IT3070
Information Assurance and Security
3rd Year, 2nd Semester

Risk Management Assignment

Registration Number	Student Name
IT21032806	Jayasinghe K.A.K.N
IT21033032	Nishshanka N.A.P.K.R

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

02.10.2023

Table of Contents

1. Introduction

This assignment includes a comprehensive investigation of the information asset risk assessment for **MediWay**, a private hospital. We have determined five unique danger scenarios that necessitate our attention following a thorough assessment of the hospital's operations and infrastructure.

1. **DDOS Attack**
2. **Financial Data Breach**
3. **SQL Injection Attack**
4. **Transfer of a patient's medical records with those of another patient**
5. **Natural Disasters**

The main goal of this work is to identify these potential risk scenarios and to offer thorough mitigation measures. As we complete the OCTAVE Allegro 10 worksheets, we will also examine the rationale behind the likelihood and severity numbers allocated to each risk. We hope to strengthen MediWay's information security posture, improve its capacity to safeguard sensitive patient data, and ensure operational continuity by starting this comprehensive risk management.

2.1 DDOS Attack

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Patient details and Laboratory details Record Servers		
	Area of Concern	DDOS Attack		
	(1) Actor *Who would exploit the area of concern or threat?*	Invader		
	(2) Means *How would the actor do it? What would they do?*	The invader will make many requests to the targeted web resource, ignore the site's capacity to handle multiple demands, and obstruct its normal operation.		
	(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud)		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ☑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	System failure due to inaccessibility of patient information and laboratory information records		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Due to the hospital's inability to secure patient information and lab record information, reputation and customer confidence suffer. Patients won't schedule doctor visits or go to the lab. The financial revenue will thereafter steadily decline.	Reputation & Customer Confidence	8	6
	Financial	9	6.75
The hospital's productivity will suffer as a result of the additional work required for damage investigation and harm prevention.	Productivity	5	3.75
	Safety & Health	0	0

	Patients will not receive lab results on time if they do not receive appointment days and times. Patients might take legal actions for these matters	Fines & Legal Penalties	4	3
		User Defined Impact Area	0	0
			Relative Risk Score	**19.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Investing in a secure IT network	The hospital can invest in a more bandwidth-efficient secure IT network. It will provide protection against DDOS attacks.
Defense using DDS	A Dos Defense System (DDS) can stop connection-based DOS attacks as well as those with genuine content but malicious intent. A DDS can also defend against rate-based and protocol assaults.
Set Firewall to Active	A straightforward rule may be applied to the firewall to block any incoming traffic from the attackers, regardless of the protocols, ports, or IP addresses from which it originated.
Host EHR (Electronic Health Record) system in hospital internal network	If the network is hosted on a cloud-based server or another external network, the attackers will launch a DDOS attack against it.

2.1.1 Justification of probability and severity values

Attribute	Value	Justification
(6) Probability	75%	The Probability is high. The medical sections are unable to get urgent lab findings and cannot access the patient's appointment information. cannot timely deliver patient reports. Due to the laboratory server being down, the patient's procedures and inpatient treatments are also delayed. Hospital staff, patients, and physicians are all at great danger from DDOS attacks. As a result, a Probability value of 75% is provided.
Reputation & Customer Confidence	8	The hospital's reputation will suffer. because the hospital is unable to access patient information and reports. Patients are unable to obtain their medical records, and customer confidence has been damaged. Patients can become less confident in receiving medical reports from hospitals. As a result, a high value is placed on reputation and client confidence. (8/10)
Financial	9	a huge financial loss. Patients won't show up to pick up reports and schedule appointments. Inability to locate appointment information may cause doctors to skip the hospital. The hospital's financial earnings will thereafter gradually decline. To prevent DDOS assaults in the future, you must follow the computer engineers' suggestions and enforce security measures. A DDOS assault puts the hospital's finances at significant danger. Consequently, a high value is provided. (9/10)
Productivity	5	Hospital employees will be less productive since they won't be able to obtain patient information and lab report information, and because internet connectivity would be slower. As a result, an average value is provided. (5/10)
Safety & Health	0	Health and safety are unaffected. As a result, no value is provided. (0/10)
Fines & Legal Penalties	4	The hospital must investigate the attackers and pursue legal action against them. Patients have occasionally been known to file lawsuits when their lab results are delayed. Consequently, a medium value is provided. (4/10)
User Defined Impact Area	0	User defined impact areas don't exist. As a result, no value is provided. (0/10)

2. Allegro – Worksheets

2.2 Financial Data Breach

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Financial Management System		
	Area of Concern	Financial Data Breach		
	(1) Actor *Who would exploit the area of concern or threat?*	Internal Staff Member		
	(2) Means *How would the actor do it? What would they do?*	An internal staff member, regardless of their awareness of the hospital or country's regulations, could potentially disclose financial data to external parties, a situation often described as the inadvertent sharing of insider data with a third party.		
	(3) Motive *What is the actor's reason for doing it?*	Intentional (Fraud) or accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure**	❑ **Destruction**	
		❑ **Modification**	❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	The financial system should exclusively be accessible to authorized stakeholders within the hospital, and sharing with other responsible parties should only occur when compelled by government regulations. Any exposure of financial data to a third party would result in financial losses for the hospital.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	☑ **Medium** **50%**	❑ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
The hospital's reputation and patient confidence deteriorate.	Reputation & Customer Confidence	8	4
Financial issues will arise in hospitals when the financial management is flawed.	Financial	9	4.5

	The hospital's productivity may suffer because of the additional work required for damage investigation and harm prevention. can use the footage from CCTV cameras to identify anyone who entered the area and used the system.	Productivity	4	2
		Safety & Health	0	0
	Legal measures to impose fines and legal penalties for the hospital may be enforced by clients, physicians, hospital staff, shareholders, or someone else.	Fines & Legal Penalties	3	1.5
		User Defined Impact Area	0	0
			Relative Risk Score	**12**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Utilize a backup system	Use an external backup machine or device to regularly backup and keep the financial information about hospitals. The backup data can be utilized to restore lost data if the primary database data is destroyed.
Use a Fingerprint Machine	Installing a fingerprint reader at the room's entry will allow authorized individuals to enter the database server rooms.
Conducting awareness programs	After bringing on new employees, put together a proper orientation program for them, and keep the entire team informed of any dangers that might have an impact on the hospital's systems.
Legal Actions	After determining who committed the criminal or unintentional act, file a lawsuit against that employee. Funds should be recovered for fraud victims, and the employee should be fired from the hospital. In the wake of those legal activities, take careful to inform other staff members.

2.2.1 Justification of probability and Severity values

Attribute	Value	Justification
(6) Probability	50%	Medium danger probability. Access to the financial system is difficult. To enter the system, it is necessary to circumvent any security changes. However, if the system security is breached, the financial data of the hospital will be at risk. Therefore, there is a 50% possibility of a financial data leak.
Reputation & Customer Confidence	8	Patients become dissatisfied with hospital safety because of the financial difficulties facing the hospital, which harms the institution's reputation. A high impact value is therefore provided. (8/10)
Financial	9	The financial system was attacked, and as a result, there is a very high chance of damage. There are all the financial details. Consequently, a high value is provided. (9/10)
Productivity	4	The hospital's productivity may suffer because of the additional work required for damage investigation and harm prevention. The effect on productivity is temporary, though. The hospital's production will return to a stable level once the answer is found. Consequently, a medium rating (4/10) is provided.
Safety & Health	0	Health and safety are unaffected. As a result, no value is provided. (0/10)
Fines & Legal Penalties	3	Whether the hospital is at fault for what occurred or not, patients, physicians, hospital employees, shareholders, or someone else may pursue legal action. As a result, the firm must consider the legal procedure, and occasionally the hospital may end up having to pay fines. Consequently, a low value is provided. (3/10)
User Defined Impact Area	0	User defined impact areas don't exist. As a result, no value is provided. (0/10)

2.3 SQL Injection Attack

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Hospital Database		
	Area of Concern	SQL Injection Attack		
	(1) Actor *Who would exploit the area of concern or threat?*	Intruder		
	(2) Means *How would the actor do it? What would they do?*	An injection attack called SQL Injection enables the execution of malicious SQL commands. These assertions support a database server that sits behind a web application. Attackers can use SQL injection flaws to get around application security controls. They can bypass web page or web server authentication and authorization to access the complete SQL database's contents. Using SQL Injection, they can also add, modify, and delete records from the database.		
	(3) Motive *What is the actor's reason for doing it?*	Intentional		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure**	❑ **Destruction**	
		❑ **Modification**	❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the administration and other parties with permission may access hospital data and information, subject to any applicable privacy restrictions.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Sensitive information about the hospital should be well protected, and if any of it is revealed or changed, the hospital is responsible for looking into it and preserving its Reputation. The hospital can suffer significant financial losses because of this, and disgruntled patients would gradually tarnish the institution's reputation.	Reputation & Customer Confidence	8	6
	Financial	6	4.5

	To increase efficiency and safety in such a case, authorized persons should study the specific system to identify any hidden danger areas. Depending on the root of the problem, this phase may take a few hours or even days.	Productivity	4	3
		Safety & Health	0	0
	If the hospital is not legally liable for what occurred, the staff, physicians, and patients may sue for releasing their personal information, which will cost the business money for defense costs, legal services, and other expenses.	Fines & Legal Penalties	3	2.25
		User Defined Impact Area	0	0
			Relative Risk Score	**15.75**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Utilize proper privileges	It is not a good idea to connect the database with admin-level privileges using an account, unless there is some valid reason to do so. It is much better to use a limited access account, which will restrict what a hacker is able to do.
Conduct Workshops	Keep the personnel informed of potential assaults even after the initial training sessions.
Update and patch	It's critical to deploy fixes and updates as soon as practicable since hackers frequently uncover vulnerabilities in databases and programs that can be exploited using SQL injection. The cost of a patch management solution might be justified.

2.3.1 Justification of probability and severity values

Attribute	Value	Justification
(6) Probability	75%	The Probability is high because attackers might use it to obtain unwanted access to private information on patients, hospital workers, and more. One of the oldest, most common, and most harmful online application vulnerabilities is SQL Injection attacks. As a result, a value of 75% is provided.
Reputation & Customer Confidence	8	Such attacks have the potential to seriously harm the hospital's reputation. Patients who discover that a hospital is not good will be disappointed. A high value is given because the rate at which reputation and client confidence will decline is high. (8/10)
Financial	6	These kinds of circumstances are common and might result in financial losses. If patients or hospital employees file lawsuits, the hospital must deal with the legal procedure (hiring attorneys), and if they lose the lawsuit, they may also be required to pay fines. This can result in a significant financial loss. Value is therefore indicated as (6/10).
Productivity	4	Because hospital servers, databases, and queries are being disrupted, the hospital's productivity may temporarily stop. However, once the hospital manages the crisis and achieves stability, productivity can resume. Value is therefore presented as (4/10).
Safety and Health	0	Health and safety are unaffected. As a result, no rating is provided (0/10).
Fines and Legal Penalties	3	If the hospital is not legally liable for what occurred, the staff, physicians, and patients may sue for releasing their personal information, which will cost the business money for defense costs, legal services, and other expenses. Value is therefore indicated as (3/10).
User Defined Impact Area	0	User determined impact Areas don't exist. As a result, no rating is provided (0/10).

2.4 Transfer of a patient's medical record with another patient medical record

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk / Threat	Information Asset	Patient Medical Records Management System		
	Area of Concern	Transfer of a patient's medical records with those of another patient		
	(1) Actor *Who would exploit the area of concern or threat?*	Internal Staff Member		
	(2) Means *How would the actor do it? What would they do?*	Internal staff members have access to the patient medical records management system and may purposefully or unintentionally enter the medical information for one patient alongside that of another patient.		
	(3) Motive *What is the actor's reason for doing it?*	Intentional or Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only those with permission should have access to the hospital's patient records database.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
The patient is in danger because the treatments are administered incorrectly. Reputations of doctors will suffer. because the patient was given the incorrect report and medication. Patients will refuse hospital treatments and complain about the facility to others. The reputation of the hospital will suffer as a result. Patients won't go to hospitals to receive care and remain overnight. As a result, the hospital's revenue would steadily decline.	Reputation & Customer Confidence	9	6.75
	Financial	8	6

	The hospital's productivity will suffer because of the additional work required for damage investigation and harm prevention. CCTV footage can be used to identify the perpetrators and catch them. Giving the inappropriate medications and treatments will have an impact on the patients' safety and health.	Productivity	5	3.75
		Safety & Health	9	6.75
	The sufferers are going to file lawsuits. because the circumstance poses a threat to their lives and their medical treatments and medications are ineffective.	Fines & Legal Penalties	5	3.75
		User Defined Impact Area	0	0
			Relative Risk Score	**27**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Utilize a fingerprint reader	Installing a fingerprint reader at the room's entrance will allow authorized individuals finger print access to the server rooms.
Setup new security protocols and tools	Don't let users access to the entire system. The system can be partitioned to allow people access to only the necessary portions.
Legal Actions	After determining who committed the criminal or unintentional act, file a lawsuit against that employee. Funds should be recovered for fraud victims, and the staff member should be fired from the hospital. Make careful to inform other staff members of these legal actions after they are completed.
Change passwords	Encourage those with access to change passwords on a regular basis with secure ones that include letters, numbers, and other difficult-to-guess characters.

2.4.1 Justification of probability and severity values

Attribute	Value	Justification
(6) Probability	75%	The Probability is high. since all hospital staff members have access to the computer servers. They frequently access server rooms, and these things could happen.
Reputation & Customer Confidence	9	Reputable healthcare services are required. because people go there to get their ailments treated. The risk of a patient's medical records being shared with another patient is very high. The danger is really great. As a result, reputation and customer confidence are highly valued. (9/10)
Financial	8	a significant financial loss. Patients won't visit the hospital to stay, receive treatment, or request reports, which will result in a decline in financial revenues for the institution. Doctors will also decline to visit the hospital. Following the cancellation of the channelings, channeling earnings will decline. Therefore, financial is given a high value. (8/10)
Productivity	5	The hospital's productivity may suffer because of the additional work required for damage investigation and harm prevention. Finding the people who entered the server room can be done effectively by looking at the CCTV footage. As a result, an average value is provided. (5/10)
Safety and Health	9	Transferring patient medical records poses a serious threat to their lives. It will result in giving the wrong drugs to those who are sick. Consequently, a high value is provided. (9/10)
Fines and Legal Penalties	5	If the patient receives the incorrect medication or treatment, the patient may file a lawsuit. The legal system must be considered by the hospital, and occasionally fines must be paid. Consequently, a median value of 5/10 is provided.
User Defined Impact Area	0	User defined impact areas don't exist. As a result, no value is provided. (0/10)

2.5 Natural Disasters

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Resources and Properties of the Hospital		
	Area of Concern	Natural Disasters		
	(1) Actor *Who would exploit the area of concern or threat?*	Nature		
	(2) Means *How would the actor do it? What would they do?*	Natural disasters are incredibly abrupt occurrences brought on by natural causes that cause harm and material loss. Anywhere on Earth can be affected by earthquakes, storms, floods, and sicknesses, frequently without prior notice.		
	(3) Motive *What is the actor's reason for doing it?*	Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	☑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Natural catastrophes can disrupt power, close off important thoroughfares for transportation, prohibit staff members from reporting for duty, and have other effects. Hospitals must be ready for these effects and have a strategy in place to recover from them.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	☑ **Medium** **50%**	❑ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Following those sorts of disasters, if the hospital loses patients, doctors, or other personal information, that could harm the company's reputation, and on the other side, it will need to spend money to recover from those kinds of scenarios.	Reputation & Customer Confidence	5	2.5
	Financial	5	2.5

	It's possible to momentarily stop productivity. Depending on how bad the disaster is, it may close important transportation routes, impair servers, or cut off energy or other utilities. This could be detrimental to the hospital; therefore, it must be ready for any calamities that may result.	Productivity	5	2.5
		Safety & Health	4	2
		Fines & Legal Penalties	0	0
		User Defined Impact Area	0	0
			Relative Risk Score	**9.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Hospital Insurance	The hospital must have complete insurance coverage for natural disasters, which is essential in assisting it in recovering any potential financial damages.
Backup Data	The most important documents should always be backed up and kept safely.
Organize awareness sessions	This is crucial for every hospital; all staff members must be ready to protect the facility from these types of natural disasters and be aware of the potential harm they could cause. Share expertise and hold some awareness seminars with professionals.

2.5.1 Justification of probability and severity values

Attribute	Value	Justification
(6) Probability	50%	The Probability is moderate, and hospitals frequently have a backup location to recover from such types of natural catastrophes (the extent of the damage will determine this).
Reputation & Customer Confidence	5	Because those are natural disasters and the hospital has nothing to do with them, the reputation of the hospital isn't at great risk. However, there is a chance that patients or others will report or give the hospital negative feedback if they believe that the hospital is unaware of natural catastrophes. Consequently, a medium value is provided. (5/10)
Financial	5	Financial losses are common in those types of scenarios, and depending on the extent of the damage, they may be expensive to recover from. Consequently, a midway value is provided. (5/10)
Productivity	5	Depending on the extent of the disaster's damage, major transportation routes may be closed, servers may be disrupted, and lighting strikes may result in the loss of electricity or other utilities. The hospital could be harmed by this; hence it is important for the hospital to be ready for any disaster-related implications. Consequently, a midway value is provided. (5/10)
Safety and Health	4	The safety and health of the personnel will be impacted if there are any natural disasters like lightning strikes that could be damaging to the company's employees. Consequently, the value is provided. (4/10)
Fines and Legal Penalties	0	Fines and legal sanctions are absent. As a result, no value is provided. (0/10)
User Defined Impact Area	0	User defined impact areas don't exist. As a result, no value is provided. (0/10)

3. Reference

[1] techtarget.com: What is risk management and why is it important <https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important>

[2] studocu.com: < studocu.com < https://www.studocu.com/en-gb/document/kingston-university/network-security/allegro-worksheet-v1/7917216 >

[3] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process < https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf >

[4] OCTAVE® Allegro Risk Assessment Training < https://apps.dtic.mil/sti/trecms/pdf/AD1092648.pdf >

[5] Universiteit Leiden Onleading Informatica < https://theses.liacs.nl/pdf/Douramanis-Michalis-non-confidential.pdf >

[6] 10-Columns Worksheet | Perpetual System | Detailed concepts and Problems Solution | Accounting < https://www.youtube.com/watch?v=Y2Ve7oeTOIY >

[7] Quality Risk Management in Pharmaceutical Industry: A Review < https://www.researchgate.net/profile/N-Vishal-Gupta/publication/263657626_Quality_Risk_Management_in_Pharmaceutical_Industry_A_Review/links/53ff204e0cf21edafd15bbb5/Quality-Risk-Management-in-Pharmaceutical-Industry-A-Review.pdf >

[8] Dignity Health : Risk management in healthcare: What it is and why it matters < https://dhge.org/about-us/blog/risk-management-in-healthcare#:~:text=Hospital%20risk%20management,develop%20processes%20to%20reduce%20risk.>

[9] NEJM Catalyst : What Is Risk Management in Healthcare < https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0197 >

[10] National Library of Medicine : Risk Management Event Evaluation and Responsibilities <https://www.ncbi.nlm.nih.gov/books/NBK559326/ >