FMEA Spreadsheet Template

System / Product / Process	FMEA ID	Revision
HealthNetwork		Intern Supervisor
Subsystem / Product / Process (if applicable)	**Party Responsible**	**Approved By**
HNetConnect, HNetExchange, HNetPay	HelthNetwork Support	
Team		
Cybersecurity Intern Team		

Failure Mode and Effects Analysis (FMEA)

ID+B 10: M21	System / Item / Process Step	Function	Potential Failure Mode	Effects of Failure	Severity	Causes	Occurrence	Current Controls
#	Name, ID number, etc.	Primary function	How could the system / item / process potentially fail?	Consequential impact on other systems, departments, etc.		All contributing factors		Prevention
1	Epic EHR Windows Server	Transmits patient data and provides assistance with	Malware and power outages	Could cause loss of human life due to inability to access clinicak	10		4	
2	Radiology PACS System	For storing and retrieving images from processes such as MRIS and	Storing and retrieving images	Could cause radiology to not be able to upload images delaying	10		4	
3	Laboratory Information System	Lab orders and processing	Lab order and processing	Could result in inability to test and share results	8		3	
4	Financial Systems	Patient billing and payment processing. Stores PII DSS	Patient billing and payment processing	Inability to generate or process bills	5		4	
5	CrowdStrike Falcon (EDR Protection	Endpoint protection is implemented on all endpoints (847)	Power outage, network connectivity issue, and threat actor	Inability to manage endpoints and detect malicious	6		3	

6	Palo alto PA-33220 Firewalls	Endpoint protection is implemented on all endpoints (847)	Power outage/ Turned off by threat actor	Inability to ensure malicious traffic does not reach web application	8		3	
7	Active Directory 2019 with Azure AD Connect	Service used in authentication and access controls.	Turned off by threat actor/ Power outage	Inahbility to authentication users wanting to access	8		4	
8	Loadbalancers	Distributes traffic across various web applications like MyChart.	Power outages, threat actor	Inability to distribute traffic over the network leading to denial	6		5	
9	23 Servers	Servers are used for hosting web applications, databases, and	Power outages, threat actor	inahbility to how applications and data processing	8		3	
10	Rapid7 (Vulnerability Scanner)	Scans multiple IT assets for vulnerabilities	Turned off by threat actor/ power outage	Inability to scan vulnerabilities on multiple systems	7		3	
11	Databases	Stores information or various web applications	Power outage, disabled by threat actor	Inability to retrieve payments, mail, or some	8		3	
12	Log servers	Logs transactions from various web applications	Threat actor/ Power Outage	Inability to account for changes made within various	5		3	
13	Splunk	Also SOC to view centralized logs from various web applications	Threat actor/ Power Outage	Inability to view logs possibly leading to threat actors evading	5		4	
14	Patient Health Information	Used by web applications to provide patient info for hospitals	Threat actor/ Power Outage	Loss of availability, integrity, or confidentiality of data	10		3	

Date
Date Completed

RPN Columns contain a formula to auto-calculate; do not alter or delete.

						FMEA Results					
s	Detection	RPN	Recommended Actions	Owner	Date Due	Action Results	Date Completed	Severity	Occurrence	Detection	RPN
Detection		Risk Priority Number	Steps required to reduce severity, occurrence, and detection	Organization, team, or individual responsible	Target date of completion	Actions taken	actual date of completion				Risk Priority Number
	3	120									0
	3	120									0
	3	72									0
	4	80									0
	8	144									0

	10	240									0
	8	256									0
	4	120									0
	5	120									0
	8	168									0
	5	120									0
	10	150									0
	9	180									0
	2	60									0