TMI Newsletter
จดหมายข่าวสมาคมเวชสารสนเทศไทย
ฉบับที่ 4 ปีที่ 3 กรกฎาคม-สิงหาคม 2556

นพ.อาทิตย์ อังกานนท์
คณะกรรมการกลางสมาคมเวชสารสนเทศไทย

บทบาทของ CIO ในสถานพยาบาล

การประชุมวิชาการกลางปี สมาคมเวชสารสนเทศไทย สำหรับผู้บริหาร วันที่ 5 กรกฎาคม 2556

ความหมายของ CIO หรือ Chief Information Officer คือ ผู้ที่เป็นผู้รับผิดชอบโดยตรงกับการบริหารจัดการสารสนเทศ (ข้อมูล) ภายในองค์กร อาจแปลเป็นไทยได้ว่า ผู้บริหารสารสนเทศ CIO มีหน้าที่รับผิดชอบโดยตรงกับการมีสารสนเทศพร้อมใช้ในองค์กร ไม่ว่าจะเป็นสารสนเทศเพื่อการปฏิบัติงาน (information for operation) หรือสารสนเทศเพื่อการบริหาร (management information system)

CIO มีหน้าที่ดูแลและกำหนดทิศทางพัฒนาระบบสารสนเทศภายในองค์กร การพัฒนาระบบสารสนเทศใดๆ ต้องใช้ทรัพยากรไม่ว่าจะเป็นกำลังคน กำลังเงิน หรือเวลา เทคโนโลยีใหม่มักมีราคาแพง และบุคลากรที่มีความชำนาญด้านสารสนเทศมักหาได้ยากหรือมีค่าตัวสูง ดังนั้น การเลือกพัฒนาระบบสารสนเทศให้ถูกทิศทางและสอดคล้องกับเป้าหมายทางยุทธศาสตร์ขององค์กร จะทำให้องค์กรไม่เสียทรัพยากรดังกล่าวไปอย่างเปล่าประโยชน์ และระบบสารสนเทศที่พัฒนาขึ้น ยังจะช่วยเกื้อหนุนให้องค์กรสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพมากขึ้นอีกด้วย โดยทั่วไป CIO จะเป็นหนึ่งในทีมบริหารองค์กร เพื่อให้สามารถสื่อสารกับทีมนำขององค์กรได้โดยตรง และทำให้เข้าใจทิศทางยุทธศาสตร์ขององค์กรได้อย่างถูกต้องและรวดเร็ว

คำถามข้อหนึ่งที่ผู้บริหารองค์กร โดยเฉพาะผู้บริหารสารสนเทศมักจะถูกตั้งคำถามเสมอๆ ก็คือ องค์กรควรจะลงทุนเท่าไรในระบบสารสนเทศ คำถามนี้ตอบค่อนข้างยากเพราะบริบทของแต่ละองค์กรแตกต่างกันมาก Gartner ได้เคยสำรวจงบลงทุนและดำเนินการด้าน IT ในองค์กรต่างๆ ได้ข้อสรุปว่าควรจะอยู่ที่ประมาณ 1-3% ของรายได้ขององค์กรนั้น แต่หากเป็นองค์กรด้าน Healthcare ตัวเลขนี้อาจสูงถึง 3-5% ได้ สำหรับจำนวนกำลังคนด้าน IT โดยทั่วไปจะอยู่ที่ 0.5-2% ของจำนวนคนในองค์กร สำหรับโรงพยาบาลในประเทศไทย จากการสำรวจโดยสมาคมเวชสารสนเทศไทย จะอยู่ที่ประมาณ 1% ของจำนวนคนในโรงพยาบาล (personal communication) ดังนั้น CIO จึงควรดูแลการใช้ทรัพยากรเพื่อการพัฒนาและดำเนินงานระบบสารสนเทศภายในองค์กรให้เหมาะสม

คำถามที่ได้รับการถามกันบ่อยเกี่ยวกับการพัฒนาระบบสารสนเทศก็คือ ควรจะพัฒนาขึ้นเอง (in-house development) หรือจ้างผู้อื่นมาทำให้หรือซื้อระบบงานสำเร็จรูปมา (outsource) CIO ควรมีส่วนในการตัดสินใจเรื่องนี้ โดยพิจารณาว่า ระบบสารสนเทศที่จะพัฒนานั้น เป็น

อ่านต่อหน้า 4 »

Healthcare Information Security Professional

นพ.สุธี ทุวิรัตน์ (CISA)
คณะกรรมการสมาคมเวชสารสนเทศไทย

การรักษาความปลอดภัยของระบบสารสนเทศทางการแพทย์เป็นเรื่องที่มีความสำคัญเป็นอย่างมาก เนื่องจากหากเกิดความผิดพลาดจะสามารถมีผลกระทบต่อผู้รับบริการได้เป็นวงกว้างและอาจจะรุนแรงถึงขั้นเสียชีวิต ดังนั้นจึงจำเป็นที่จะต้องมีบุคลากรที่มีความรู้และความเชี่ยวชาญทางด้านนี้โดยเฉพาะมารับผิดชอบ ซึ่งในปัจจุบันยังไม่มีหลักสูตรสำหรับการผลิตบุคลากรด้านการรักษาความปลอดภัยของระบบสารสนเทศทางการแพทย์โดยเฉพาะ

สำหรับข้อกำหนดพื้นฐานความรู้และทักษะที่จำเป็นของผู้ที่จะเป็นผู้ปฏิบัติงานทางด้านการรักษาความปลอดภัยของระบบสารสนเทศ (Information Security Professional) ที่ได้รับการยอมรับอย่างแพร่หลาย ได้แก่ IT Security Essential Body of Knowledge (EBK) ซึ่งกำหนดโดย Department of Homeland Security ของประเทศสหรัฐอเมริกา โดยมาตรฐานดังกล่าวกำหนดองค์ความรู้และทักษะที่จำเป็นต้องมี (Competency) 14 หัวข้อ ได้แก่

1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training & Awareness
6. IT System Operation & Maintenance
7. Network and Telecommunication Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and Standard Compliance
12. Security Risk Management
13. Strategic Security Management
14. System and Application Security

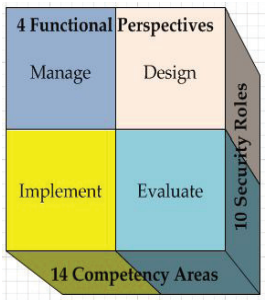
ซึ่งในแต่ละหัวข้อมีการแบ่งย่อยตามลักษณะงานได้เป็น 4 functional perspective

1. Manage ได้แก่ทักษะความรู้ที่จำเป็นสำหรับผู้บริหาร
2. Design ได้แก่ทักษะความรู้ที่จำเป็นสำหรับการออกแบบระบบ
3. Implement ได้แก่ทักษะความรู้ที่จำเป็นสำหรับการติดตั้งระบบ
4. Evaluate ได้แก่ทักษะความรู้ที่จำเป็นสำหรับผู้ตรวจสอบ (Audit)

เมื่อรวมกันแล้วจะมี Competency ที่จำเป็นทั้งสิ้น 56 Unit ซึ่งหมายความว่าในทุกองค์กรจำเป็นอย่างยิ่งที่จะต้องมีบุคลากรที่ความรู้และทักษะที่จำเป็นเหล่านี้ทั้ง 56 Unit โดยใน IT Security EBK นี้ได้มีการแบ่งกำหนดตำแหน่งงานหรือบทบาทของบุคลากรทางด้าน IT Security ออกเป็น 10 ตำแหน่ง ได้แก่

1. Chief Information Officer
2. Digital Forensic Professional
3. Information Security Officer
4. IT Security Compliance Officer
5. IT Security Engineer
6. IT Security Professional
7. IT System Operations and Maintenance Professional
8. Physical Security Professional
9. Privacy Professional
10. Procurement Professional

สำหรับการกำหนดว่าตำแหน่งงานใดจำเป็นต้องมีทักษะความรู้ด้านใด (Competency) สามารถดูได้ดังรูป



IT Security Competency Areas	IT Security Roles: Executive						Functional								Corollary					
	Chief Information Officer		Information Security Officer		Information Security Compliance Officer		Digital Forensics Professional		IT Systems Operations & Maintenance Professional		IT Security Professional		IT Security Engineer		Physical Security Professional		Privacy Professional		Procurement Professional	
1. Data Security	M		M	D							M	D		D				D		
				E		E			I	E		E		E				E		
2. Digital Forensics			M	D			M	D												
						E	I	E	I											
3. Enterprise Continuity	M		M							D						D				
				E		E			I			E			I					
4. Incident Management	M		M	D						D		D					M	D		
				E		E	I		I	E		E			I		I	E		
5. IT Security Training & Awareness	M		M									D						D		
				E		E					I	E						E		
6. IT System Operations & Maintenance								D	M	D				D						
						E	I	E	I	E			I							
7. Network and Telecommunication Security								D	M	D				D						
						E	I		I	E			I							
8. Personnel Security	M		M									D						D		
						E						E				E	I			
9. Physical and Environmental Security	M		M									D			M	D				
				E		E						E			I	E				
10. Procurement	M	D	M	D															M	D
				E		E		E		E						E			I	E
11. Regulatory and Standard Compliance	M		M	D		D											M	D		
		E		E	I	E					I						I	E		
12. Security Risk Management	M		M	D								D					M	D		
		E		E	I	E	I		I		I	E	I		I		I	E		
13. Strategic Security Management	M	D	M	D																
		E	I	E		E														
14. System and Application Security	M		M											D						
				E		E			I				I	E						

นพ.นวนรรน ธีระอัมพรพันธุ์
คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี
มหาวิทยาลัยมหิดล
nawanan.the@mahidol.ac.th

Good Communication Pays Off
การสื่อสารที่ดี คุ้มเสียยิ่งกว่าคุ้ม

จดหมายข่าวฉบับที่แล้วผมได้นำเสนอข้อคิดที่ว่า "สื่อสาร! สื่อสาร! สื่อสาร!" หรือ "Communicate! Communicate! Communicate!" และได้ชี้ให้เห็นถึงความสำคัญของการสื่อสาร ต่องานด้านเวชสารสนเทศ เพราะเป็นการลดช่องว่างที่อาจเกิดขึ้นจากการได้รับข้อมูลข่าวสารไม่เท่ากัน ความรู้สึกกลัวหรือต่อต้านที่อาจเกิดขึ้นได้เพราะความไม่รู้ หรือเพราะความเข้าใจผิด และลดโอกาสที่จะเกิดการทำงานผิดพลาดเพราะการสื่อสารที่มีปัญหาลงได้ และทิ้งท้ายเอาไว้ว่าเราจะมาดูกันในฉบับนี้ว่า ควรจะสื่อสารอย่างไรจึงจะเหมาะสม และลดโอกาสเกิดปัญหาในการทำงานด้านเวชสารสนเทศ

หัวใจสำคัญของการสื่อสารที่ดี มีประสิทธิผล คือ การให้ความสำคัญกับ What, When, Where, How, Who และ To Whom ของการสื่อสารไปด้วยกันครับ การสื่อสารที่ดี ผู้ที่ทำหน้าที่สื่อสารจะต้องมีโฟกัสที่ชัดเจนว่าต้องการจะสื่อประเด็นหรือเนื้อหาอะไร (What) เพราะหากไม่มีความชัดเจนก็จะทำให้เนื้อหาที่จะสื่อสาร มีความเยิ่นเย้อ มีหลายประเด็น หรือจับประเด็นไม่ได้ ซึ่งจะทำให้ผู้รับสารไม่สามารถเข้าใจในสิ่งที่เราต้องการจะสื่อสารได้ ในขณะเดียวกัน การให้ความสำคัญกับบริบทและรูปแบบของการสื่อสาร (ทั้ง When, Where และ How) ก็มีผลต่อประสิทธิผล (effectiveness) ของการสื่อสาร ว่าจะได้ผลเพียงใด นอกจากนี้ ผู้ส่งสาร (Who) และผู้รับสาร (To Whom) ก็มีความสำคัญ เพราะแต่ละคนมีความสนใจ ความถนัด และความชอบในเรื่องรูปแบบการสื่อสารไม่เหมือนกัน และบางครั้งการสื่อสารยังได้รับผลกระทบจากอารมณ์ ความรู้สึกนึกคิด และอคติ ที่เป็นธรรมชาติของมนุษย์ นักสื่อสารที่เก่งจึงควรตระหนักว่า การจะสื่อสารให้ผู้รับแต่ละคน ควรจะใช้ใครเป็นผู้ส่งสาร (เพราะคนเราฟังข้อความจากคนสองคนไม่เท่ากัน แม้ทั้งสองคนนั้นจะสื่อสารข้อความเดียวกันด้วยวิธีเดียวกันก็ตาม)

ผมมีคำแนะนำเล็กๆ น้อยๆ เกี่ยวกับแนวทางการสื่อสารที่เหมาะสมดังนี้ครับ

1. บางครั้งเราอาจจะนึกว่าในสถานการณ์ที่ไปได้ดี ราบรื่นอยู่แล้ว เช่น Project ที่ implement ระบบสารสนเทศ เป็นไปด้วยดี เราจึงไม่จำเป็นจะต้องสื่อสารอะไรให้ทีมงาน ผู้ใช้งาน หรือผู้มีส่วนได้เสีย (stakeholders) ทราบก็ได้ ความคิดนี้เป็นความคิดที่ผิด เพราะในสถานการณ์ที่ไปได้ดี นี่คือโอกาสในการประชาสัมพันธ์เพื่อให้คนรับทราบ สนใจติดตาม และเกิดความเชื่อมั่นกับโครงการที่กำลังจะเข้ามาเกี่ยวข้องกับพวกเขา หากเราเลือกที่จะอยู่นิ่งๆ ไม่พูดไม่จา นอกจากจะเสียโอกาสประชาสัมพันธ์ดีๆ (missed opportunities) แล้ว ยังอาจทำให้ผู้ใช้งานหรือผู้มีส่วนได้เสีย ที่ไม่ได้รับทราบข่าวคราวของโครงการ เกิดความรู้สึกกลัว วิตกกังวล และอาจพยายามต่อต้าน หรือบ่อนทำลายความสำเร็จของโครงการได้

2. ในทางกลับกัน บางครั้งในช่วงที่สถานการณ์ของโครงการกำลังประสบปัญหาอุปสรรค เราอาจมีความรู้สึกว่าควรปิดข่าว ไม่ควรแพร่งพรายให้ผู้อื่นทราบ เพราะจะทำให้เกิดความรู้สึกในแง่ลบต่อโครงการ เกิดความไม่เชื่อมั่น ซึ่งอาจส่งผลให้โครงการเกิดความล้มเหลว หรือทำให้เกิดความอับอายขายหน้าขึ้นได้ ความคิดเช่นนี้ก็เป็นความคิดที่ผิดมหันต์ครับ จริงอยู่ที่การสื่อสารแจ้งข่าวปัญหาอุปสรรคจะทำให้เกิดความไม่เชื่อมั่นหรือความวิตกกังวลต่อโครงการได้ แต่ต้องยอมรับครับว่า แม้เราจะพยายามปิดข่าวอย่างไร ในความเป็นจริง มีโอกาสที่ข่าวเกี่ยวกับปัญหาอุปสรรคของโครงการจะหลุดรอดให้คนอื่นได้ยินเสมอ และคนอื่นไม่ได้ยินอะไรจากเราเลย หรือหากเราโกหก ปฏิเสธว่าไม่มีอะไรเกิดขึ้น ผลที่จะเกิดขึ้นคือ อาจมีข่าวลือที่ไม่เป็นความจริงเกิดขึ้นหรือมีความรุนแรงเกินความเป็นจริง นอกจากนั้น เรายังเสียความเชื่อมั่นจากคนอื่นไปด้วย เพราะความพยายามที่จะปิดข่าว ความพยายามที่จะโกหก หรือควบคุมสถานการณ์ กลายเป็นการบั่นทอนความไว้วางใจและความเชื่อมั่นที่ผู้อื่นมีต่อโครงการ สุดท้ายโครงการที่ไม่มี trust ก็จะไม่ได้รับการยอมรับและความร่วมมือ และจะประสบความล้มเหลวในที่สุด ศิลปะในการสื่อสารในช่วงที่มีปัญหาอุปสรรคหรือเกิดวิกฤติขึ้นในโครงการ จึงมีความสำคัญมาก การยอมรับปัญหาและสื่อสารข้อเท็จจริงที่สำคัญและจำเป็นอย่างจริงใจ ให้ผู้เกี่ยวข้องทราบ พร้อมทั้งชี้แจงให้ทราบถึงความพยายามที่จะแก้ไขปัญหาดังกล่าว แม้จะส่งผลในแง่ลบได้บ้างในระยะสั้น แต่จะช่วยสร้างความไว้วางใจ ความเชื่อมั่น และความศรัทธาขึ้นได้ในระยะยาว ซึ่งมีความสำคัญมากต่อความสำเร็จของโครงการ นอกจากนี้ยังอาจทำให้เกิดความร่วมมือร่วมใจกันและความช่วยเหลือสนับสนุนต่างๆ เพื่อฝ่าฟันอุปสรรคดังกล่าวได้อีกด้วย ลองสังเกตดูครับเวลาบริษัทเอกชนทำอะไรผิดพลาดแล้วออกมายอมรับและขอโทษต่อสาธารณชน เรามีความรู้สึกอย่างไร เมื่อเทียบกับอีกบริษัทที่พยายามปิดข่าว ไม่เปิดเผยข้อมูล ไม่ยอมรับปัญหา และไม่แสดงท่าทีว่ามีความรับผิดชอบหรือความใส่ใจต่อปัญหาที่เกิดขึ้น

3. การสื่อสารที่ดี ควรมีการสื่อสารในทุกทิศทาง ทั้งขาขึ้น (ไปยังผู้บังคับบัญชา หัวหน้าทีม และหน่วยงานระดับสูงกว่า) และขาลง (ไปยังผู้ใต้บังคับบัญชา ลูกทีม และหน่วยงานในสังกัดที่กำกับดูแล) ซึ่งเป็นการสื่อสารในแนวดิ่ง (vertical communications) รวมทั้งการสื่อสารในแนวขวาง (horizontal communications) ไปยังเพื่อนร่วมงาน ทีมงานที่เกี่ยวข้อง และหน่วยงานในระดับเดียวกันที่ควรทราบข้อมูล

4. การสื่อสารอย่างรวดเร็ว ทันท่วงที มีความสำคัญ โดยเฉพาะในช่วงที่มีความสำคัญหรือเกิดปัญหาอุปสรรคต่างๆ ขึ้น เพราะหากปราศจากการสื่อสารที่ทันท่วงทีแล้ว ผู้เกี่ยวข้องอาจได้รับข่าวสารจากแหล่งอื่น ซึ่งอาจไม่ตรงกับข้อเท็จจริง และอาจเกิดความรู้สึกไม่เชื่อมั่นต่อตัวทีมงานได้ นอกจากนี้ สำหรับเรื่องที่มีความสำคัญ เราควรสื่อสารซ้ำเป็นระยะๆ อย่างเหมาะสม เพราะในบางครั้ง เราอาจมีช่องว่างในการสื่อสาร เกิดการตกสำรวจ ทำให้เป้าหมายบางคนไม่ได้รับทราบการสื่อสารก็ได้ การสื่อสารซ้ำจะช่วยให้แน่ใจว่าโอกาสเกิดการสื่อสารตกหล่นมีน้อยลง ทั้งยังอาจเป็นการเตือนความจำผู้ที่ได้รับการสื่อสารไปก่อนแล้วอีกด้วย

5. หลักการที่สำคัญข้อหนึ่งของการสื่อสาร คือ ใช้หลากหลายวิธีการและช่องทางในการสื่อสาร ทั้งนี้เพราะคนแต่ละคน มีความชอบและความสามารถในการรับสารในแต่ละรูปแบบ แต่ละช่องทางแตกต่างกัน หากทำได้จึงควรสื่อสารหลายช่องทาง ซึ่งรวมถึงทางวาจา ทางเอกสาร (เช่น เอกสารทางการ สื่อสิ่งพิมพ์ จดหมายข่าว โปสเตอร์) ทางสื่ออิเล็กทรอนิกส์ (เช่น อินทราเน็ต กระดานข่าว อีเมล SMS หรือ social media) หรือสื่อที่เข้าถึงคนในวงกว้าง (เช่น ระบบเสียงตามสายภายในองค์กร สื่อโทรทัศน์หรือวิทยุ เป็นต้น) โดยปรับแต่งเนื้อหาและรูปแบบของการสื่อสารให้เหมาะสมกับเนื้อหาและผู้รับสาร (tailored communications) ด้วย

ผมเคยแต่งกลอนง่ายๆ เป็นภาษาอังกฤษ เพื่อย้ำถึงความสำคัญของการสื่อสารอย่างเหมาะสม จึงขอทิ้งท้ายไว้ด้วยข้อคิดที่ว่า "การสื่อสารที่ดี คุ้มเสียยิ่งกว่าคุ้ม" หรือ "Good Communication Pays Off" และกลอนต่อไปนี้ครับ

"Communicate, in good times and bad,
Communicate, will prevent people from being mad,
Communicate, even if you do well,
Since it's a brief period that you can sell.

Communicate up, communicate down,
Communicate sideways, to everyone you found,
Communicate early, communicate repeatedly,
Use multiple channels, coz everyone varies.

Most important of all, be sincere,
Only this will let people revere,
People can smell lies and cover-ups from a distance,
Without truth in what you say, be successful you can't."

core competency ของสถานพยาบาลหรือไม่ และเป็นระบบสารสนเทศที่ support ระบบงานที่ได้มีการทำงานกันมายาวนานจนเกิดความลงตัวในกระบวนการการทำงานแล้วหรือยัง (process maturity) ระบบงานที่ควรจะ outsource มากที่สุดคือระบบงานที่ไม่ใช่ core competency และมี process maturity ดีแล้ว ส่วนระบบงานที่เป็น core competency ขององค์กร หากจะ outsource ควรเป็นระบบงานที่มี process maturity ดีเช่นเดียวกัน เนื่องจากระบบงานที่ยังไม่มี process maturity มักจะมีการปรับปรุงกระบวนการทำงานอยู่เสมอ หาก outsource จะทำให้โครงการนั้นมีความยุ่งยากในการบริหารจัดการมาก

การดูแลเรื่องความปลอดภัยด้านสารสนเทศ (Information Security) ขององค์กร เป็นอีกบทบาทสำคัญของ CIO ในสถานพยาบาล ซึ่งข้อมูลสุขภาพของผู้รับบริการเป็นข้อมูลที่อ่อนไหวและมีความลับสูง การรักษาความปลอดภัยของข้อมูลเป็นเรื่องที่ยิ่งสำคัญมากขึ้น CIO ควรศึกษาให้เข้าใจถึงองค์ประกอบทั้งหมดของความปลอดภัยสารสนเทศ เข้าใจถึงความเสี่ยงด้านสารสนเทศ กำกับดูแล หรือสร้างนโยบายความปลอดภัยสารสนเทศขององค์กร และรณรงค์ประชาสัมพันธ์ให้ประชาคมในองค์กรตระหนักถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศดังกล่าวด้วย

นอกจากนโยบายความปลอดภัยสารสนเทศ ซึ่งเป็นข้อกำหนดที่สร้างขึ้นภายในองค์กร CIO ควรมีความรู้ถึงกฎหมายและประกาศต่างๆ เกี่ยวกับเทคโนโลยีสารสนเทศของราชการ เพื่อประโยชน์และความปลอดภัยในการทำงานของตนเองและองค์กร ได้แก่ พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น เพื่อให้เข้าใจผลกระทบและความผูกพันของกฎหมายและประกาศเหล่านี้ต่อองค์กรด้วย

CIO มีหน้าที่ในการดูแลกำกับการพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศของบุคลากรในองค์กร ไม่ว่าจะเป็นบุคลากรสายผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติงานด้านอื่นๆ CIO ควรร่วมมือกับผู้ที่ดูแลด้านทรัพยากรบุคคล เป็นเจ้าภาพในการประเมินและพัฒนาสมรรถนะเหล่านี้ โดยกำหนดเกณฑ์สมรรถนะขั้นต่ำของบุคลากรที่ปฏิบัติงานในตำแหน่งต่างๆ วัดและประเมินผล ตลอดจนทำแผนพัฒนาสมรรถนะเพื่อให้บุคลากรขององค์กรมีสมรรถนะด้านเทคโนโลยีสารสนเทศที่ดีและพร้อมเป็นกำลังสำคัญในการขับเคลื่อนองค์กรไปสู่จุดมุ่งหมายได้

จะเห็นว่า CIO ต้องทำงานเกี่ยวข้องกับบุคลากรทุกระดับในองค์กร ตั้งแต่ผู้บริหารสูงสุด ผู้ปฏิบัติงานด้าน IT ไปจนถึงผู้ใช้งานระบบซึ่งเป็นผู้ปฏิบัติงานระดับปฏิบัติการ และมีหน้าที่ต้องติดต่อกับผู้รับบริการโดยตรงขององค์กร ดังนั้น CIO จะต้องมีความสามารถในการสื่อสารด้วย “ภาษา” ที่เหมาะสมให้ผู้ที่ติดต่อด้วยเข้าใจได้ง่าย เพราะการสื่อสารให้เข้าใจตรงกันเป็นหัวใจสำคัญของการขับเคลื่อน technology adoption ในองค์กรให้สำเร็จ CIO ที่จะประสบความสำเร็จจะต้องประเมินสถานการณ์และบุคคลที่ติดต่อเกี่ยวข้องด้วย และปฏิบัติให้เหมาะสม ขอแนะนำให้ใช้ธรรมะของ “สัตบุรุษ” หรือ “สัปปุริสธรรม 7” ซึ่งได้แก่ การรู้จัก “เหตุ ผล ตน ประมาณ กาล บริษัท บุคคล” ซึ่งหาก CIO ปฏิบัติได้ ก็จะสามารถนำพาองค์กรให้สามารถใช้ประโยชน์จากสารสนเทศและเทคโนโลยีได้เต็มที่

สมาคมเวชสารสนเทศไทย : http://www.tmi.or.th/

จดหมายข่าว : เพื่อเผยแพร่ข่าวสาร เรื่องน่ารู้ และกิจกรรมต่างๆ ของสมาคมเวชสารสนเทศไทย แก่สมาชิกสมาคม และผู้สนใจทั่วไป

ที่ปรึกษา : นพ.ชุษณะ มะกรสาร

บรรณาธิการ : ทญ.ศิริวรรณ สืบนุการณ์

กองบรรณาธิการ : นพ.บุญชัย กิจสนาโยธิน, นพ.ถาวร สกุลพานิช, นพ.วรรษา เปาอินทร์, นพ.ยลศิลป์ สุชนวนิช, นพ.บดินทร์ ทรัพย์สมบูรณ์, นพ.พินิจ ฟ้าผลอำนวย, ภก.อนุชัย ธีระเรืองไชยศรี, นพ.นวนรรน ธีระอัมพรพันธุ์, ดร.มะลิวัลย์ ยืนยงสุวรรณ, คุณนุศรา สมกลิ่น

จัดทำโดย : สมาคมเวชสารสนเทศไทย สำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข
ถ.ติวานนท์ อ.เมือง จ.นนทบุรี 11000 โทรศัพท์ 0-2590-1492 โทรสาร 0-2965-9816 อีเมล official@tmi.or.th

พิมพ์ที่ : บริษัท สามเจริญพาณิชย์ โทรศัพท์ 0-2885-4932 โทรสาร 0-2435-2794