1 OCTAVE Allegro Worksheets v1.0

In this appendix, you will find all of the worksheets necessary for completing the OCTAVE Allegro assessment for **one information asset**.

Allegro Worksheet 1	**Risk Measurement Criteria – Reputation and Customer Confidence**		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Localized concern within the hospital; limited to internal communication. Issue is handled quietly, no media attention.	Hospital credibility is questioned by local media and patients. Negative press coverage and minor decline in public trust.	Major public scandal with national or medical community media coverage. Loss of patient trust and damage to university's reputation in healthcare
Customer Loss	Less than 2% of patients or partnerships lost due to perceived data management issues.	Between 2% and 6% of patients opt to seek services elsewhere. Medical collaborations temporarily paused.	More than 6% of patients and institutional partners withdraw. Major decline in hospital's patient inflow and referrals.
Other: {Stakeholder Trust)	Temporary concern among internal staff (e.g., doctors, IT) about data handling. Resolved via internal training or patching.	Staff morale drops; clinicians raise formal concerns. Hospital board initiates internal audit or quality review.	Medical oversight bodies and ethics committees intervene. Hospital faces external investigations or accreditation review.

Allegro Worksheet 2	**Risk Measurement Criteria – Financial**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 3% in yearly IT operating costs (e.g., due to patching, internal audit).	Yearly operating costs increase by 3% to 10% due to incident response, legal consultations, and temporary staff overtime.	Yearly operating costs increase by more than 10% due to full system restoration, long-term monitoring, and regulatory penalties.
Revenue Loss	Less than 2% of annual service billing lost due to system downtime or patient withdrawal.	Between 2% and 7% of yearly hospital revenue lost due to delays, loss of trust, and patient migration.	Greater than 7% loss in yearly hospital billing; long-term damage to public image and service volume.
One-Time Financial Loss	One-time cost of less than $25,000 (e.g., IT diagnostics, quick fixes, temporary downtime).	One-time cost of $25,000 to $100,000 for breach recovery, legal services, and PR control.	One-time cost greater than $100,000 for system rebuild, lawsuits, fines, and partner compensations.
Other: (Insurance Premium Impact)	No change in insurance coverage or premiums.	Slight increase in insurance premiums due to breach report and risk reevaluation.	Hospital's cyber liability or malpractice insurance premiums rise significantly due to breach exposure.

Allegro Worksheet 3	**Risk Measurement Criteria – Productivity**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff hours increased by less than 10% for 1 to 2 days due to login delays or temporary offline access.	Staff hours increased by 10% to 25% for 3 to 5 days due to partial system outages or manual record-keeping.	Staff hours increased by more than 25% for over 5 days due to total downtime or data restoration procedures.
Other: (Operational Delays)	Minor appointment rescheduling or patient registration delays with no impact on treatment schedules.	Access to medical records is noticeably slower; some appointments or procedures are delayed. Interdepartmental communication becomes inefficient, affecting coordination of care.	Severe workflow disruptions across key departments (e.g., emergency, diagnostics, radiology). System downtime forces widespread appointment rescheduling and significantly delays patient treatment.
Other: (Manual Workload Increase)	Brief use of paper-based records, handled efficiently by trained staff.	Staff must revert to semi-manual processes for critical functions; moderate confusion or miscommunication occurs.	Staff are overwhelmed with paperwork; increased risk of medical errors due to poor record availability.

Allegro Worksheet 4	**Risk Measurement Criteria – Safety and Health**		
Impact Area	**Low**	**Moderate**	**High**
Life	No threat to life. Clinical staff work around system delays using backups or verbal handovers.	Patient lives are potentially threatened due to delayed diagnosis or treatment, but recover after intervention.	Loss of patient life due to unavailable medical history, allergies, or delayed treatment from healthcare system outage.
Health	Minor and immediately treatable effects on patient care. For example, a slight increase in wait times or short delays in accessing diagnostic information (with no lasting impact on health outcomes).	Temporary decline in care quality, such as miscommunication about medication history or allergies. Patients may experience delays in diagnosis or treatment but recover fully with no permanent harm.	Permanent impairment (e.g., untreated complications, surgical errors) due to lack of access to time-sensitive data.
Safety	Routine safety procedures remain intact. No disruption to patient or staff safety protocols. Minor inconveniences may occur, but there is no risk of harm to individuals.	Safety of patients or staff is affected due to breakdown in coordination or missed alerts.	Critical safety violations occur (e.g., incorrect medication or procedures performed due to absent records or alerts).
Other: (Ethical/Legal Duty of Care)	Staff can still provide appropriate care, but administrative tasks (e.g., timely documentation or updates) are slightly delayed. No harm to patients occurs, and care standards are maintained.	A reportable incident occurs where patient care quality is compromised due to delays or incomplete documentation. The issue is addressed through internal review.	Legal violations of duty of care or malpractice claims filed due to severe outcome caused by data unavailability.

Allegro Worksheet 5	**Risk Measurement Criteria – Fines and Legal Penalties**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $10,000 imposed by internal governance or local data protection agencies.	Fines between $10,000 and $100,000 from national health regulators or data protection authorities.	Fines greater than $100,000 under GDPR, HIPAA-like regulations, or national healthcare cybersecurity laws.
Lawsuits	Frivolous or non-frivolous lawsuits less than $25,000 are filed by patients, staff, or external parties. These are typically minor, quickly settled, or dismissed without trial, with no long-term impact on operations or reputation.	One or more non-frivolous lawsuits between $25,000 and $150,000 are filed. These may involve patients alleging moderate harm, staff legal disputes, or claims by partner institutions. Legal involvement and potential settlements are required.	Non-frivolous lawsuits exceeding $150,000 are filed. These may include critical malpractice cases, class-action lawsuits, or regulatory legal actions involving significant patient harm or systemic failure. Legal defense and potential damages pose serious financial and reputational risk.
Investigations	No external investigation; issue handled internally.	Low-profile investigation initiated by health ministry, data commissioner, or accreditation body.	High-profile, in-depth investigation launched with press coverage and risk to university hospital accreditation..
Other: (Regulatory Sanctions)	Verbal/written warnings from local bodies; no impact on operations.	Temporary restrictions on patient data processing or system usage.	Suspension of EHR system certification or license; restrictions on hospital operations imposed by authorities.

Allegro Worksheet 6	Risk Measurement Criteria – User Defined		
Impact Area	**Low**	**Moderate**	**High**
Research & Academic Integrity	Minor delays in accessing non-critical research data; no impact on deadlines or publication quality.	Data access issues delay research progress or submission; temporary reputational concern within academic circles.	Critical research data is lost or corrupted; clinical trials are halted or publications retracted; loss of grants or institutional credibility.
System Recovery Burden	Minimal downtime; IT staff can restore systems with routine effort and no additional resources.	Recovery requires external support, significant overtime, or temporary reallocation of staff.	Restoration is prolonged and resource-intensive; long-term infrastructure overhaul or vendor replacement is required.

Allegro Worksheet 7	Impact Area Prioritization Worksheet
Priority	Impact Areas
2	**Reputation and Customer Confidence**
4	**Financial**
5	**Productivity**
1	**Safety and Health**
3	**Fines and Legal Penalties**
6	**User Defined**

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Electronic Health Record (EHR) System	The EHR system stores and manages sensitive patient data, medical histories, lab results, prescriptions, and clinical notes. It is essential for delivering timely, accurate, and coordinated patient care.	A centralized digital platform that allows authorized hospital staff (doctors, nurses, admin) to access, update, and manage patient medical records securely and in real time.
(4) Owner(s) *Who owns this information asset?*		
Owned by the hospital's IT Department and overseen by the Chief Medical Information Officer (CMIO), who is responsible for its secure and compliant operation.		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Authorized medical staff and hospital administrators may access specific patient records based on their role and clearance level.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Doctors and designated clinicians can update diagnosis or treatment records; audit logs track every change to maintain traceability.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	All clinical and administrative staff must have real-time access during working hours to ensure safe and efficient care delivery.
	This asset must be available for 24 hours, 7 days/week, 52 weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	This asset must comply with GDPR, HIPAA (if applicable), and national healthcare cybersecurity regulations. It requires secure access, encryption, and audit logging to protect patient data. Non-compliance may lead to legal penalties, regulatory sanctions, or loss of accreditation.

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

❑ Confidentiality	❑ Integrity	[✓ ❑ Availability]	❑ Other

Allegro Worksheet 9a	Information Asset Risk Environment Map (Technical)
Internal	
Container Description	**Owner(s)**
1. On-premise hospital data servers hosting EHR databases	Hospital IT Department
2. Internal hospital network infrastructure (routers, switches, firewalls)	Network Administrator
	IT Security Team
3. Hospital-issued desktop and mobile devices used by clinical staff	Clinical IT Support Team
4. Backup servers used for data recovery and redundancy	IT Infrastructure Lead
External	
Container Description	**Owner(s)**
1. Cloud-based patient portal platform (if used)	External HealthTech Vendor
	Cloud Provider
2. Email systems integrated with EHR alerts or appointment systems	Third-party Email Service Provider
3. Remote access systems (e.g., VPN for off-site doctors)	IT Security Team
	Remote Access Vendor
4. Diagnostic device integrations (e.g., lab systems or PACS)	External Equipment Vendors
	Hospital IT

Allegro Worksheet 9b	Information Asset Risk Environment Map (Physical)
Internal	
Container Description	**Owner(s)**
1. On-site server room/data center storing the EHR database	IT Infrastructure Manager
2. Hospital wards and clinics (devices accessing EHR system)	Department Heads
	Clinical Staff
3. Staff offices with administrative access to EHR	Hospital Administration
4. Backup storage vault or secure hardware backup room	IT Backup Administrator
External	
Container Description	**Owner(s)**
1. Off-site cloud data center housing EHR backups	External Cloud Hosting Provider
2. Remote workstations used by authorized telehealth staff	Hospital IT
	Remote Access Staff
3. Third-party diagnostic labs connected to the EHR	Partner Organization
	Integration Lead
4. Transport systems (e.g., USBs or external drives used in emergencies)	Hospital IT Security Officer

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
1. Physicians and Surgeons	Clinical Departments (e.g., ICU, ER, Surgery)
2. Nurses and Medical Assistants	Wards and Specialty Units
3. IT Systems Administrators	IT Department
4. Hospital Administrative Staff	Patient Records
	Admissions Office
External Personnel	
Contractor, Vendor, Etc.	**Organization**
1. Cloud Services Provider (if applicable)	External Hosting
	Cloud Vendor
2. Medical Equipment Technicians	Partner Diagnostic Vendors
3. Software Support & Maintenance Provider	EHR Vendor
4. Telehealth Practitioners (if offsite)	Affiliated Partner Network
	Remote Team

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**

Information Asset Risk	Threat	Information Asset	Electronic Health Record (EHR) System
		Area of Concern	Unauthorized access through phishing targeting hospital staff, resulting in the potential disclosure and unavailability of electronic health records (EHR). This may constitute a violation of HIPAA due to the unauthorized exposure of protected health information (PHI), leading to regulatory penalties, reputational damage, and disruption of patient care services.
		(1) Actor *Who would exploit the area of concern or threat?*	External attacker (cybercriminal) targeting hospital employees
		(2) Means *How would the actor do it? What would they do?*	Attacker sends a phishing email impersonating IT, prompting users to click a fake login page and enter credentials.
		(3) Motive *What is the actor's reason for doing it?*	The attacker aims to access patient data for financial or malicious purposes and to disrupt hospital operations by encrypting or locking access to patient records, rendering them temporarily unavailable.
		(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?*	**Availability** – Access to patient records is disrupted, delaying treatment and affecting care coordination. **Confidentiality** – Unauthorized users may access sensitive health information.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High** ❑ **Medium** ❑ **Low**

(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**
Patient records become inaccessible, causing delays in diagnosis, treatment, and surgical procedures.	Reputation & Customer Confidence	High	4
	Financial	Moderate	3

	Hospital operations are disrupted, forcing staff to revert to manual processes and increasing the risk of medical errors.	Productivity	Low	2
		Safety & Health	critical	5
	Sensitive data may be exposed, resulting in loss of patient trust, legal reporting obligations, and potential regulatory investigations.	Fines & Legal Penalties	Moderate	3
		User Defined Impact Area	Low	2
			Relative Risk Score	3.17

(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 Email System (phishing entry point)	**Administrative**: Staff awareness training, mandatory phishing simulations every quarter. **Technical**: Advanced email filtering, anti-spoofing policies (SPF, DKIM, DMARC), URL/link analysis. **Residual Risk**: Minimal chance remains due to human error despite training.
Staff Workstations and Devices	**Technical**: Endpoint protection (antivirus, EDR), enforced multi-factor authentication (MFA), browser isolation for external links. **Physical**: Auto screen lock, secured access to terminals. **Residual Risk**: Slight chance of credential misuse if workstation is left unattended.
Credential Management System	**Technical**: Role-based access controls (RBAC), password complexity policies, MFA. **Administrative**: Access review policies every 90 days. **Residual Risk**: Residual insider misuse risk if staff ignore policies.
EHR System Servers (core data access)	**Technical**: Network segmentation, intrusion detection/prevention (IDS/IPS), daily backups with restricted access. **Administrative**: Disaster recovery policies and data access audits. **Residual Risk**: Very low, though minor disruptions may occur during patching or false positives.
Remote Access Systems (VPN, Telehealth Access)	**Technical**: Enforce secure VPN with MFA, session timeouts, and logging of all remote access sessions. **Administrative**: Grant access only to verified staff with signed usage agreements; conduct quarterly access reviews.

	Physical: Ensure remote users access systems from secured environments (e.g., hospital-issued devices). **Residual Risk**: Slight risk remains if remote devices are compromised or personal devices are used despite policy.

Allegro - Worksheet 10		**Information Asset Risk Worksheet**	
Information Asset Risk	Threat	Information Asset	Electronic Health Record (EHR) System
		Area of Concern	Ransomware attack encrypts patient records, rendering the EHR system inaccessible and potentially violating HIPAA if backups or data integrity controls are compromised.
		(1) Actor *Who would exploit the area of concern or threat?*	External attacker (ransomware group) targeting healthcare systems for financial extortion and operational disruption.
		(2) Means *How would the actor do it? What would they do?*	Attacker gains initial access via phishing or software vulnerability, then executes ransomware that encrypts critical EHR files and systems, locking out users.
		(3) Motive *What is the actor’s reason for doing it ?*	The attacker seeks to financially extort the hospital by demanding ransom in exchange for decrypting the EHR system, while also potentially leaking sensitive data to increase pressure.
		(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?*	**Availability** – Entire patient database becomes inaccessible, halting diagnostics and treatments. **Confidentiality** – Some ransomware strains exfiltrate data, causing patient data exposure. **Integrity** – Records may be altered or deleted during encryption or incomplete recovery..
		(6) Probability *What is the likelihood that this threat scenario could occur?*	[✓ ❑ **High**] ❑ **Medium** ❑ **Low**

(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**
Patient care is severely delayed or suspended due to inaccessibility of digital records.	Reputation & Customer Confidence	High	4
	Financial	Moderate	3

	Emergency care may be compromised.	Productivity	Low	2
		Safety & Health	critical	5
	Reputational harm and legal consequences follow data exposure.	Fines & Legal Penalties	Moderate	3
	Hospital may need to pay ransom or spend heavily on system rebuild.	User Defined Impact Area	Low	2
			Relative Risk Score	3.17

(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?*
Staff Workstations & Email Entry Point	**Administrative**: Quarterly anti-ransomware training, phishing simulations. **Technical**: EDR with behavior-based ransomware detection, email sandboxing, anti-spoofing policies (SPF, DKIM, DMARC). **Residual Risk**: Moderate — phishing and zero-day variants may bypass filters.
EHR System Servers (Core Data)	**Technical:** Network segmentation, frequent patching, ransomware-resistant backups. **Administrative:** Scheduled restore testing, backup access logging. **Residual Risk:** Low — if immutable backups and separation from core network are ensured.
Backup & Recovery Systems	**Technical**: Immutable storage, air-gapped backups, off-site replication. **Administrative**: Strict role-based access to backup servers, backup policy audits. **Residual Risk**: Low — but still vulnerable to overlooked misconfigurations.
Remote Access Systems (VPN, RDP)	**Technical:** Secure VPN with MFA, access rate-limiting, endpoint validation before session approval. **Administrative:** Regular remote access reviews, device policy enforcement. **Residual Risk:** Low to moderate — possible abuse from stolen credentials**.**

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	Threat	Information Asset	Electronic Health Record (EHR) System
		Area of Concern	Distributed Denial of Service (DDoS) attack targeting the hospital's EHR access portal or supporting network infrastructure, overwhelming it with traffic and rendering the system inaccessible to staff, patients, and telehealth services. This results in significant care delays, potential HIPAA compliance violations, and operational downtime.
		(1) Actor *Who would exploit the area of concern or threat?*	External attacker (cybercriminal, hacktivist, or DDoS-for-hire group) aiming to disrupt services or make a political/financial statement.
		(2) Means *How would the actor do it? What would they do?*	Attackers use a botnet to flood hospital servers or network gateways with fake traffic, exhausting bandwidth and system resources, preventing legitimate access to the EHR system.
		(3) Motive *What is the actor's reason for doing it ?*	The attacker aims to disrupt hospital operations for extortion, reputational damage, or ideological motives (e.g., protest against healthcare policies or practices).
		(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?*	**Availability** – Legitimate users are blocked from accessing the EHR system, delaying treatments and administrative coordination. **Confidentiality & Integrity** – Not directly affected, but prolonged access loss may lead to workaround practices that create secondary risks.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ☑ **Medium** ❑ **Low**

(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**
Staff and clinicians are unable to access patient records in real time.	Reputation & Customer Confidence	High	4

		Financial	Moderate	3
	Emergency procedures and digital workflows are disrupted.	Productivity	Low	2
		Safety & Health	critical	5
	Public trust may be affected due to perceived insecurity or instability.	Fines & Legal Penalties	Moderate	3
	Potential legal and regulatory impact if care delays result in harm.	User Defined Impact Area	Very Low	1

Relative Risk Score 3

(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?*
Public-Facing EHR Portals (e.g., patient access)	**Technical**: Deploy DDoS protection service (e.g., reverse proxy/CDN like Cloudflare), rate limiting, and IP reputation filtering. **Administrative**: Monitor traffic baselines; define escalation protocols with IT and ISP. **Residual Risk**: Low to moderate — volumetric attacks may still overwhelm if protection is not auto-scaled.
Hospital Network Gateway / Firewalls	**Technical**: Intrusion prevention systems (IPS), firewall traffic throttling, geo-blocking for foreign attack sources. **Administrative**: Incident response policy for DDoS events, coordination with ISP during peacetime. **Residual Risk**: Low — protection depends on early detection and upstream filtering.
Telehealth and Remote Access Services	**Technical**: Isolate services behind separate subdomains; apply API-level throttling and health checks. **Administrative**: Communicate downtime scenarios and alternate access routes to telehealth staff. **Residual Risk**: Moderate — attack spillover can impact these services even if not directly targeted.
Staff Alert and Communication Channels	**Administrative**: Establish backup communications (e.g., SMS alerts, physical routing instructions) during system outages. **Residual Risk**: Low — if fallback procedures are routinely rehearsed and kept updated.