

รายการประมวลผลข้อมูลส่วนบุคคล (ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์

รหัสกิจกรรม	ชื่อกิจกรรมการประมวลผล	ฝ่าย/กลุ่มงานที่รับผิดชอบ	วันที่บันทึก
ROPA-REF-001	ระบบส่งต่อผู้ป่วย (Referral System)	ศูนย์ Refer กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-HIS-002	ระบบเวชระเบียนอิเล็กทรอนิกส์ (HIS / EHR):	งานเวชระเบียน กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-LINE-003	ระบบนัดหมายและบริการออนไลน์ (เช่น LINE Official Account / SCH Connect)	งานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-PACS-004	ระบบสารสนเทศรังสีวินิจฉัยและภาพถ่ายทางการแพทย์ (PACS)	กลุ่มงานรังสีวินิจฉัย กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-REG-005	ระบบทะเบียนมะเร็งและวิจัย (Cancer Registry / Clinical Trials)	งานทะเบียนมะเร็ง คณะกรรมการวิจัย กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-TELM-006	ระบบการแพทย์ทางไกล (Telemedicine / Tele-Oncology)	OPD งานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569
ROPA-CCTV-007	ระบบกล้องวงจรปิด (CCTV) และระบบลงทะเบียนผู้มาติดต่อ	งานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์ DPO	5 พ.ย.2569

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-REF-001	**ระบบส่งต่อผู้ป่วย (Referral System)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อใช้ในการประสานงาน ส่งตัว รับตัว และให้บริการรักษาพยาบาลอย่างต่อเนื่องแก่ผู้ป่วยโรคมะเร็งระหว่างสถานพยาบาล • เพื่อการวินิจฉัยทางการแพทย์ การบำบัดรักษา และการบริหารจัดการด้านสาธารณสุขให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task) เพื่อการดำเนินการตามหน้าที่ในการให้บริการสาธารณสุขของรัฐ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): ฐานความจำเป็นในการบำบัดรักษาทางการแพทย์ (Medical Diagnosis / Treatment) ตามมาตรา 26(5)(ก) แห่ง พ.ศ. 2562
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยของโรงพยาบาลมะเร็งสุราษฎร์ธานี (ทั้งผู้ป่วยใน IPD และผู้ป่วยนอก OPD) • ญาติ หรือผู้แทนโดยชอบธรรมของผู้ป่วย (กรณีติดต่อประสานงานแทน)
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลทั่วไป: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก), วันเดือนปีเกิด, อายุ, ที่อยู่, เบอร์โทรศัพท์, ข้อมูลญาติที่ติดต่อได้ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): ข้อมูลสุขภาพ, ประวัติการรักษาพยาบาล, ผลการวินิจฉัยโรค, ผลตรวจทางห้องปฏิบัติการ (Lab), ผลชิ้นเนื้อ (Pathology Report), ภาพถ่ายรังสีวินิจฉัย (X-ray, CT, MRI), แผนการรักษา, ประวัติการแพ้ยา/สารเคมีบำบัด
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: แพทย์เจ้าของไข้, พยาบาลประจำตึก/ห้องตรวจ, เจ้าหน้าที่เวชระเบียน, และเจ้าหน้าที่ศูนย์รีเฟอร์ • ภายนอกองค์กร: โรงพยาบาลต้นทางที่ส่งตัวมา หรือโรงพยาบาลปลายทางที่รับส่งต่อ (เช่น โรงพยาบาลมหาราชนครศรีธรรมราช, โรงพยาบาลสุราษฎร์ธานี และสถานพยาบาลในเครือข่ายภาคใต้ตอนบน) • ระบบเครือข่ายกลาง: ระบบ Thai Refer, ระบบ Health Data Center (HDC) ของกระทรวงสาธารณสุข

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-REF-001	**ระบบส่งต่อผู้ป่วย (Referral System)**
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี • มี (ระบุประเทศปลายทางและมาตรการคุ้มครอง: .....)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• จัดเก็บในระบบเวชระเบียนอิเล็กทรอนิกส์ (HIS) และระบบส่งต่อเป็นเวลา อย่างน้อย 5 ปี นับจากวันที่ผู้ป่วยสิ้นสุดการรักษากับโรงพยาบาล (หรือเป็นไปตามระเบียบกระทรวงสาธารณสุขว่าด้วยการทำลายเวชระเบียน)
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค: • จำกัดสิทธิ์เข้าถึงข้อมูลตามหน้าที่ (Role-Based Access Control) • ยืนยันตัวตนสองชั้น (2FA) สำหรับบุคลากรทางการแพทย์ก่อนเข้าระบบส่งต่อ • เข้ารหัสข้อมูลระหว่างการส่งผ่านเครือข่าย (Encryption in Transit) ผ่านระบบ VPN หรือ TLS 1.3 • เปิดระบบบันทึกประวัติการเข้าใช้งานข้อมูล (Audit Log) • มาตรการเชิงบริหารจัดการ: • จัดทำข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA) ร่วมกับโรงพยาบาลภาคีเครือข่าย • จัดอบรมด้านความรอบรู้ PDPA ให้แก่เจ้าหน้าที่ศูนย์ส่งต่อผู้ป่วยปีละ 1 ครั้ง
ผู้บันทึกรายการ: นางปนัดดา กลับรินทร์ นักวิชาการสาธารณสุขชำนาญการ วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-HIS-002	**ระบบเวชระเบียนอิเล็กทรอนิกส์ (HIS / EHR)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อจัดทำและจัดเก็บประวัติการรักษาพยาบาลของผู้ป่วยโรคมะเร็งอย่างเป็นระบบ • เพื่อใช้ประกอบการวินิจฉัยทางการแพทย์ การวางแผนการรักษา (ผ่าตัด/เคมีบำบัด/รังสีรักษา) การสั่งยา และการพยาบาล • เพื่อการบริหารจัดการสิทธิ์ค่ารักษาพยาบาล (เช่น บัตรทอง, ประกันสังคม, จ่ายตรงกรมบัญชีกลาง) • เพื่อสถิติทางการแพทย์และการรายงานข้อมูลตามหน้าที่ที่กฎหมายกำหนด
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: • ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task): การปฏิบัติหน้าที่ในการให้บริการสาธารณสุขและการรักษาพยาบาลขององค์กรภาครัฐ • ฐานการปฏิบัติตามกฎหมาย (Legal Obligation): ตาม พ.ร.บ.สถานพยาบาล และ พ.ร.บ.วิชาชีพเวชกรรม • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): • ฐานความจำเป็นในการบำบัดรักษาทางการแพทย์ (Medical Diagnosis / Treatment): ตามมาตรา 26(5)(ก) แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยของโรงพยาบาลมะเร็งสุราษฎร์ธานี (ทั้งผู้ป่วยนอก OPD และผู้ป่วยใน IPD) • ผู้ใช้อำนาจปกครอง หรือผู้แทนโดยชอบธรรมของผู้ป่วย (กรณีผู้ป่วยเป็นผู้เยาว์ หรือผู้ไร้ความสามารถ)
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลทั่วไป: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก) หรือเลข Passport, วัน เดือนปีเกิด, สัญชาติ, ที่อยู่, เบอร์โทรศัพท์, อีเมล, ข้อมูลผู้ติดต่อฉุกเฉิน/ญาติสายตรง, สิทธิ์การรักษาพยาบาล • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): ข้อมูลสุขภาพ, อาการสำคัญ (Chief Complaint), ประวัติการเจ็บป่วย, ผลการตรวจร่างกาย, ผลการตรวจทางห้องปฏิบัติการ (Lab/ชิ้นเนื้อ), ภาพถ่ายทางการแพทย์ (X-ray, CT Scan, MRI), รายการยาและประวัติการแพ้ยา/สารเคมี, สัญญาณชีพ (Vital Signs), ข้อมูลพันธุกรรม (หากมีการตรวจเพื่อรักษาโรคมะเร็งเฉพาะบุคคล)

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-HIS-002	**ระบบเวชระเบียนอิเล็กทรอนิกส์ (HIS / EHR)**
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: แพทย์, พยาบาล, เภสัชกร, นักรังสีการแพทย์, เจ้าหน้าที่ห้องปฏิบัติการ, เจ้าหน้าที่เวชระเบียน, และเจ้าหน้าที่การเงินที่มีส่วนเกี่ยวข้องกับการรักษาและสิทธิ์การรักษาของผู้ป่วยรายนั้นๆ • ภายนอกองค์กร: • สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.), กรมบัญชีกลาง, สำนักงานประกันสังคม (เพื่อการเบิกจ่ายค่ารักษา) • กรมการแพทย์ และกระทรวงสาธารณสุข (ตามหน้าที่ระเบียบรายงานข้อมูล) • บริษัทประกันภัยเอกชน (เฉพาะกรณีผู้ป่วยให้ความยินยอมเปิดเผยข้อมูลเพื่อเคลมประกัน) • สถานพยาบาลเครือข่ายภาคใต้ตอนบน (กรณีการส่งต่อผู้ป่วยตามระบบรีเฟอร์)
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี • มี (ระบุรายละเอียด: .....)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• จัดเก็บข้อมูลในระบบ HIS / EHR ไว้เป็นเวลา อย่างน้อย 5 ปี นับจากปีที่ผู้ป่วยมารับการรักษาพยาบาลครั้งสุดท้าย (ตามระเบียบกระทรวงสาธารณสุขว่าด้วยความลับและเวชระเบียน) หรืออาจเก็บนานกว่านั้นในกรณีที่เป็นข้อมูลเพื่อการศึกษาและวิจัยทางระบาดวิทยาโรคมะเร็ง ภายใต้มาตรการปกปิดตัวตน
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • จำกัดสิทธิ์เข้าถึงข้อมูลด้วยระบบ Role-Based Access Control (RBAC) (เช่น เภสัชกรดูประวัติยาได้แต่ดูภาพ X-ray ไม่ได้, แพทย์เจ้าของไข้ดูข้อมูลได้ทั้งหมด) • บังคับใช้ระบบยืนยันตัวตนสองชั้น (2FA) สำหรับการเข้าถึงระบบจากนอกเครือข่ายโรงพยาบาล (Remote Access) • เปิดใช้งาน Audit Log บันทึกประวัติการ เปิดดู (View), แก้ไข (Edit), หรือดึงข้อมูล (Export) อย่างละเอียดและห้ามลบ Log • เข้ารหัสข้อมูล (Encryption) ทั้งในระบบฐานข้อมูล (At Rest) และระบบการส่งผ่านเครือข่าย (In Transit)

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-HIS-002	**ระบบเวชระเบียนอิเล็กทรอนิกส์ (HIS / EHR)**
	• มาตรการเชิงบริหารจัดการ (Administrative Measures): • ลงนามข้อตกลงรักษาความลับ (Confidentiality Agreement) กับบุคลากรและบริษัทผู้พัฒนาระบบ (Vendor) ทุกราย • จัดอบรมจริยธรรมทางการแพทย์และความรอบรู้ด้าน PDPA ให้บุคลากรผู้ใช้งานระบบทุกปี
ผู้บันทึกรายการ: นางสาวพวงทิพย์ ย้อยด้วง เจ้าพนักงานเวชสถิติชำนาญการ งานเวชระเบียน วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-LINE-003	**ระบบนัดหมายและบริการออนไลน์ (เช่น LINE Official Account / SCH Connect)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อให้บริการนัดหมายแพทย์ล่วงหน้า นัดตรวจคัดกรองมะเร็ง (เช่น มะเร็งปากมดลูก, มะเร็งเต้านม) และการแจ้งเตือนวันนัดหมาย • เพื่ออำนวยความสะดวกในการตรวจสอบสิทธิ์การรักษาและสถานะคิวรับบริการของผู้ป่วย • เพื่อใช้เป็นช่องทางในการสื่อสาร ประชาสัมพันธ์ข้อมูลข่าวสาร ข้อมูลสุขภาพ และตอบคำถามทั่วไปเกี่ยวกับบริการของโรงพยาบาล
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: • ฐานความยินยอม (Consent): ผู้รับบริการกดยอมรับเงื่อนไขการใช้งาน (Terms & Conditions) และนโยบายความเป็นส่วนตัวเมื่อลงทะเบียนผูกบัญชีครั้งแรก • ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task): เพื่อการอำนวยความสะดวกในการเข้าถึงบริการสาธารณสุขของรัฐ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): • ฐานความจำเป็นในการบำบัดรักษาทางการแพทย์ (Medical Diagnosis / Treatment): ประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการจัดคิวนัดตรวจและเตรียมการรักษาพยาบาลล่วงหน้า ตามมาตรา 26(5)(ก) แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยหรือผู้มารับบริการของโรงพยาบาลมะเร็งสุราษฎร์ธานี • ประชาชนทั่วไปที่สนใจลงทะเบียนรับข้อมูลข่าวสารหรือบริการตรวจคัดกรอง
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลทางเทคนิคของแพลตฟอร์ม: LINE User ID, ชื่อโปรไฟล์ (Display Name), รูปภาพโปรไฟล์ • ข้อมูลทั่วไปที่ใช้ยืนยันตัวตน: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก), วันเดือนปีเกิด, เบอร์โทรศัพท์, รหัสเลขประจำตัวผู้ป่วย (HN) • ข้อมูลสุขภาพและการบริการ (Sensitive Data โดยสภาพการใช้งาน): วัน-เวลาที่นัดหมาย, แผนกวิชาชีพที่เข้ารับการตรวจ, ประวัติคิวนัดหมายตรวจคัดกรองมะเร็ง, ประวัติข้อความการสอบถามอาการเบื้องต้นผ่านแชต

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-LINE-003	**ระบบนัดหมายและบริการออนไลน์ (เช่น LINE Official Account / SCH Connect)**
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: เจ้าหน้าที่ผู้ดูแลระบบ (Admin) แผนกประชาสัมพันธ์, พยาบาลประสานงานศูนย์นัดหมาย, และทีมไอทีกลุ่มงานดิจิทัลการแพทย์ • ภายนอกองค์กร: • บริษัท LINE Company (Thailand) Limited (ในฐานะเจ้าของแพลตฟอร์มโครงสร้างพื้นฐาน) • บริษัทผู้พัฒนาและดูแลระบบเชื่อมต่อ API (SCH Connect Developer / Vendor) ที่ได้รับอนุญาตตามสัญญา
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• มี (เนื่องจากเซิร์ฟเวอร์หลักของแพลตฟอร์ม LINE ตั้งอยู่ต่างประเทศ เช่น ประเทศญี่ปุ่น/สิงคโปร์ แต่เป็นการส่งผ่านบริการที่เป็นไปตามมาตรามาตรฐานความปลอดภัยไอทีระดับสากล)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• ข้อมูลประวัติการแชตและการลงทะเบียนบน LINE OA จะจัดเก็บไว้ตลอดระยะเวลาที่ผู้ใช้ยังคงเป็นเพื่อน (Follower) และผูกบัญชีกับระบบ • กรณีที่ผู้ใช้ยกเลิกการผูกบัญชี (Unlink) หรือบล็อก (Block) ระบบจะทำการระงับการเชื่อมโยงข้อมูลกับระบบ HIS ทันที และจะลบข้อมูลล็อกอินออกจากระบบ SCH Connect ภายใน 30 วัน
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • จำกัดข้อมูลสุขภาพที่แสดงผลบนหน้าจอ LINE (Data Minimization) เช่น แสดงเฉพาะ วัน เวลา และแผนก โดย ไม่แสดงชื่อโรค ผลวินิจฉัย หรือรายละเอียดชิ้นเนื้อ บนหน้าจอแชตโดยตรง • ใช้ระบบยืนยันตัวตน (Authentication) เพื่อผูกสิทธิ์ HN ของผู้ป่วยเข้ากับ LINE User ID อย่างปลอดภัยในครั้งแรก • เชื่อมต่อข้อมูลระหว่างระบบนัดหมายออนไลน์และระบบเวชระเบียนโรงพยาบาล (HIS) ผ่านระบบ API ที่มีการเข้ารหัสความปลอดภัย (Secure API Token / HTTPS) • จำกัดสิทธิ์เจ้าหน้าที่แอดมิน (Admin Role) ในการเข้าหลังบ้านของ LINE OA ตามหน้าที่ความรับผิดชอบ

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-LINE-003	**ระบบนัดหมายและบริการออนไลน์ (เช่น LINE Official Account / SCH Connect)**
	• มาตรการเชิงบริหารจัดการ (Administrative Measures): • จัดทำ Data Processing Agreement (DPA) ร่วมกับบริษัทผู้พัฒนาระบบ SCH Connect เพื่อควบคุมไม่ให้นำข้อมูลผู้ป่วยไปใช้ในวัตถุประสงค์อื่น • จัดทำ Privacy Notice ชี้แจงสิทธิ์และหน้าที่อย่างชัดเจนบนหน้าลงทะเบียนระบบนัดหมาย

ผู้บันทึกรายการ: นายชัชพล จันทร์ทอง นักวิชาการคอมพิวเตอร์ งานคอมพิวเตอร์

วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569

ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-PACS-004	**ระบบสารสนเทศรังสีวินิจฉัยและภาพถ่ายทางการแพทย์ (PACS)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อจัดเก็บและบริหารจัดการภาพถ่ายรังสีวินิจฉัยของผู้ป่วยโรคมะเร็ง (เช่น ภาพ X-ray, CT Scan, MRI, Mammogram, Ultrasound) ในรูปแบบดิจิทัล (DICOM format) • เพื่อใช้ประกอบการตรวจวินิจฉัย การวางแผนการรักษาทางรังสีวิทยา การผ่าตัด และการติดตามผลการรักษาโรคมะเร็งของแพทย์ผู้เชี่ยวชาญ • เพื่อใช้เปรียบเทียบผลการเปลี่ยนแปลงของรอยโรคโรคมะเร็งในแต่ละช่วงเวลาของการรักษา
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: • ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task): การดำเนินการตามหน้าที่ในการให้บริการสาธารณสุขและการรักษาพยาบาลของรัฐ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): • ฐานความจำเป็นในการบำบัดรักษาทางการแพทย์ (Medical Diagnosis / Treatment): ประมวลผลเพื่อวัตถุประสงค์ในการวินิจฉัยโรคและบำบัดรักษาโรคทางการแพทย์ ตามมาตรา 26(5)(ก) แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยของโรงพยาบาลมะเร็งสุราษฎร์ธานีที่เข้ารับการตรวจทางรังสีวินิจฉัย
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลระบุตัวตนบนภาพถ่าย (DICOM Metadata): ชื่อ-นามสกุล, เลขประจำตัวผู้ป่วย (HN), เลขประจำตัวประชาชน (13 หลัก), วันเดือนปีเกิด, เพศ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): ภาพถ่ายรังสีวินิจฉัยภายในและภายนอกร่างกาย, รายงานผลการอ่านภาพรังสีโดยรังสีแพทย์ (Radiology Report), ตำแหน่งและขนาดของก้อนเนื้อ/รอยโรคโรคมะเร็ง, ข้อมูลสรีระที่ปรากฏในภาพถ่าย
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: รังสีแพทย์, นักรังสีการแพทย์, แพทย์เจ้าของไข้/แพทย์ผู้ทำการรักษา, พยาบาลประจำศูนย์รังสี และทีมผู้ดูแลระบบไอที

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-PACS-004	**ระบบสารสนเทศรังสีวินิจฉัยและภาพถ่ายทางการแพทย์ (PACS)**
	• ภายนอกองค์กร: สถานพยาบาลต้นทางหรือปลายทาง (เฉพาะกรณีผู้ป่วยมีใบส่งตัวในระบบ Referral System และได้รับการประสานงานเพื่อส่งต่อข้อมูลภาพเพื่อการรักษาต่อเนื่อง)
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี (ระบบจัดเก็บใน On-Premise Server หรือ Private Cloud ภายในประเทศ) • มี (ระบุรายละเอียด: .....)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• จัดเก็บข้อมูลไฟล์ภาพและรายงานผลในระบบ PACS ไว้เป็นเวลา อย่างน้อย 5 ปี นับจากวันที่ผู้ป่วยสิ้นสุดการตรวจรักษา หรือจัดเก็บตามระเบียบกระทรวงสาธารณสุข อย่างไรก็ตาม เนื่องจากข้อมูลภาพถ่ายรังสีโรคมะเร็งมีความสำคัญต่อการศึกษาประวัติโรคและการวิจัยระยะยาว โรงพยาบาลอาจพิจารณาเก็บรักษาในรูปแบบคลังข้อมูลถาวรโดยจะจำกัดการเข้าถึงอย่างเคร่งครัด
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • จำกัดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่อย่างเคร่งครัด (Role-Based Access Control: RBAC) โดยกำหนดให้เฉพาะกลุ่มงานรังสีและแพทย์ผู้รักษามีสิทธิ์เปิดดูภาพได้ • ระบบการเชื่อมต่อระหว่างเครื่องมือแพทย์ (เครื่อง CT/MRI) ไปยังเซิร์ฟเวอร์ PACS ต้องทำงานผ่านเครือข่ายภายในโรงพยาบาลที่แยกเฉพาะ (Isolated VLAN) • มีระบบบันทึก Audit Log ทุกครั้งที่มีการเรียกดูภาพ (View), ดาวน์โหลด (Export), หรือพิมพ์รายงานผลการตรวจรังสี • การเรียกดูภาพผ่านเว็บหรือระบบภายนอกโรงพยาบาลโดยแพทย์ (ถ้ามี) ต้องผ่านระบบ VPN (Virtual Private Network) และต้องยืนยันตัวตนแบบ 2FA เท่านั้น • มาตรการเชิงบริหารจัดการ (Administrative Measures): • กำหนดนโยบายห้ามเจ้าหน้าที่ใช้หน่วยความจำพกพา (เช่น Flash Drive / External Harddisk) ที่ไม่ได้ลงทะเบียน มารับ-ส่งไฟล์ภาพถ่ายทางการแพทย์เด็ดขาด • กำหนดแนวปฏิบัติการขอรับสำเนาภาพถ่ายทางการแพทย์ (เขียนแผ่น CD/DVD หรือโอนย้ายไฟล์) ให้แก่ผู้ป่วย โดยต้องมีการยืนยันตัวตนเจ้าของข้อมูลอย่างถูกต้องก่อนส่งมอบ

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-PACS-004	**ระบบสารสนเทศรังสีวินิจฉัยและภาพถ่ายทางการแพทย์ (PACS)**
ผู้บันทึกรายการ: นายธัชนนท์ ศรีทอง นักรังสีการแพทย์ชำนาญการ วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-REG-005	**ระบบทะเบียนมะเร็งและวิจัย (Cancer Registry / Clinical Trials)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อจัดทำสถิติ ทะเบียนราษฎร์ และระบาดวิทยาของผู้ป่วยโรคมะเร็งในเขตสุขภาพภาคใต้ตอนบน (Hospital-based และ Population-based Cancer Registry) • เพื่อนำส่งข้อมูลสถิติโรคมะเร็งให้แก่สถาบันมะเร็งแห่งชาติ กรมการแพทย์ ในการวางแผนนโยบายสาธารณสุขระดับประเทศ • เพื่อใช้ศึกษา วิเคราะห์ และทำวิจัยทางคลินิก (Clinical Trials) ในการพัฒนาแนวทางการรักษาโรคมะเร็งชนิดต่างๆ ให้มีประสิทธิภาพยิ่งขึ้น
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: • ฐานการปฏิบัติตามกฎหมาย (Legal Obligation): การรายงานข้อมูลสถิติตามระเบียบกระทรวงสาธารณสุขและภารกิจของกรมการแพทย์ • ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task): เพื่อการดำเนินงานด้านสาธารณสุขและการศึกษาวิจัยที่เป็นประโยชน์ต่อสังคม • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): • ฐานเพื่อประโยชน์สาธารณะด้านการสาธารณสุข (Public Health): ตามมาตรา 26(5)(ข) แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (การคุ้มครองด้านสุขภาพและสถิติสาธารณสุข) • ฐานการศึกษาวิจัยทางวิทยาศาสตร์หรือสถิติ (Scientific or Historical Research / Statistics): ตามมาตรา 26(5)(ง) ซึ่งผ่านการอนุมัติจากคณะกรรมการจริยธรรมการวิจัยในมนุษย์ (IRB) ของสถาบันแล้ว • ฐานความยินยอม (Consent): เฉพาะกรณีโครงการวิจัยทางคลินิก (Clinical Trials) ที่ผู้ป่วยลงนามในเอกสารแสดงความยินยอมเข้าร่วมการวิจัย (Informed Consent Form)
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยที่ได้รับการวินิจฉัยว่าเป็นโรคมะเร็ง (หรือเนื้องอกบางชนิด) ณ โรงพยาบาลมะเร็งสุราษฎร์ธานี • ผู้ป่วยที่สมัครใจเข้าร่วมโครงการวิจัยทางคลินิก

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-REG-005	**ระบบทะเบียนมะเร็งและวิจัย (Cancer Registry / Clinical Trials)**
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลทั่วไปและประชากรศาสตร์: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก), เพศ, วันเดือนปีเกิด, อาชีพ, ที่อยู่ตามทะเบียนบ้านและที่อยู่ปัจจุบัน, สถานะการมีชีวิตอยู่ • ข้อมูลสุขภาพและพยาธิวิทยา (Sensitive Data): วันที่วินิจฉัยโรค, ตำแหน่งอวัยวะที่เกิดมะเร็ง (Primary Site), ลักษณะทางพยาธิวิทยาของเซลล์มะเร็ง (Histology), ระยะของโรคมะเร็ง (Staging), วิธีการรักษาที่ได้รับ (ผ่าตัด/เคมีบำบัด/รังสีรักษา), ผลการตอบสนองต่อการรักษา, สาเหตุการเสียชีวิต (กรณีเสียชีวิต)
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: เจ้าหน้าที่งานทะเบียนมะเร็ง, คณะผู้วิจัยที่ได้รับอนุมัติโครงการ, DPO, และทีมไอทีสนับสนุน • ภายนอกองค์กร: • สถาบันมะเร็งแห่งชาติ กรมการแพทย์ (เพื่อรวมกลุ่มข้อมูลระดับประเทศ) • กองยุทธศาสตร์และแผนงาน กระทรวงสาธารณสุข • สถาบันการศึกษา หรือหน่วยงานวิจัยภาคีเครือข่าย (เฉพาะข้อมูลที่ผ่านกระบวนการจำกัดการระบุตัวตนแล้ว และมีสัญญา DSA ผูกพัน)
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี (กรณีทะเบียนมะเร็งปกติของโรงพยาบาล) • มี (เฉพาะบางโครงการวิจัยทางคลินิกร่วมกับสถาบันนานาชาติ โดยจะต้องระบุมาตรการปกปิดตัวตนและการเข้ารหัสข้อมูลอย่างเข้มงวดก่อนส่งออก)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• ข้อมูลในระบบทะเบียนมะเร็ง (Cancer Registry) จะถูกจัดเก็บไว้เป็นคลังข้อมูลระยะยาว (ถาวร) เนื่องจากมีความจำเป็นอย่างยิ่งต่อการศึกษาอัตราการรอดชีพ (Survival Rate) และระบาดวิทยาในระยะยาว 20-30 ปี โดยข้อมูลที่ถูกนำมาวิเคราะห์ในอดีตจะถูกแปลงเป็นข้อมูลสถิติที่ไม่ผูกพันกับตัวบุคคล • กรณีข้อมูลโครงการวิจัย (Clinical Trials) จะจัดเก็บไว้ตามที่ระบุในโครงร่างการวิจัย (มักกำหนดไว้ที่ 5-10 ปี หลังสิ้นสุดโครงการวิจัย) จากนั้นจะทำการทำลายตามมาตรฐาน
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • ทำ De-identification / Pseudonymization (การตัดชื่อ-นามสกุล เลขบัตรประชาชนออก แล้วแทนที่ด้วยรหัส ID วิจัย) ก่อนส่งมอบข้อมูลให้ผู้วิจัยนำไปวิเคราะห์ • แยกฐานข้อมูลระบบทะเบียนมะเร็งออกจากระบบ HIS หลัก และจำกัดสิทธิ์ให้เข้าถึงได้เฉพาะเจ้าหน้าที่งานทะเบียนมะเร็งที่ได้รับมอบหมายเท่านั้น

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-REG-005	**ระบบทะเบียนมะเร็งและวิจัย (Cancer Registry / Clinical Trials)**
	• มีระบบบันทึก Audit Log ติดตามว่าใครเป็นผู้ดึงไฟล์ข้อมูลสถิติ (Export) ออกจากระบบ • มาตรการเชิงบริหารจัดการ (Administrative Measures): • โครงการวิจัยทุกโครงการที่ใช้ข้อมูลผู้ป่วย ต้องผ่านการรับรองจาก คณะกรรมการจริยธรรมการวิจัยในมนุษย์ (IRB) ก่อนเริ่มดำเนินการประมวลผลข้อมูล • จัดทำข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA) หรือข้อตกลงการประมวลผลข้อมูล (DPA) หากเป็นการร่วมวิจัยกับหน่วยงานภายนอก
ผู้บันทึกรายการ: นายวสันต์ จันทร์สอาด นักวิชการการสถิติ งานทะเบียนมะเร็ง วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-TELM-006	**ระบบการแพทย์ทางไกล (Telemedicine / Tele-Oncology)**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อให้บริการปรึกษาทางการแพทย์ วินิจฉัย ติดตามอาการ และให้คำแนะนำในการรักษาแก่ผู้ป่วยโรคมะเร็งที่ไม่สะดวกเดินทางมาโรงพยาบาล • เพื่อประสานงานการจัดส่งยาเคมีบำบัดชนิดกิน (Oral Chemo) หรือยารักษาประคับประคองไปยังบ้านของผู้ป่วยหรือสถานพยาบาลใกล้บ้าน • เพื่อเก็บบันทึกประวัติการตรวจรักษาทางไกลไว้เป็นหลักฐานในเวชระเบียน
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ข้อมูลส่วนบุคคลทั่วไป: • ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Task): การปฏิบัติหน้าที่บริการสาธารณสุขของรัฐในการขยายการเข้าถึงการรักษา • ฐานความยินยอม (Consent): ผู้ป่วยลงนามหรือกดยอมรับข้อตกลงการเข้ารับบริการแพทย์ทางไกลและการประมวลผลข้อมูลก่อนเริ่มใช้งานระบบ • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): • ฐานความจำเป็นในการบำบัดรักษาทางการแพทย์ (Medical Diagnosis / Treatment): ประมวลผลข้อมูลสุขภาพเพื่อการบำบัดรักษาโรคตามมาตรฐานแพทยสภาและมาตรา 26(5)(ก) แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วยโรคมะเร็งของโรงพยาบาลมะเร็งสุราษฎร์ธานีที่ได้รับความเห็นชอบจากแพทย์ให้รับบริการทางไกลได้ • ญาติหรือผู้ดูแลผู้ป่วย (กรณีร่วมรับฟังการปรึกษาหรือให้ข้อมูลแทนผู้ป่วย)
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ข้อมูลระบุตัวตนและการติดต่อ: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก), เลขประจำตัวผู้ป่วย (HN), ที่อยู่สำหรับจัดส่งยา, เบอร์โทรศัพท์, อีเมล • ข้อมูลมัลติมีเดีย (ขณะให้บริการ): ภาพใบหน้า/สรีระของผู้ป่วย, เสียงสนทนาระหว่างแพทย์และผู้ป่วย, ภาพถ่ายรอยโรคหรือสิ่งผิดปกติที่ผู้ป่วยส่งให้แพทย์ประเมิน • ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data): ข้อมูลอาการปัจจุบัน, ผลข้างเคียงจากการรับยาเคมีบำบัดหรือรังสีรักษา, ประวัติการแพ้ยา, ข้อมูลสัญญาณชีพที่ผู้ป่วยบันทึกมาจากบ้าน (เช่น ความดันโลหิต, ชีพจร)

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-TELM-006	**ระบบการแพทย์ทางไกล (Telemedicine / Tele-Oncology)**
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: แพทย์ผู้ตรวจ, พยาบาลประสานงาน Telemedicine, เภสัชกร (ฝ่ายจัดจ่ายยา), เจ้าหน้าที่เวชระเบียน, และทีมไอทีสนับสนุนระบบ • ภายนอกองค์กร: • บริษัทผู้ให้บริการโครงสร้างพื้นฐานระบบวิดีโอคอล/แพลตฟอร์ม Telemedicine (Vendor) ที่ได้รับอนุญาตตามสัญญา • ไปรษณีย์ไทย หรือบริษัทขนส่งเอกชน (เฉพาะข้อมูลชื่อ ที่อยู่ เบอร์โทรศัพท์ เพื่อการจัดส่งยา)
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี (ใช้เซิร์ฟเวอร์ระบบภายในประเทศ หรือ Private Cloud ที่ผ่านการตรวจสอบความมั่นคงปลอดภัยไซเบอร์) • มี (ระบุรายละเอียด: .....)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• บันทึกสรุปผลการตรวจรักษาทางไกล (Text) จะถูกซิงค์เข้าระบบ HIS หลัก และจัดเก็บไว้เป็นเวลา อย่างน้อย 5 ปี นับจากวันที่มารับการรักษาครั้งสุดท้าย • ไฟล์บันทึกวิดีโอหรือเสียงการสนทนา (ถ้ามีการบันทึกเพื่อประโยชน์ทางการแพทย์) จะจัดเก็บไว้บนคลังข้อมูลที่มีการจำกัดสิทธิ์ขั้นสูงเป็นเวลา ไม่เกิน 1 ปี หรือลบทันทีเมื่อแพทย์บันทึกประวัติลงเวชระเบียนหลักเสร็จสิ้น ยกเว้นเคสที่มีความซับซ้อนทางกฎหมาย
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • ช่องทางการสื่อสารวิดีโอคอลต้องมีการเข้ารหัสแบบ End-to-End Encryption เพื่อป้องกันการดักฟังหรือดักจับข้อมูลระหว่างทาง • กำหนดให้แพทย์และเจ้าหน้าที่ต้องล็อกอินเข้าระบบ Telemedicine ผ่านเครือข่ายภายใน หรือใช้ระบบ VPN + 2FA เท่านั้นหากเข้าจากภายนอก • ข้อมูลภาพถ่ายรอยโรคของผู้ป่วยที่ส่งผ่านแชต ต้องได้รับการอัปโหลดเข้าสู่ระบบจัดเก็บที่ปลอดภัย และมีระบบตั้งเวลาลบไฟล์อัตโนมัติจากเซิร์ฟเวอร์ชั่วคราว • มีระบบ Audit Log บันทึกการเข้าใช้งานระบบ วันเวลา และรายชื่อเจ้าหน้าที่ที่เข้าร่วมในเซสชันการตรวจรักษาทางไกล

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-TELM-006	**ระบบการแพทย์ทางไกล (Telemedicine / Tele-Oncology)**
	• มาตรการเชิงบริหารจัดการ (Administrative Measures): • กำหนดให้เจ้าหน้าที่ปฏิบัติงานใน ห้องปฏิบัติการที่ปิดมิดชิดและเงียบสงบ เพื่อป้องกันไม่ให้บุคคลอื่นได้ยินหรือเห็นหน้าจอการรักษาผู้ป่วย (ป้องกันการรั่วไหลทางกายภาพ) • จัดทำ Data Processing Agreement (DPA) ร่วมกับผู้ให้บริการแพลตฟอร์ม Telemedicine เพื่อควบคุมและห้ามนำภาพ เสียง หรือข้อมูลผู้ป่วยไปประมวลผลต่อเพื่อวัตถุประสงค์อื่น
ผู้บันทึกรายการ: ว่าที่ร้อยตรีจักรพันธุ์ ชาตะเวที นักวิชาการคอมพิวเตอร์ งานคอมพิวเตอร์ วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	

	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-CCTV-007	**ระบบกล้องวงจรปิด (CCTV) และระบบลงทะเบียนผู้มาติดต่อ**
1. สถานะขององค์กร (Activity Details)	• ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) • ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
2. วัตถุประสงค์ในการประมวลผล (Purposes of Processing)	• เพื่อการรักษาความปลอดภัยของอาคาร สถานที่ ทรัพย์สิน ของโรงพยาบาล บุคลากร และผู้ป่วย • เพื่อป้องกัน ระงับ หรือตรวจสอบเหตุอาชญากรรม การลักขโมย อุบัติเหตุ หรือเหตุการณ์ความไม่สงบภายในพื้นที่โรงพยาบาล • เพื่อควบคุมและตรวจสอบการเข้า-ออกพื้นที่หวงห้าม (เช่น คลังยาเสพติดให้โทษ, ศูนย์ข้อมูลคอมพิวเตอร์, ห้องปฏิบัติการรังสี)
3. ฐานทางกฎหมายในการประมวลผล (Lawful Basis)	• ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest): เพื่อประโยชน์ในการรักษาความปลอดภัยทางกายภาพและทรัพย์สินของโรงพยาบาลและบุคคลทั่วไป ซึ่งมีน้ำหนักเหนือกว่าผลกระทบขั้นพื้นฐานต่อความเป็นส่วนตัวในพื้นที่สาธารณะขององค์กร • ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ (Vital Interest): ในกรณีเกิดเหตุฉุกเฉิน อุบัติเหตุร้ายแรง หรือภัยพิบัติที่จำเป็นต้องใช้ภาพวงจรปิดช่วยชีวิตบุคคล • หมายเหตุทางกฎหมาย: กิจกรรมนี้ประมวลผลข้อมูลภาพใบหน้าเพื่อวัตถุประสงค์ด้านความปลอดภัยโดยทั่วไป ไม่ได้นำไปใช้ในระบบระบุตัวตนอัตโนมัติ (Automated Facial Recognition) เพื่อคัดกรองบุคคลในวงกว้าง จึงไม่ถือเป็นการประมวลผลข้อมูลชีวมิติ (Biometrics) ภายใต้มาตรา 26 ที่ต้องขอความยินยอมล่วงหน้า
4. ประเภทของเจ้าของข้อมูล (Categories of Data Subjects)	• ผู้ป่วย ญาติผู้ป่วย และผู้มาติดต่อประสานงานทุกประเภท • เจ้าหน้าที่ บุคลากรทางการแพทย์ และผู้รับเหมาภายนอกที่ปฏิบัติงานในโรงพยาบาล
5. ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ (Categories of Personal Data)	• ระบบกล้องวงจรปิด (CCTV): ภาพนิ่ง ข้อมูลภาพเคลื่อนไหว (วิดีโอ) ของใบหน้า สรีระร่างกาย และพฤติกรรมของบุคคล รวมถึงภาพป้ายทะเบียนยานพาหนะที่เข้ามาในพื้นที่โรงพยาบาล • ระบบลงทะเบียนผู้มาติดต่อ: ชื่อ-นามสกุล, เลขประจำตัวประชาชน (13 หลัก) หรือเลขใบขับขี่, ภาพถ่ายหน้าบัตร, สังกัด/หน่วยงาน, วัตถุประสงค์การมาติดต่อ, บุคคลหรือแผนกที่ต้องการเข้าพบ, วันและเวลาที่เข้า-ออก

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-CCTV-007	**ระบบกล้องวงจรปิด (CCTV) และระบบลงทะเบียนผู้มาติดต่อ**
6. การเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคล (Categories of Recipients)	• ภายในองค์กร: ผู้บริหารโรงพยาบาลที่ได้รับมอบหมาย, หัวหน้างานอาคารสถานที่, เจ้าหน้าที่ศูนย์ควบคุม CCTV และ DPO (กรณีตรวจสอบเหตุละเมิด) • ภายนอกองค์กร: • เจ้าพนักงานตำรวจ หรือหน่วยงานความมั่นคง (เฉพาะกรณีที่มีหนังสือร้องขออย่างเป็นทางการเพื่อการสืบสวนสอบสวนคดีความตามกฎหมาย) • บริษัทผู้ให้บริการรักษาความปลอดภัยภายนอก (Outsource Security) ที่เข้ามาปฏิบัติหน้าที่ตามสัญญา
7. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)	• ไม่มี (ระบบจัดเก็บในเครื่องบันทึก DVR/NVR Local Server ภายในโรงพยาบาล)
8. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Period)	• ข้อมูลภาพถ่ายวิดีโอ CCTV: จัดเก็บไว้เป็นเวลา 30 วัน นับจากวันที่บันทึกภาพ โดยระบบจะทำการบันทึกทับอัตโนมัติ (Loop Recording) ยกเว้นกรณีที่ภาพดังกล่าวถูกดึงออกมาระหว่างกระบวนการสอบสวนเหตุการณ์ ซึ่งจะจัดเก็บจนกว่าคดีหรือการตรวจสอบจะสิ้นสุด • ข้อมูลสมุดอนุทิน/ระบบลงทะเบียนผู้มาติดต่อ: จัดเก็บไว้เป็นเวลา 1 ปี นับจากวันที่เข้ามาติดต่อ จากนั้นจะทำการลบทำลายไฟล์ดิจิทัล หรือทำลายเอกสารกระดาษด้วยเครื่องทำลายเอกสาร
9. มาตรการรักษาความมั่นคงปลอดภัย (Technical & Administrative Security Measures)	• มาตรการเชิงเทคนิค (Technical Measures): • จำกัดสิทธิ์การเข้าถึงห้องควบคุมระบบกล้องวงจรปิด (CCTV Control Room) และสิทธิ์การเปิดดูภาพย้อนหลัง/ดาวน์โหลดวิดีโอเฉพาะผู้ที่ได้รับอนุมัติอย่างเป็นลายลักษณ์อักษรเท่านั้น • เครื่องบันทึกข้อมูลภาพ (NVR/DVR) และระบบลงทะเบียนต้องใช้รหัสผ่านที่ปลอดภัย และมีการบันทึก Audit Log ทุกครั้งที่มีการเข้าดูหรือส่งออกไฟล์ภาพ • ห้ามเชื่อมต่อระบบ CCTV เข้ากับเครือข่ายอินเทอร์เน็ตสาธารณะ โดยให้ทำงานบนเครือข่ายภายในที่ปิดแยกเฉพาะ (Isolated Infrastructure)

กรมการแพทย์ โรงพยาบาลมะเร็งสุราษฎร์ธานี	**แบบฟอร์มบันทึกรายการประมวลผลข้อมูลส่วนบุคคล** **(Records of Processing Activities: ROPA)** **โรงพยาบาลมะเร็งสุราษฎร์ธานี กรมการแพทย์**
ROPA-CCTV-007	**ระบบกล้องวงจรปิด (CCTV) และระบบลงทะเบียนผู้มาติดต่อ**
	• มาตรการเชิงบริหารจัดการ (Administrative Measures): • ติดตั้งป้ายประกาศ CCTV Privacy Notice (บอร์ดแจ้งเตือนการใช้กล้องวงจรปิด) บริเวณทางเข้าหลักของโรงพยาบาลและจุดสำคัญอย่างชัดเจน เพื่อแจ้งให้เจ้าของข้อมูลทราบ • กำหนด Sop แนวทางปฏิบัติในการขอตรวจสอบภาพกล้องวงจรปิดโดยบุคคลภายนอกหรือผู้ป่วยอย่างเคร่งครัด โดยจะต้องขอดูได้เฉพาะมุมที่เห็นตัวเอง และต้องไม่ละเมิดสิทธิ์เห็นภาพบุคคลอื่น (เว้นแต่จะทำการเบลอภาพบุคคลอื่นออกก่อน)
ผู้บันทึกรายการ: นายสมชาย โสมจันทร์ งานคอมพิวเตอร์ วันที่บันทึก/อัปเดตล่าสุด: 5 พฤศจิกายน 2569 ผู้ตรวจสอบ: นางปนัดดา กลับรินทร์ หัวหน้ากลุ่มงานดิจิทัลการแพทย์ ภารกิจด้านพัฒนาระบบสุขภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	