , terus udah tinggal di edit aja” (IU 1)
 “*Primary care* tuh sudah ada batas nya misal kaya tekanan darah itu tuh ada minimal dan *maxsimal* tapi kalau melewati batas itu di *Pcare* nya gamau tertulis mba, jadi *Pcare* nya gamau nyimpen” (IU 3)

Dari hasil wawancara diketahui bahwa pengguna yang telah menginput data lalu terjadi kesalahan dapat diubah dengan cara mengedit nya secara manual dan semua petugas dapat mengedit untuk memperbaiki data yang salah tetapi tidak ada pemberitahuan siapa yang mengubah dan mengganti data tersebut. Pengguna yang menginput data pasien pada aplikasi *primary care* di puskesmas Gamping I mengisi data rekam medis pasien diisi dengan lengkap karena sudah ada batas minimal maximal dan jika terdapat kolom yang belum terisi atau tidak sesuai aplikasi *primary care* tidak dapat menyimpan nya sehingga untuk kelengkapannya pun akan terjamin.

Hal tersebut juga disampaikan oleh informan triangulasi sumber yang menyatakan bahwa dalam pengubahan data yang ada pada aplikasi *primary care* ini sangat lah mudah, berikut adalah kutipan wawancaranya:

Kotak 7

“Mudah sekali, langsung diganti aja, nanti ada tulisan edit lalu simpan selesai sudah” (TS 1)

Dari hasil wawancara triangulasi sumber dapat diketahui jika aspek *integrity* ini belum berjalan dengan baik karena siapa saja dapat mengubah dan mengedit data pasien dengan mudah yang terdapat pada aplikasi *primary care*. Aplikasi *primary care* tidak memberikan pemberitahuan jika ada perubahan

data pasien oleh petugas lain, setiap petugas yang mempunyai *acces* dapat merubah data pasien yang telah ada pada aplikasi tersebut dengan mudah hal tersebut menyebabkan kurangnya aspek *integrity* yang nantinya akan menyebabkan kesalahpahaman. Hal tersebut dapat dilihat dari responden berikut:

Kotak 8

“Kalau mengetahui yang merubah gaada yang tau, gada pemberitahuan siapa siapanya.” (IU 2,4)

Hal tersebut juga disampaikan oleh informan triangulasi sumber yang menyatakan bahwa dalam setiap perubahan yang ada pada aplikasi *primary care* seperti perubahan data pasien, salah penginputan diagnosis dan lain – lain tidak diketahui siapa yang mengubah maupun mengeditnya dan tidak ada pemberitahuan untuk mengetahui siapa petugas yang telah merubah data tersebut. Berikut adalah kutipan wawancaranya

Kotak 9

“Kalau untuk mengetahui siapa yang merubah nya tidak ada pemberitahuan nya jadi gatau siapa yang ubah” (TS 1)

No	No. KARTU	NAMA PESERTA	KELAMIN	USIA	POLI/KEGIATAN	SUMBER	STATUS	H
A19-1	000...	SATAM	L	79	POLI UMUM	Web Antrean	Baru	
A19-2	000...	TIAS HALIMATUSADYA	P	21	POLI UMUM	Web Antrean	Baru	
A19-3	000...	RAFFASYA MALIK AL FATIR	L	2	POLI UMUM	Web Antrean	Baru	
A19-4	0002...	RAZENDRA ALFARIZKY RAMADHAN PRATAMA	L	6	POLI UMUM	Web Antrean	Baru	
A19-5	000...	ROBY FEBRIANSYAH PRATAMA	L	37	POLI UMUM	Web Antrean	Baru	
A19-6	...	SUTINI	P	67	POLI UMUM	Web Antrean	Baru	
A19-7	...	SUPRAPTO	L	60	POLI UMUM	Web	Baru	

Gambar 4 Riwayat pendaftaran pasien

Gambar 4 menunjukkan Riwayat pendaftaran pasien yang bisa dilihat, diedit dan di hapus oleh petugas kapanpun tanpa adanya pemberitahuan yang jelas.

3. Aspek *Authentication*

Pengguna menilai verifikasi dan akses pada aplikasi *primary care* di puskesmas Gamping I belum berjalan dengan lancar. Hal tersebut dilihat dari pernyataan responden berikut:

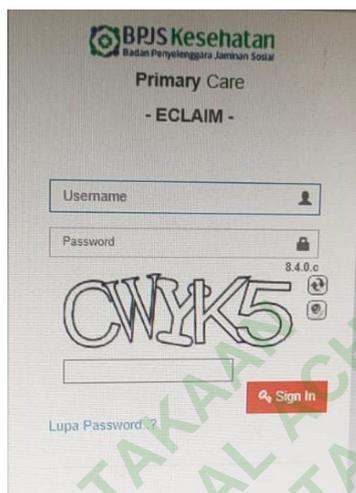
Kotak 10

“Kalau disini tuh *Pcare* nya gaada level nya jadi mau pake pendaftaran atau pake yang dokter itu sama saja bisa akses dan menu nya sama aja” (IU 3)

“menu menu pada aplikasi *Pcare* semua bisa buka si de “ (IU 1)

Dari hasil wawancara diketahui bahwa pengguna yang sudah mempunyai *user* dan *password* yang berbeda tetapi masih bisa mengakses semua menu yang ada pada aplikasi *primary care* hal ini menyebabkan pengguna dapat mengakses semua, yang berdampak pada keamanan data pasien

karena tidak ada batasan setiap petugas dapat melihat semua dari mulai data dan *history* pasien yang ada pada aplikasi. Di Puskesmas Gamping I ini juga masih terdapat beberapa *username* dan *password* yang pengguna lain ketahui, seperti pada bagian pendaftaran petugas pendaftaran mengetahui *username* dan *password* milik petugas pendaftaran lainnya.



Gambar 5 halaman *login*

Gambar 5 menunjukkan halaman login aplikasi *primary care*, hanya petugas yang mempunyai akses yang dapat menggunakan aplikasi *primary care*, dengan mengisi *username* dan *password* yang petugas punya, setelah itu masukan kode verifikasi data yang akan muncul berbeda setiap *login* untuk memastikan bahwa petugas yang mempunyai hak akses saja yang dapat menggunakan aplikasi *primary care*.

Hal tersebut juga disampaikan oleh informan triangulasi sumber yang menyatakan bahwa setiap petugas dapat melihat semua menu yang tersedia pada aplikasi, selain melihat petugas juga dapat mengakses semua menu yang ada pada aplikasi *primary care* ini yang akan berdampak kepada data pasien yang ada. Berikut adalah kutipan wawancaranya:

Kotak 11

“Disini aplikasi *Pcare* akses nya sama aja, semua *user* menunya sama dan bisa kapan saja dibuka dan dilihat” (TS 1)

Verifikasi pada aspek *authentication* di aplikasi *primary care* puskesmas Gamping I ini belum maksimal karena belum menerapkan otentikasi 2 faktor untuk login pengguna, tidak ada pemberitahuan kepada email maupun sms untuk memastikan apakah benar petugas tersebut yang memiliki akun ataupun bukan, hanya saja pada aplikasi *primary care* terdapat kode verifikasi yang perlu diisi oleh petugas agar bisa *login* ke aplikasi *primary care*.

4. Aspek *Availability*

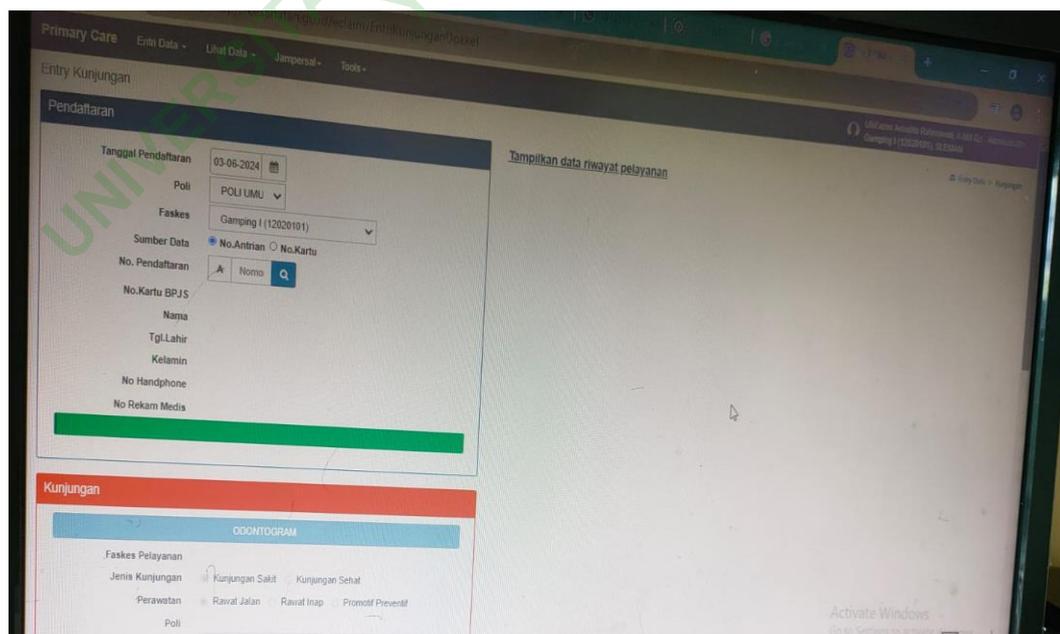
Pengguna menilai kelengkapan data dan menu yang tersedia pada aplikasi *primary care* sudah cukup mudah dimengerti dan sudah sangat lengkap. Hal tersebut dilihat dari pernyataan responden berikut:

Kotak 12

“Bagus banget, udah jelas, dan mudah dipahami aja“ (IU 1)

“Cukup bagus, cukup sederhana, gaterlalu ribet menurut saya mudah dipahami”(IU 2,3,4)

Dari hasil wawancara diketahui bahwa ketersediaan yang ada pada aplikasi *primary care* seperti fitur informasi tagihan, fasilitas Kesehatan, pendaftaran pasien, data pasien, history pasien, menu lain nya seperti menu tagihan yang ada sudah cukup dimengerti dan dipahami oleh pengguna.



Gambar 6 Menu awal pada aplikasi *primary care*

Gambar 6 menunjukkan menu awal pada aplikasi *primary care* yang terdiri kolom pendaftaran dan kunjungan, kolom pendaftaran terdiri dari tanggal pendaftaran ditunjukkan untuk melihat kapan pasien mendaftar, poli, faskes, sumber data, nomor pendaftaran. Jika semua sudah terisi dengan benar lalu tekan tombol pencarian pada nomor pendaftaran tersebut setelah itu nomor kartu dan lainnya akan muncul.

Hal tersebut juga disampaikan oleh informan triangulasi yang menyatakan bahwa menu yang tersedia, kelengkapan data yang ada aplikasi *primary care* sudah sangat lengkap dan mudah dimengerti, menu pada aplikasi sudah cukup jelas dan mudah digunakan untuk para penggunanya, berikut adalah kutipan wawancaranya.

Kotak 13

“Sudah bagus dan jelas si aplikasi *Pcare* ini” (TS 1)

Dari penjelasan di atas dapat diketahui bahwa menu yang ada pada aplikasi dan informasi pada aplikasi *primary care* sudah lengkap dengan adanya menu yang terdapat pada aplikasi *primary care* diantaranya seperti informasi tagihan, fasilitas Kesehatan, pendaftaran pasien, data pasien, histori pasien. Dengan kelengkapan menu yang ada pada aplikasi *primary care* memudahkan petugas melakukan pelayanan dan memudahkan petugas untuk mendapatkan informasi data pasien.

5. Aspek *Non – reputation*

Pengguna menilai bahwa perubahan data dapat disangkal karena tidak ada pemberitahuan untuk perubahan data nya. Hal tersebut dilihat dari pernyataan responden berikut :

Kotak 14

“Biasanya kalau isinya gabener aplikasi gamau nyimpen nanti ada tanda merah merah nya ini, kalau ini udah selesai nanti kita cross check ke simpus” (IU 3)

“Kalau apa yang kita tulis bisa diliat de, karna ada history layanan nya tapi data langsung dikirim ke pusat BPJS jadi biasanya aman” (IU 4)

“Kita gatau siapa yang ubah atau data itu diubah juga kita gatau” (IU 2)

Dari hasil wawancara diketahui bahwa pada perubahan data tidak dapat diketahui siapa yang mengubahnya, tidak diketahui jam dan tanggalnya. Apa saja yang diubah contohnya seperti diagnosis, data sosial pasien dan lain lain. Tetapi jika terdapat kesalahan input data aplikasi tidak mau menyimpan data tersebut. Hal tersebut yang menyebabkan seseorang mudah untuk menyangkal dalam perubahan data tersebut dan sangat berdampak pada keamanan di aplikasi *primary care*. Pemulihan data pada aplikasi *primary care* jika terjadi bencana dapat dipulihkan kembali karena data–data yang ada pada aplikasi langsung dikirimkan ke pusat BPJS jadi untuk keamanan data rekam medis pada puskesmas Gamping I bisa terjaga dengan baik.

Hal tersebut juga disampaikan oleh informan triangulasi yang menyatakan bahwa tidak dapat diketahui dan tidak ada pemberitahuan jika seseorang merubah data yang sudah tersimpan pada aplikasi *primary care* tetapi jika ada kesalahan data pada penginputan data pasien jika tidak sesuai tidak bisa tersimpan kepusatnya.

Kotak 15

“Kalau perubahan yang dilakukan petugas tidak ada pemberitahuan nya sih, kalau informasi kita punya grup nya tersendiri”(TS 1)

“Dilacak sih gabisa, cuman bisa liat dari history tetapi untuk pemulihan data jika terkena bencana bisa diambil dari BPJS soalnya data tersebut kan di kirim” (TS 1)

Dari penjelasan diatas dapat diketahui jika setiap perubahan yang dilakukan tidak dapat diketahui siapa yang mengubahnya, karena tidak ada pemberitahuan yang muncul jika seseorang telah mengubah data yang telah diinput pada aplikasi tersebut jadi seseorang dapat dengan mudah menyangkal jika bukan dia yang mengubah nya karen tidak ada bukti kuat. Sedangkan jika

informasi–informasi yang ada itu melalui grup yang telah disediakan oleh BPJS Kesehatan langsung, untuk mengetahui adakah informasi terbaru atau tentang *maintance* yang terjadi sewaktu- waktu pada aplikasi *primary care*. Pemulihan data pada aplikasi *primary care* dapat dipulihkan kembali karena data yang telah diinputkan ke aplikasi langsung tersimpan ke pusat BPJS.

D. Pembahasan

1. Aspek *Privacy*

Karena data pasien tersimpan dalam aplikasi *primary care*, setiap pengguna harus menggunakan *username* dan *password* yang berbeda, sehingga orang yang tidak berkepentingan tidak dapat mengaksesnya. Setiap *username* dan *password* yang berbeda menjadikan petugas memiliki akses personal, dengan adanya akses sendiri yang dimiliki oleh petugas tersebut memudahkan untuk setiap petugas menginputkan data, mengawasi, mengontrol penggunaan aplikasi *primary care* dan data pasien yang ada di dalamnya. Ini sejalan dengan penelitian sebelumnya. Privasi atau kerahasiaan adalah upaya untuk mencegah pihak yang tidak berwenang mengakses informasi. Penyalahgunaan data medis yang disimpan dan disebarluaskan secara elektronik dapat merugikan pasien. Penting untuk memastikan bahwa rekam medis pasien aman dan aman dari segi keamanan dan privasi. Pengelolaan data pasien adalah bagian dari privasi ini, dan mencakup proses pengumpulan data, pengelolaan kualitas data, dan pengaturan akses ke data (Sofia et al., 2022).

Serupa dengan penelitian sebelumnya, privasi merupakan hak yang melekat pada setiap individu yang harus dilindungi dengan baik. Oleh karena itu, setiap aplikasi atau sistem harus memiliki kebijakan privasi yang menjelaskan tanggung jawab operasional dalam melindungi hak privasi individu yang telah mengungkapkan data mereka. Penelitian sebelumnya menunjukkan bahwa keamanan data pasien terkait dengan aspek privasi mencapai 70% dari total aspek yang diperhatikan, karena aplikasi perlu menambahkan regulasi dan standar operasional, serta memberikan jaminan atas

keamanan, integritas, kerahasiaan, dan ketersediaan informasi yang tersimpan sebagai data rekam medis elektronik pengguna. (Yulianengtiyas et al., 2023).

2. Aspek *integrity*

Perubahan pada data di aplikasi *primary care* puskesmas Gamping I yaitu dapat diubah oleh seluruh pemilik *username* dan *password*, sedangkan pada penelitian sebelumnya penghapusan data atau perubahan data yang aplikasi harus menghubungi rekam medis dan meminta dilakukan penghapusan atau perubahan terhadap data yang salah serta memberikan alasan yang jelas. Hal ini dapat mengurangi kesalahan pada aspek pengguna, salah satu diantaranya yaitu terhapus. *Human eror*, yaitu kesalahan yang sering disebabkan oleh factor manusia seperti kelelahan atau kurangnya pelatihan, dapat menyebabkan data salah. Oleh karena itu, penting untuk memberikan penjelasan yang jelas mengenai penyebab kesalahan data agar dapat dihindari dimasa mendatang (Desti Irlaili , 2018).

Berbeda dengan peneliti sebelumnya, pada RSUD Ratu zalecha Martapura perubahan signifikan dalam sistem harus melalui konfirmasi dari bagian IT. Bagian IT akan melakukan perubahan dengan persetujuan dari semua pihak yang terlibat, karena tanpa prosedur seperti itu, integritas data yang meliputi keakuratan, konsistensi, dan kelengkapan dari data tersebut dapat terganggu. Kondisi ini dapat menimbulkan risiko besar terhadap perubahan informasi dan bahkan pemalsuan data asli pasien (Sofia et al., 2022).

Dalam penelitian ini, kita dapat melihat bahwa tidak ada pemberitahuan yang diberikan untuk setiap perubahan dan penghapusan data pasien. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis Elektronik, menegaskan bahwa pentingnya jaminan terhadap keakuratan data dan informasi dalam rekam medis elektronik, serta bahwa perubahan data hanya dapat dilakukan oleh individu yang memiliki otorisasi untuk melakukannya.

3. Aspek *authentication*

Akses aplikasi *primary care* di puskesmas Gamping I menunjukkan bahwa setiap petugas yang mempunyai *username* dan *password* dapat

menggunakan aplikasi *primary care*. Petugas yang mempunyai *username* dan *password* dinilai belum maksimal menjaga keamanan data pada aplikasi *primary care* dikarenakan setiap petugas dapat mengakses semua menu dan dapat mengganti data dengan mudah.

Authentication berkaitan dengan proses akses terhadap informasi. Dalam konteks rekam medis, tidak semua tenaga kesehatan memiliki wewenang untuk memasukkan atau mengubah data. Setiap tenaga kesehatan memiliki tingkat akses yang berbeda-beda, sehingga penting untuk melakukan pembatasan akses yang sesuai. Setiap perubahan yang dilakukan harus dijalankan dengan pertanggungjawaban yang jelas. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mengamanatkan bahwa dalam pencatatan rekam medis dengan menggunakan teknologi informasi elektronik, kewajiban untuk memberikan tanda tangan dapat digantikan dengan *Personal Identification Number* (PIN) atau sandi.

Password pengguna aplikasi *primary care* sudah ditentukan masa berlakunya sehingga pengguna tidak bisa menggunakan *password* yang awal jika masa berlakunya sudah habis, dan otomatis langsung *off* harus menggantinya dengan yang baru. Hal ini sama dengan penelitian Isa I (2019), keamanan data adalah prioritas utama dalam era digital saat ini. Salah satu langkah penting untuk menjaga keamanan data adalah dengan mengganti kata sandi secara berkala. Idealnya, kata sandi harus diganti minimal tiga bulan sekali. Namun, untuk sistem yang dimiliki risiko tinggi terhadap serangan siber, pergantian kata sandi yang lebih sering sangat disarankan. Dengan rutin mengganti kata sandi, pengguna dapat meminimalisir risiko peretasan dan melindungi data dari akses yang tidak sah.

Penelitian sebelumnya yang di lakukan oleh Mahardika (2020), menjelaskan bahwa proses pengiriman kode otentikasi ganda menggunakan SMS sangat tergantung pada pulsa. Kemungkinan gagalnya kode terkirim karena pulsa habis sangat mungkin terjadi, maka pemanfaatan *E-mail* guna mengirimkan kode otentikasi tanpa terhalang pulsa dan hemat biaya. Sedangkan di Puskesmas Gamping I tidak ada proses verifikasi ganda menggunakan email

maupun sms, oleh karena itu siapa saja bisa dengan mudah menggunakan dan petugas masih bisa menggunakan akun milik petugas lainnya. 2FA merupakan fitur keamanan yang sangat berguna dalam melindungi akun online. Meskipun tidak ada jaminan mutlak bahwa data anda akan selalu aman, 2FA memberikan lapisan keamanan data tambahan yang sangat penting. Dengan mewajibkan pengguna untuk memasukkan kode verifikasi yang dikirimkan ke perangkat terdaftar, 2FA membuat proses login menjadi lebih sulit bagi peretas. Namun, penting untuk diingat bahwa keamanan akun juga bergantung pada faktor-faktor lain, seperti ekuatan kata sandi dan kebiasaan online yang baik.

Peneliti sebelumnya yang dilakukan oleh Raka Herdiantoro (2023), menyatakan bahwa Mekanisme otentikasi dua faktor (2FA) telah terbukti efektif dalam meningkatkan keamanan website. Dengan adanya 2FA, pelaku kejahatan siber tidak hanya perlu mendapatkan kredensial login pengguna, tetapi juga harus memperoleh akses ke akun email yang terkait. Hal ini secara signifikan meningkatkan kesulitan bagi pelaku untuk melakukan serangan siber. Namun, penggunaan sistem whitelist sebagai lapisan keamanan tambahan dapat menimbulkan tantangan bagi pengguna yang sering berpindah-pindah jaringan. Jika pengguna mencoba mengakses sistem dari jaringan yang tidak terdaftar dalam whitelist, mereka akan terblokir meskipun telah memasukkan kode verifikasi yang benar. Oleh karena itu, perlu dilakukan pertimbangan yang matang dalam implementasi sistem whitelist untuk menyeimbangkan antara keamanan dan kenyamanan pengguna. Berbeda dengan Puskesmas Gamping I belum diterapkannya otentikasi ganda untuk menggunakan aplikasi *primary care* tidak ada pemberitahuan ke email maupun sms untuk memastikan apakah benar itu petugas yang mempunyai *user* dan *password* tersebut atau bukan, tetapi hanya ada pengisian kode verifikasi sesuai dengan gambar yang muncul dan itu sangat memudahkan petugas lain untuk meminjam atau memakai *user* dan *password* milik petugas lainnya.

4. Aspek *availability*

Aplikasi *primary care* di Puskesmas Gamping I diperuntukan bagi pengguna, seperti petugas pendaftaran, dokter, farmasi, perawat, rekam medis,

kepala instalansi, dan lain-lain. Ketersediaan informasi, data, fitur yang ada pada aplikasi *primary care* sudah maksimal, cukup lengkap bagi petugas nya. Sesuai dengan penelitian sebelumnya, integritas dapat memastikan bahwa pengguna dapat mengakses informasi secara bebas gangguan dan dalam format yang dapat digunakan, dengan metode seperti patching dan pencadangan data. (Dwinanto & Setiyani, 2021)

Peneliti sebelumnya menyatakan *availability* atau ketersediaan yaitu pengguna *username* dan *password* merupakan salah satu bentuk autentification yang bertujuan untuk memverifikasi data identitas pengguna sebelum memberikan akses ke data. Namun, autentikasi saja tidak cukup untuk menjamin ketersediaan data. Sistem juga harus dirancang agar dapat di akses secara terus-menerus. contoh penerapan *availability* adalah dengan menggunakan *username* dan *password* sebelum mengakses data yang ada didalam *web app*. Aspek *availability* adalah faktor yang berkaitan dengan ketersediaan informasi pada saat dibutuhkan. Oleh karena itu, harus dapat menjamin bahwa pengguna informasi yang sah selalu memiliki akses ke sumber daya dan informasi mereka sendiri. Implementasinya meliputi penambahan *password* pada data sensitif pada aplikasi rekam medis untuk memastikan bahwa pengguna sah dan berwenang untuk menggunakan informasi tersebut, Irma Listiani et al., (2022) Sedangkan Puskesmas Gamping I untuk melihat ketersediaan data atau mengakses menu sudah menggunakan *username* dan *password* yang berbeda setiap pengguna tetapi setiap pengguna dapat mengakses menu yang sama dan tidak ada keterbatasan khusus.

5. Aspek *non-repudiation*

Non repudiation adalah terkait dengan suatu transaksi atau perubahan informasi di mana aspek ini mencegah seseorang untuk menyangkal bahwa mereka telah melakukan transaksi atau perubahan tersebut. Implementasi non repudiation dalam aplikasi *primary care* di Puskesmas Gamping I belum optimal karena tidak ada mekanisme identifikasi yang memastikan siapa yang melakukan pengisian dan perubahan data pasien pada aplikasi *primary care*. Berbeda dengan penelitian sebelumnya di mana setiap input atau penghapusan

data dalam rekam medis elektronik menyebabkan pemberitahuan langsung muncul dalam *log file* yang dikelola oleh bagian IT. Sistem elektronik yang dijalankan wajib menyediakan *audit trail* untuk semua kegiatan operasional sistem elektronik. *Audit trail* ini digunakan untuk tujuan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, uji coba, dan pemeriksaan lainnya (Saputra & Kurniadi, 2019).

Pada penelitian sebelumnya di RSUD dr. Moewardi, disebutkan bahwa aspek *non repudiation* belum diterapkan dengan baik, sehingga sistem tidak dapat mengidentifikasi pengguna yang telah melakukan perubahan informasi pada rekam medis elektronik pasien. Hal ini dapat memungkinkan pengguna untuk dengan mudah menyangkal bahwa mereka telah melakukan transaksi dalam sistem elektronik tersebut, yang berpotensi menimbulkan risiko ketidakamanan rekam medis dari pihak yang tidak bertanggung jawab. Sama seperti di puskesmas Gamping I ini petugas dengan mudah menyangkal jika ada perubahan data atau kehilangan data pasien karena tidak adanya pemberitahuan siapa saja yang mengganti, mengubah dan menghapus data pasien yang sudah ada pada aplikasi *primary care*. (Sofia et al., 2022).

E. Keterbatasan penelitian

Keterbatasan yang dihadapi penelitian ini hanya menggunakan data kualitatif tidak mendapatkan data kuantitatif.