E-mail

กลุ่มดิจิตอลสุขภาพ
เลขรับ 383
วันที่ 9/9/65
เวลา 09.46 น.

ห้อง ผอ.กยผ.
เลขที่ 8629
วันที่ 8/9/65
เวลา 16.50

กองยุทธศาสตร์และแผนงาน
เลขที่ 7817
วันที่ 8 ก.ย. 65
เวลา 10.17

ที่ สพร ๒๕๖๕/๙๙๔

๗ กันยายน ๒๕๖๕

เรื่อง ขอนำส่งความคิดเห็นต่อ (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อม กระทรวงสาธารณสุข

เรียน ผู้อำนวยการกองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุข

อ้างถึง หนังสือกองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๐๙.๑๐/๔๙๒๖ ลงวันที่ ๓ สิงหาคม ๒๕๖๕

สิ่งที่ส่งมาด้วย ความคิดเห็นต่อ (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อม กระทรวงสาธารณสุข จำนวน ๑ ฉบับ

ตามหนังสือที่อ้างถึง กองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุข ขอให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. พิจารณา (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อม กระทรวงสาธารณสุข เพื่อพิจารณาความถูกต้อง เหมาะสม รวมถึงข้อเสนอแนะการดำเนินงานอื่น ๆ เพื่อประกาศใช้เป็นแนวปฏิบัติ ในการกำกับดูแลข้อมูลระบบหมอพร้อมต่อไป นั้น

ในการนี้ สพร. ได้พิจารณาให้ความเห็นต่อ (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อมกระทรวงสาธารณสุข โดยมีความเห็นเพื่อพิจารณา รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ทั้งนี้ ได้มอบหมายให้นายธีรวัฒน์ โรจนไพฑูรย์ หมายเลขโทรศัพท์เคลื่อนที่ ๐๘ ๐๐๔๕ ๓๔๒๖ หรือไปรษณีย์อิเล็กทรอนิกส์ theerawat.rojanapitoon@dga.or.th เป็นผู้ประสานงานกับท่านต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

- มอบดิจิทัล

(นายสุพจน์ เธียรวุฒิ)
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

(นายสุภโชค เวชภัณฑ์เภสัช)
ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

- มอบ กส2 รวบรวม

9 กย 65

กลุ่มงานพัฒนามาตรฐานดิจิทัล
ทีมพัฒนามาตรฐานดิจิทัล ๑
มือถือ ๐๘ ๐๐๔๕ ๓๔๓๗ (พิมพ์ชนก)
ไปรษณีย์อิเล็กทรอนิกส์สารบรรณกลาง saraban@dga.or.th

ความคิดเห็นต่อ (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อม กระทรวงสาธารณสุข

ตามที่กองยุทธศาสตร์และแผนงาน สำนักงานปลัดกระทรวงสาธารณสุข ขอให้พิจารณาให้ความเห็นต่อ (ร่าง) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ระบบหมอพร้อม สพร. ได้เปรียบเทียบกับมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย สามารถสรุปตามบทบาทที่เกี่ยวข้อง ได้แก่ผู้ให้บริการภาครัฐ (Relying Party - RP) ของระบบหมอพร้อม ตามตารางที่ ๑ และบทบาทผู้พิสูจน์และยืนยันตัวตน (Identity Provider : IdP) ของบริการพิสูจน์และยืนยันตัวตน (MOPH DID) ตามตารางที่ ๒ และ ๓

ตารางที่ ๑ การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ของระบบหมอพร้อมซึ่งมีบทบาทเป็นผู้ให้บริการภาครัฐ เทียบกับมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

บริการ	ระดับ IAL ระบบหมอพร้อม	ระดับ AAL ระบบหมอพร้อม	ข้อกำหนดขั้นต่ำการพิสูจน์ยืนยันตัวตนทางดิจิทัล (มรด. ๑-๒:๒๕๖๔)		ผ่านข้อกำหนด[๑]	รายละเอียดความเห็น
			IAL	AAL		
บริการส่วนที่ให้ข้อมูลทั่วไป	IAL1	AAL1	IAL1	IAL1	✓	สอดคล้องกับข้อกำหนดขั้นต่ำ กลุ่มการให้บริการข้อมูลพื้นฐาน
บริการข้อมูลสุขภาพสำหรับประชาชน	IAL2.2	AAL2	IAL2	AAL2	✓	สอดคล้องกับข้อกำหนดขั้นต่ำ กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ ซึ่งบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตน ให้กำหนดระดับความน่าเชื่อถือขั้นต่ำที่ระดับ ๒
บริการส่วนที่เกี่ยวข้องกับข้อมูลสุขภาพ (ข้อมูลการรักษา) สำหรับเจ้าหน้าที่ เช่น แพทย์	IAL2.2	AAL2	IAL2	AAL2	✓	สอดคล้องกับข้อกำหนดขั้นต่ำ กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ โดยหากบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตน ให้กำหนดระดับความน่าเชื่อถือขั้นต่ำที่ระดับ ๒ และ มีการขอความยินยอมจากเจ้าของข้อมูล

หมายเหตุ ๑ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

ทั้งนี้ จากตารางเบื้องต้น สามารถอธิบายพอสังเขปได้ ดังนี้

๑. **บริการส่วนที่ให้ข้อมูลทั่วไป** กำหนดให้ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนระดับต้น (IAL1) และความน่าเชื่อถือของการยืนยันตัวตนระดับต้น (AAL1) ซึ่งพิจารณาแล้วมีขั้นตอนและวิธีการผ่านข้อกำหนดขั้นต่ำในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล และข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล ตามมาตรฐานรัฐบาลดิจิทัลฯ (มรด. ๑-๒:๒๕๖๔) สำหรับกลุ่มการให้บริการข้อมูลพื้นฐาน หรือกลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ ที่ไม่มีแสดงข้อมูลส่วนบุคคล

๒. **บริการข้อมูลสุขภาพสำหรับประชาชน** มีการกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ระดับ IAL2.2 ตามมาตรฐานสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ หรือ สพธอ. (ขมธอ. ๑๙-๒๕๖๕) ซึ่งสอดคล้องกับความน่าเชื่อถือของการพิสูจน์ตัวตนระดับปานกลาง (IAL2) ตามมาตรฐานรัฐบาลดิจิทัลฯ และความน่าเชื่อถือของการยืนยันตัวตนระดับปานกลาง (AAL2) โดยกลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ ที่มีการใช้ข้อมูลส่วนบุคคลต้องกำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับปานกลาง (IAL2) และระดับความน่าเชื่อถือของการยืนยันตัวตนระดับปานกลาง (AAL2)

๓. **บริการส่วนที่เกี่ยวข้องกับข้อมูลสุขภาพ (ข้อมูลการรักษา) สำหรับเจ้าหน้าที่** เช่น แพทย์ มีการกำหนดความน่าเชื่อถือของการพิสูจน์ตัวตนระดับ IAL2.2 ตามมาตรฐาน สพธอ. (ขมธอ. ๑๙-๒๕๖๕) ซึ่งพิจารณาแล้วมีขั้นตอนและวิธีการสอดคล้องกับความน่าเชื่อถือของการพิสูจน์ตัวตนระดับปานกลาง(IAL2) ตามมาตรฐานรัฐบาลดิจิทัลฯ และความน่าเชื่อถือของการยืนยันตัวตนระดับปานกลาง (AAL2) โดยมีการขอความยินยอมจากเจ้าของข้อมูล (Data Owner) โดยบริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการที่มีการใช้ข้อมูลส่วนบุคคลต้องกำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับปานกลาง (IAL2) และระดับความน่าเชื่อถือของการยืนยันตัวตนระดับปานกลาง (AAL2)

๔. **ความเห็นเพิ่มเติมต่อร่างฯ เอกสาร** เนื่องจากมีการแสดงรายละเอียดเป็นภาพรวมทั้งบทบาทผู้ให้บริการพิสูจน์และยืนยันตัวตน (Identity Provider - IdP) ในส่วนของบริการพิสูจน์และยืนยันตัวตน (MOPH ID) และผู้ให้บริการภาครัฐ (Relying Party - RP) ในส่วนของระบบหมอพร้อม โดยกองยุทธศาสตร์และแผนงานได้ปรับปรุงและส่งมอบเอกสารเพิ่มเติม ซึ่งสพร.ได้พิจารณารายละเอียดและสรุปข้อคิดเห็นไว้ในตารางที่ ๒ และตารางที่ ๓

ตารางที่ ๒ การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ของบริการพิสูจน์และยืนยันตัวตน (MOPH DID) ของกระทรวงสาธารณสุข ตามบทบาทผู้พิสูจน์และยืนยันตัวตน (Identity Provider : IdP)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ที่ให้บริการ	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น IAL1			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง IAL2			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับสูง IAL3		
	MOPH DID	มรด.	ผ่านข้อกำหนด[๒]	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด
การแสดงตน (Presences)	ไม่มีการแสดงตน	ไม่มีข้อกำหนด	✓	แบบพบเห็นต่อหน้า ณ หน่วยบริการ หรือที่ "หมอพร้อม Station" (โดยผู้ประกอบวิชาชีพ[๑])	แบบพบเห็นต่อหน้า หรือ แบบไม่พบเห็นต่อหน้า	✓	แบบพบเห็นต่อหน้า ณ หน่วยบริการ หรือที่ "หมอพร้อม Station" (โดยผู้ประกอบวิชาชีพ[๑])	แบบพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า	✓
รวบรวมข้อมูลเพื่อระบุตัวตน (Resolution)	มีการรวบรวมข้อมูล	มีการรวบรวมข้อมูล หรือไม่ก็ได้	✓	มีการรวบรวมข้อมูล	มีการรวบรวมข้อมูล	✓	มีการรวบรวมข้อมูล	มีการรวบรวมข้อมูล	✓
การขอหลักฐานแสดงตน (Evidence)	ขอหลักฐานบัตรประชาชน	ขอหลักฐานหรือไม่ก็ได้	✓	ขอหลักฐานบัตรประชาชน	ขอหลักฐาน	✓	ขอหลักฐานบัตรประชาชน	ขอหลักฐาน	✓

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ที่ให้บริการ	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น IAL1			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง IAL2			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับสูง IAL3		
	MOPH DID	มรด.	ผ่านข้อกำหนด[๒]	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด
ตรวจสอบหลักฐานการแสดงตน (Validation)	ตรวจสอบบัตรประจำตัวประชาชนกับแหล่งข้อมูลกรมการปกครอง -เลขประจำตัว ปชช. - เลขหลังบัตร ปชช. - ชื่อ-นามสกุล - วันเดือนปีเกิด - สถานะของบัตร	ตรวจสอบหรือไม่ก็ได้	✓	- ใช้ระบบตรวจสอบ (dip chip/kiosk) -ตรวจสอบบัตรประจำตัวประชาชนกับแหล่งข้อมูลกรมการปกครอง -เลขประจำตัว ปชช. - เลขหลังบัตร ปชช. - ชื่อ-นามสกุล - วันเดือนปีเกิด - สถานะของบัตร	-ตรวจสอบโดยเจ้าพนักงาน หรือเทคโนโลยีที่เหมาะสม เช่น Dip chip หรือเทียบเท่า -ตรวจสอบข้อมูลกับแหล่งข้อมูลที่น่าเชื่อถือ (Authoritative Source หรือ AS)	✓	- ใช้ระบบตรวจสอบ (dip chip/kiosk) -ตรวจสอบบัตรประจำตัวประชาชนกับแหล่งข้อมูลของกรมการปกครอง	-ตรวจสอบโดยเจ้าพนักงานหรือเทคโนโลยีที่เหมาะสม เช่น Dip chip หรือเทียบเท่า -ตรวจสอบข้อมูลกับแหล่งข้อมูลที่น่าเชื่อถือ	✓
ตรวจสอบตัวบุคคล (Verification)	ไม่ตรวจสอบตัวบุคคล	ไม่ตรวจสอบตัวบุคคล	✓	ตรวจสอบตัวบุคคลโดยผู้ประกอบวิชาชีพ โดย เจ้าหน้าที่ถ่ายภาพใบหน้าของผู้รับบริการ และบันทึกเข้าระบบเพื่อให้ระบบประมวลผลการเปรียบเทียบใบหน้า (Facial Recognition)	ตรวจสอบตัวบุคคลโดยการเปรียบเทียบทางกายภาพ หรือเทคโนโลยีชีวมิติ	✓	ตรวจสอบตัวบุคคลโดยผู้ประกอบวิชาชีพ โดย เจ้าหน้าที่ถ่ายภาพใบหน้าของผู้รับบริการ และบันทึกเข้าระบบเพื่อให้ระบบประมวลผลการเปรียบเทียบใบหน้า (Facial Recognition)	ตรวจสอบตัวบุคคลโดยการเปรียบเทียบด้วยเทคโนโลยีชีวมิติ	✓

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) ที่ให้บริการ	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น IAL1			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง IAL2			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับสูง IAL3		
	MOPH DID	มรด.	ผ่านข้อกำหนด[๒]	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด
รวบรวมข้อมูลชีวมิติ (Biometric Collection)	ไม่มีการรวบรวมข้อมูลชีวมิติ	ไม่มีข้อกำหนด	✓	เจ้าหน้าที่ถ่ายภาพใบหน้าของผู้รับบริการและบันทึกเข้าระบบเพื่อการประมวลผลการเปรียบเทียบใบหน้า (Facial Recognition)	รวบรวมข้อมูลชีวมิติ หรือไม่ก็ได้	✓	เจ้าหน้าที่ถ่ายภาพใบหน้าของผู้รับบริการและบันทึกเข้าระบบเพื่อประมวลผลการเปรียบเทียบใบหน้า (Facial Recognition)	รวบรวมข้อมูลชีวมิติ	✓
ตรวจสอบช่องทางการติดต่อ (Address Confirmation)	หมายเลขโทรศัพท์เคลื่อนที่			หมายเลขโทรศัพท์เคลื่อนที่			หมายเลขโทรศัพท์เคลื่อนที่		

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

ตารางที่ ๓ การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ของบริการพิสูจน์และยืนยันตัวตน (MOPH DID) ของกระทรวงสาธารณสุข ตามบทบาทผู้พิสูจน์และยืนยันตัวตน (Identity Provider : IdP)

การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ที่ให้บริการ	**ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น AAL1**			**ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2**			**ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2 (สำหรับแพทย์)**		
	MOPH DID	**มรด.**	**ผ่านข้อกำหนด**	**MOPH DID**	**มรด.**	**ผ่านข้อกำหนด**	**MOPH DID**	**มรด.**	**ผ่านข้อกำหนด**
ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้ (Permitted Authenticator Types)	๑. Single - Factor Memorized Secret (username & password) ๒.PIN หรือ OTP	ชนิดของสิ่งยืนยันตัวตนหนึ่งปัจจัยหรือมากกว่า	✓	Multi-factor ๑.Memorized Secret ๒.PIN หรือ OTP ๓ Biometric (ถ้ามี)	มีชนิดของสิ่งยืนยันตัวตนสองปัจจัย หรือมากกว่า (Multi-factor) หรือสิ่งยืนยันตัวตนแบบเข้ารหัสในระดับ AAL3	✓	Multi-factor ๑ PIN แบบ Onetime ผ่าน app หมอพร้อม (มีอายุ 2 ชั่วโมง) หรือเจ้าของข้อมูลให้ความยินยอมด้วยตัวเอง ๒ ตรวจสอบ Biometric	มีชนิดของสิ่งยืนยันตัวตนสองปัจจัยหรือมากกว่า (Multi-factor) หรือสิ่งยืนยันตัวตนแบบเข้ารหัสในระดับ AAL3	✓
การยืนยันตัวตนซ้ำ (Reauthentication)	ทุก ๓๐ วัน	ทุก ๓๐ วัน	✓	ทุก ๑๒ ชั่วโมง หรือ ๓๐ นาที กรณีไม่มีกิจกรรมใดๆ เกิดขึ้น	ทุก ๑๒ ชั่วโมง หรือ ๓๐ นาที กรณีไม่มีกิจกรรมใดๆ เกิดขึ้น	✓	ทุก ๑๒ ชั่วโมง หรือ ๑๕ นาที กรณีไม่มีกิจกรรมใดๆ เกิดขึ้น	ทุก ๑๒ ชั่วโมง หรือ ๑๕ นาที กรณีไม่มีกิจกรรมใดๆ เกิดขึ้น	✓

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ที่ให้บริการ	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น AAL1			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2 (สำหรับแพทย์)		
	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด
ป้องกันการโจมตี Man-in-the-Middle Attack (MitM Resistance)	ข้อกำหนด การสื่อสารระหว่างผู้ใช้บริการและ IdP ผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดย คนกลาง (man-in-the-middle resistance) การ login ด้วย User และ password ส่งผ่านช่องทางเข้ารหัส ด้วย https	จำเป็นต้องมีมาตรการป้องกัน	✓	ข้อกำหนด การสื่อสารระหว่างผู้ใช้บริการและ IdP ผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดย คนกลาง (man-in-the-middle resistance) การ login ด้วย User และ password ส่งผ่านช่องทางเข้ารหัส ด้วย https	จำเป็นต้องมีมาตรการป้องกัน	✓	ข้อกำหนด การสื่อสารระหว่างผู้ใช้บริการและ IdP ผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดย คนกลาง (man-in-the-middle resistance) การ login ด้วย User และ password ส่งผ่านช่องทางเข้ารหัส ด้วย https	จำเป็นต้องมีมาตรการป้องกัน	✓

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ที่ให้บริการ	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับต้น AAL1			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2			ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับปานกลาง AAL2 (สำหรับแพทย์)		
	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด	MOPH DID	มรด.	ผ่านข้อกำหนด
ป้องกันการโจมตี Replay Attack (Replay Resistance)	ข้อกำหนด สิ่งที่ใช้ยืนยันตัวตนอย่างน้อย ๑ สิ่งต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance) มีการใช้ SSL หรือ TLS (https)	ไม่จำเป็น	✓	SMS OTP (out-of-band device) รหัสลับแบบสุ่ม ๖ หลัก จำกัดระยะเวลา ๑๕ นาที หรือ PIN แบบ Onetime ผ่าน app หมอพร้อม (มีอายุ ๒ ชั่วโมง) และใช้ SSL หรือ TLS (https)	จำเป็น	✓	SMS OTP (out-of-band device) รหัสลับแบบสุ่ม ๖ หลัก จำกัดระยะเวลา ๑๕ นาที หรือ PIN แบบ Onetime ผ่าน app หมอพร้อม (มีอายุ ๒ ชั่วโมง) และใช้ SSL หรือ TLS (https)	จำเป็น	✓
ป้องกัน IdP ปลอม (IdP Impersonation Resistance)	มีการใช้ SSL หรือ TLS (https) และมีการตรวจสอบใบรับรอง (CA) สำหรับการสื่อสารระหว่าง IdP และ RP	ไม่ตรวจสอบตัวบุคคล	✓	มีการใช้ SSL หรือ TLS (https) และมีการตรวจสอบใบรับรอง (CA) สำหรับการสื่อสารระหว่าง IdP และ RP	ไม่จำเป็น	✓	มีการใช้ SSL หรือ TLS (https) และมีการตรวจสอบใบรับรอง (CA) สำหรับการสื่อสารระหว่าง IdP และ RP	จำเป็น	✓

หมายเหตุ ๑ ผู้ประกอบวิชาชีพได้รับการฝึกอบรมวิธีตรวจสอบบัตรประจำตัวประชาชน และตรวจสอบรายการบุคคลกับแหล่งข้อมูลของกรมการปกครองฯ

๒ ผ่านข้อกำหนด คือ สอดคล้องกับข้อกำหนดตามมาตรฐานรัฐบาลดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (มรด. ๑-๒:๒๕๖๔)

๕. เพื่อประโยชน์ต่อการจัดทำเอกสารที่เกี่ยวข้องต่อไป และการปฏิบัติตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ซึ่งตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลฯ ได้กำหนดให้ผู้พิสูจน์และยืนยันตัวตน ดำเนินการตามรายละเอียดในหมวด ๒ ข้อ ๔ และให้ผู้ให้บริการภาครัฐดำเนินการตามหมวด ๒ ข้อ ๕ อาจพิจารณารายละเอียดเพิ่มเติมดังนี้

หมวด ๒ ข้อ ๔ ให้ผู้พิสูจน์และยืนยันตัวตน ดำเนินการดังต่อไปนี้

๑) กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัล และจัดสรรบุคลากร ระบบเทคโนโลยีที่จำเป็น ให้สอดคล้องกับระดับความน่าเชื่อถือ

๒) กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสาร ทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

๓) กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐให้ดำเนินการตามข้อกำหนดการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามมาตรฐานและหลักเกณฑ์นี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๔) จัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

๕) จัดให้มีการแสดงตนและรวบรวมข้อมูล เพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการเพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

๖) ตรวจสอบหลักฐานแสดงตนของผู้สมัครใช้บริการ เพื่อตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน รวมทั้ง ตรวจสอบข้อมูลในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

๗) ตรวจสอบตัวบุคคลของผู้สมัครใช้บริการที่แสดงหลักฐานแสดงตน ว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจตรวจสอบช่องทางติดต่อว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อ และสามารถติดต่อหรือส่งข้อมูลไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง

๘) เก็บรักษาข้อมูลและหลักฐานแสดงตน รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยระยะเวลาการเก็บรักษาและการบันทึกดังกล่าวให้เป็นไปตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

๙) ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๐)ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

หมวด ๒ ข้อ ๕ ให้ผู้ให้บริการภาครัฐดำเนินการ ดังต่อไปนี้

๑) กำหนดความต้องการและระบบของหน่วยงานที่ต้องการใช้ดิจิทัลไอดี

๒) ประเมินความเสี่ยงเพื่อพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์หรือยืนยันตัวตนผิดพลาด

๓) นำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือทั้งระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๔) เลือกรูปแบบ และวิธีการลงทะเบียน การพิสูจน์ตัวตนและยืนยันตัวตนทางดิจิทัล รวมถึงกำหนดเงื่อนไขให้สอดคล้องตามข้อกำหนดในแต่ละระดับความน่าเชื่อถือตามกลุ่มให้บริการภาครัฐ และแจ้งให้ทราบล่วงหน้า