HMIS COMMITTEE

Ranjeet Deshmukh Dental College & Research Centre, Nagpur

STANDARD OPERATING PROCEDURES

(ISO 21001: 2018)

Issue No.: 2
Issue Date: 06.10.2023
Copy No: Master copy
Holder Name : Committee Chairperson

HMIS COMMITTEE- SOP

Ranjeet Deshmukh Dental College & Research Centre, Nagpur

Standard Operating Procedures

Purpose -

The purpose of Hospital Management Information Systems (HMIS) in dental institutions is to streamline and enhance various aspects of healthcare administration and patient care. Specifically within dental institutions, HMIS serves several important purposes:

1. Patient Records Management: HMIS helps in the digital management of patient records, including dental history, treatment plans, and progress notes. This facilitates easy access to patient information, reducing paperwork and improving efficiency.
2. Appointment Scheduling: It assists in scheduling dental appointments efficiently, reducing waiting times for patients and ensuring that dental professionals can manage their time effectively.
3. Billing and Financial Management: HMIS helps in managing billing, insurance claims, and financial transactions related to dental treatments, making the financial aspects of patient care more organized and accurate.
4. Inventory Management: Dental clinics require various supplies and equipment. HMIS helps in tracking inventory levels, ensuring that necessary items are always available for patient care.
5. Treatment Planning: It aids dental professionals in creating and updating treatment plans for patients, helping to keep track of ongoing treatments and follow-ups.
6. Reporting and Analytics: HMIS can generate reports and analytics on various aspects of patient care, such as patient demographics, treatment outcomes, and resource utilization. This data can be used for decision-making and quality improvement.
7. Patient Communication: Some HMIS systems include features for patient communication, such as appointment reminders and educational materials, which can improve patient engagement and adherence to treatment plans.
8. Security and Privacy: Ensuring the security and privacy of patient data is a critical function of HMIS, helping dental institutions comply with healthcare regulations and protect patient information.
9. Research and Education: Data collected through HMIS can be valuable for research purposes and educational programs within dental institutions, contributing to advancements in dental care.
10. Interoperability: HMIS can integrate with other healthcare systems and institutions, facilitating seamless sharing of patient information and referrals when necessary.

Overall, the purpose of HMIS in dental institutions is to improve the efficiency of administrative tasks, enhance patient care, and contribute to the overall quality and effectiveness of dental services. It plays a crucial role in modernizing dental practice and ensuring that patients receive the best possible care.

Scope-

The scope of Hospital Management Information Systems (HMIS) is extensive, encompassing a wide range of functions and activities that contribute to the efficient operation and enhanced patient care within the institution. Scope of HMIS in dental institution is vast and multifaceted, with the primary goal of enhancing patient care, improving operational efficiency, and ensuring the effective management of dental services. It plays a critical role in modernizing dental practice and promoting high-quality dental care.

Operating Procedure-

1. The HMIS committee is formed by the head of institution for electronic / paperless patient OPD service management.
2. HMIS Committee ensures paperless and hassle free patient referral across all departments of the institute.
3. HMIS Committee ensures smooth functioning of the HMIS software for patients record ,indent and billing transactions.
4. Committee is responsible to maintain and provide patients records daily, monthly, or yearly and make them available whenever required by the institute.
5. Committee conducts meetings biannually and as & when required with department representatives to discuss any HMIS related issue.
6. Committee conducts training/ workshops for smooth conduct and referral of patients as and when required.
7. The committee takes review of each department on regular basis.

Dr.Mukta Motwani
Chairperson
HMIS Committee

RANJEET DESHMUKH DENTAL COLLEGE AND RESEARCH CENTRE, NAGPUR

ENTERPRISE RESOURCE PLANNING (ERP)

SOP/GUIDELINES/MECHANISM/CODE OF CONDUCT

Date of formation of committee: November 2021

The Enterprise Resource Planning (ERP) Committee is functioning to make the educational operating process more efficient through Sack Information System (Synchronic Software). ERP System increases productivity, and the efficiency of planning, designing, and operating academic resources through access to real time data and analytics of institute.

Objectives:

1) To manage student's attendance and curriculum data updates.
2) To track student's progress through centralized dashboard view anytime by teachers.
3) To assist in administrative process management.
4) To streamline student's section and account section management related to admission and fees records.
5) To allow information sharing across various departments while establishing clear communication between management, staffs and students.
6) To enhance communication between parents and institution by sharing progress of their wards.

Functions:

1) **Structure of the committee:**

   It consists of Dean, chairperson, Co-Chairperson, Coordinator and members from each department. The ERP Committee functions with the coordination of main committee and all department HOD's, department representatives, all faculties, Student sections, IT Department, Account section and Software Coordinator.

ERP COMMITTEE

Committee Designation	Name	Designation
Dean	Dr. Usha Radke	Dean
Chairman	Dr. Mukta Motwani	Vice-Dean (Clinical)

Co-Chairman	**Dr. K. Venugopal Reddy**	**Professor & HOD**
Coordinator	**Dr. Jaishree Chahande**	**Lecturer**
Members	**Dr. Purva Choudhary**	**Reader**
	Dr. Tapasya Karemore	**Reader**
	Dr. Sandeep Khandaitkar	**Sr. Lecturer**
	Dr. Pratik Burad	**Sr. Lecturer**
	Dr. Dawal Mody	**Reader**
	Dr. Pritam Khorgade	**Sr. Lecturer**
	Dr. Rakshata Sorte	**Sr. Lecturer**
	Dr. Swapnil Patil	**Lecturer**
Frequency of meeting	**Quarterly**	

2) Meetings:

ERP committee meetings are conducted quarterly or as and when required; first meeting in every new academic session (July and January-Summer and Winter academic sessions) to plan and execute new batches updates in software and other meetings to take follow up of all department attendance updates.

3) Features/Mechanism:

a) **Feedback**: - With the help of Feedback Module, we take feedback from Students related to Associated Feedback and General Feedback. Also we take feedback from Teaching, Non-Teaching, and Parents about our Institute.

b) Grievance: - We Submit Grievance for maintenance department & also for Grievance committee, there is provision for Anonymous, if someone won't like to disclose his/her identity.

c) Academic Monitoring: - With the help of Academic Monitoring, we maintain Students Academic Records like, Students Attendance, Teaching Plan, Time Table, etc.

d) Accounts: - With the help of Accounts Module, we maintain Book Keeping.

e) Admission: - With the help of Admission Module, we maintain online Admission process of Students.

f) Clearance: - With the help of Clearance Module, we maintain Clarence of All Section like Accounts Dues, Library Dues, Hostel Dues, or Any Other Departments Dues.

g) **Committee**: - With the Help of Committee, we maintain All Committees Meeting records such as Meeting Attendance, Minute of Meetings, Action Taken, after Creation of Meeting Automatic SMS also sent to all committee Members.

h) **Establishment:** - With the help of Establishment module, all Employees update his/he records on portal.

i) **Events**: - With the help of Events module, we maintain All types of Events All Academic & Non Academic on portal such as Event Photos, Guest name, First, Second, Third position name, etc.

j) **Exam Section:** - With the help of Exam Section, we maintain Examination mark of students subject wise, term wise, etc.

k) **Fees:** - With the help of Fees module, we maintain Fees of All Students, such as Outstanding position, etc.

l) **Front Office**: - With the help of Front Office Module, we maintain Notices, dashboard Events Photos, etc. Also generate students related Certificate such as Bonafied, Character, Expenditure Certificate, etc.

m) **Hostel**: - With the help of Hostel Module, we maintain all records related Hostel, Such as Fees, Room No., Mess Bill, Hostel Attendance, etc.

n) **Inward & Outward:** - With the help of Inward & Outward module, we maintain all Inward & Outward Letters records.

o) **Library:** - With the help of Library Module, we maintain all types of Library records such as Book issued to Students, Employee., No. of Books, etc.

p) **Student Section: -** With the help of Student Section Module, we maintain All Records related to Students.

q) **Training & Placement: -** With the help of Training & Placement, we maintain all record of Training, such as Trainer Name, Trainee Details, Trainee Attendance, Remarks, etc.

r) **User Management:** - With the Help of User Management, we maintain SMS Module, Complaint Management, etc.

POLICY & GENERAL STATEMENT

I. POLICY & GENERAL STATEMENT

Information resources are owned by VSPM AHEand exist to support its mission. VSPM AHE's information resources must be used, managed and protected appropriately to ensure that data is:

1. available;
2. accurate and complete; and
3. Disclosed appropriately when required.

VSPM AHE's information resources fall under the authority and responsibility of the Chief Information Officer (CIO) and are subject to federal, state, and local laws and regulations, and VSPM AHE policies. The Management delegates the responsibility to department heads for ensuring the university is in compliance with all relevant laws, regulations and policies. The Chief Information Security Officer (CISO) assists department heads by establishing security policies, procedures and guidance for university information resources.

VSPM AHE's information resources are subject to many different threats that can reduce or eliminate data availability, compromise integrity and violate confidentiality; so it is imperative they are safeguarded appropriately. Individual users' actions can contribute to or reduce the risk of most threats; so all users are responsible for their use, management and protection of information resources and are accountable for their actions. All users have one or more roles to fulfill related to university information resources.

II. DEFINITIONS

Information Resources – Data, software, equipment, facilities and devices that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit VSPM AHE information. Any electronic equipment, devices or media that a user connects to the network or uses to process or store university information, including equipment, devices or media owned by the user or funded by another source, are considered university information resources for the purpose of compliance with laws, regulations and policies.

Examples:

Applications, web sites, software programs, servers, personal computers, notebook computers, netbook computers, personal digital assistant (PDA), pagers, mobile phones, USB flash drives, external hard drives, CDs, DVDs, backup tape, telephones, fax machines, routers, switches, cabling, network attached data storage, printers, network attached or computer controlled medical and laboratory equipment.

III. RESPONSIBILITIES

All users must identify their information resource role(s) and accept the associated responsibilities.

Each user, by default, is assigned the User information resource role. Users may have more than one role, and are responsible for identifying all of their additional roles and meeting the responsibilities of each role. For example, a User who is responsible for a business function that depends on a system may also be a System Owner; a User who is responsible for the implementation of a new system may also be a Project Manager; a User who is responsible for technical support of a system may also be a Custodian.

Information Resource Roles:

- User
- System Owner (Information Owner, Data Owner)
- Custodian / Information Security Administrator
- Project Manager
- IT Infrastructure Owner
- Chief Information Security Officer
- Chief Information Officer
- Auditing & Advisory Services
- Office of Institutional Compliance
- Triage Team

A. User

A User is anyone who is granted access to information resources.

Examples of Users include faculty, students, residents, staff, alumni, retirees, continuing and distance education students, researchers, principal investigators, visiting faculty, observers, volunteers, business partners, affiliate hospitals and clinics, contractors, vendors and consultants.

User's primary responsibilities:

1. Use university information resources responsibly and for their intended purposes as established by the System Owner; comply with controls established by the System Owner and be accountable for their actions.
2. Know and comply with published policies and procedures.
3. Read and sign the Information Resources User Acknowledgement Form.
4. Do not share passwords or similar information or devices used for identification and authorization purposes.
5. Protect data appropriately regardless of the method of access.
6. Determine if other information resource roles apply to him or her, accept responsibility for the role(s) and meet the associated responsibilities.
7. Report information security incidents, including unintentional or intentional misuse, in accordance with Computer Security Incident Response Policy.

B. System Owner (Information Owner, Data Owner)

A System Owner is the person responsible for the business function or project that depends on a system. If the system supports multiple business functions, the system owner is the person responsible for carrying out the overall program that the system supports. A system is a university information resource.

Examples of System Owners include department heads, individuals with financial and/or administrative responsibility and accountability for their departments or projects.

System Owner's primary responsibilities:

1. Formally assign/acknowledge the Custodians for the system, including outsourced systems. Approve the level of access the Custodian needs to perform, required administration and maintenance and to implement required security controls and procedures.
2. Ensure the system is in compliance with applicable laws and regulations.
3. Determine the system's value.
4. Perform a risk assessment annually for mission critical systems and biennially for non-mission critical systems. Identify and document actions required and taken to meet acceptable risk levels.
5. Classify and secure data appropriately, taking into consideration security or operational controls required to ensure the availability, confidentiality and integrity of the system's data. Communicate these controls to the Custodian, train the users as needed and confirm the controls are in place on a regular basis.
6. Document, obtain approval and be accountable for exceptions to security controls. The System Owner must obtain approval for exceptions to security controls from the CISO.
7. Determine appropriate access for system users based on the minimum necessary access required to perform their assigned job responsibilities. Approve new access assignments and review all assigned access for appropriateness on a regular basis.
8. Report information security incidents, including unintentional or intentional misuse.
9. Create, maintain and train users on a departmental business continuity plan.
10. Include an adequate disaster recovery plan for the system as part of the departmental business continuity plan. Assure the assigned Custodian has a copy of the disaster recovery plan.
11. Retain and destroy records in accordance with policy.

C. Custodian / Information Security Administrator

A Custodian provides technical facilities and/or hardware, software or application production support services for a university information resource. Information Technology management and/or the System Owner assign him or her and should have the knowledge and experience required to adequately perform the associated responsibilities.

An Information Security Administrator (ISA) is a Custodian that has additional, security-focused responsibilities. A third party providing outsourced support cannot be an ISA.

Examples of Custodians include IT Infrastructure Owners, system, database and application administrators, third parties providing outsourced support, school or department support personnel who have physical or logical control over hardware, software or services.

Custodian's primary responsibilities:

1. Perform required administration and maintenance of the VSPM AHE information resources.
2. Implement applicable information resource policies, procedures and guidance,including change management and security safeguards and controls.
3. Report information security incidents, including unintentional or intentional misuse.
4. Assist System Owner in performing risk assessments and evaluating the cost effectiveness of controls.
5. Implement controls specified by System Owner and confirm they are in place as appropriate.
6. Implement processes that aid in detecting, reporting and investigating security incidents.
7. Assist System Owners in disaster recovery planning for the university information resource. Maintain a copy of the disaster recovery plan in the appropriate location(s).
8. Assist System Owners with the destruction of records.

D. Project Manager

A Project Manager for an information technology project is responsible for its entire implementation from concept to rollout, which includes strategic, financial and technical responsibilities, and ensuring the project is built and implemented securely. The implementation includes all or most of the following: procurement, functional and technical specification documentation, development, testing, integration, installation and training. Consideration must also be given to any manual or automated processes the implementation will impact. An information technology project is any project that includes or relies on a university information resource.

Typical Examples of Project Managers include System Owners, Custodians, IT Infrastructure Owners.

Project Manager's primary responsibilities:

1. Determine if existing resources can be used to deliver the information technology project by contacting the Central Information Technology department.
2. If the existing university resources are not adequate, the information technology project will be outsourced or hosted by a third party who will transmit, process or store data.
3. Follow the necessary guidelines when implementing information technology projects.
4. Ensure the information technology project is in compliance with applicable laws and regulations.
5. Identify, document, and address security requirements in all phases of development or acquisition of information resources.

E. IT Infrastructure Owner

An IT Infrastructure Owner is a Custodian of shared technology and is responsible for maintaining and operating hardware and associated software to provide computing services, storage and connectivity for information resources. IT Infrastructure Owners are information technology professionals who report to the Central Information Technology department directly or indirectly.

IT Infrastructure Owner's primary responsibilities:

1. Procure, support, maintain and/or operate computing services, storage and connectivity, including but not limited to:

•Servers •Storage systems •Internet •Intranet •Wide Area Ethernet network (clinics and business partner connections) •Fire

alarm system•Security camera systems•Telephone system•Firewalls•Intrusion detection/protection

2. Implement applicable information resource policies, procedures and guidance, including security and change management controls.

F. Chief Information Security Officer (CISO)

The Management designates the CISO to serve as the information security officer. The CISO leads the Information Security and Disaster Recovery Planning department and reports directly to the Management, with an indirect reporting relationship to the Chief Compliance Officer and the Chief Information Officer. The IT Security Core team and Information Security Administrators (ISAs) assist the CISO.

CISO's primary responsibilities:

1. Develop, oversee the implementation of, and monitor a documented Information Security Program and related security policies and procedures (including monitoring the effectiveness of defined controls for mission critical information).
2. Obtain approval of the Information Security Program by the Management.
3. Provide regular reports and updates to the Compliance Team.
4. Promote the information resource security policies, procedures, standards and guidelines applicable to central and decentralized areas of VSPM AHE.
5. Work with System Owners, Custodians, ISAs, IT Infrastructure Owners, Project Managers and other information technology professionals to determine security requirements for information resources and security solution implementations that protect against unauthorized or accidental modification, destruction or disclosure.
6. Have authority over security solutions and implementation decisions.
7. Review and approve security requirements for purchases of hardware, software, applications, information services or system development services.
8. Perform risk assessments to determine if information resources are adequately protected.
9. Make policy and procedure changes and practice recommendations as appropriate to improve security posture.
10. Establish and administer a process to address violations of security policies and procedures.
11. Exercise authority to issue exceptions to security policies and procedures after appropriate review. Any such exceptions shall be justified, documented and communicated as part of the risk assessment process.
12. Obtain access to any university information resource as needed.
13. Report certain violations to the Triage Team as required.
14. Ensure information security awareness training is provided to all employees on a regular basis and to all new employees within 30 days of date of hire.

G. Chief Information Officer

The Management has designated the CIO as the information resource manager. The CIO is responsible for overseeing the management of the information resources and risk management program.

CIO's primary responsibilities:

1. Develop strategic information technology plans and operating and capital budgets for the university to provide reliable and secure university information resources, which include applications and infrastructure supporting the administrative, academic, research and clinical functions of the university.
2. Promote the university information resource administrative and operational policies, procedures, standards and guidelines applicable to central and decentralized areas of the university.
3. Promote record management policies and procedures and provide appropriate systems and services for effective and efficient records management capabilities consistent with industry standards and federal, state, and local laws and regulations.
4. Promote partnerships with internal and external parties.
5. Serve as VSPM AHE's technical representative.
6. Perform an annual risk assessment for university information resources.
7. Responsible for the design, execution and effectiveness of internal controls providing reasonable assurance that operations are effective and efficient, assets are safeguarded, financial information is reliable, and applicable laws, regulations, policies and procedures are met.
8. Respond to information resource audit recommendations and risk mitigation requirements.

H. Auditing & Advisory Services

Auditing and Advisory Services assess information resources and the control environment and reports results to management and the Audit Committee. Failure on the part of management to enforce compliance may result in fines and penalties.

I. Office of Institutional Compliance (OIC)

OIC promotes compliance with all applicable legal, regulatory and policy requirements. The OIC assists the Information Technology department in conducting an annual risk assessment, identifying high risk areas, developing risk mitigation plans and performing verification activities to ensure the level of information resource risk is within a range acceptable.

J. Triage Team

The Triage Team meets regularly to review incidents of suspected non-compliance. The Triage Team is made up of the following permanent members, with others requested to attend as needed:

- Chief Legal Officer
- Chief Human Resources Officer
- Chief Audit Officer
- Chief Compliance Officer

Triage Team's primary responsibilities:

1. The Chief Compliance Officer, in coordination with the Triage Team, investigates or coordinates the investigation of all reports of suspected non-compliance with federal, state or local laws or regulations, VSPM AHE System policies.
2. The Triage Team recommends an appropriate course of action, which may include counseling, disciplinary action and/or reporting to another agency as required.

The Triage Team reviews the results of all investigations and recommends further action as necessary.

IV.PROCEDURES

Service Requests

1. User inputs requests via helpdesk system, email or telephone.
2. Request is assigned to appropriate personnel in IT Department.

3. User is contacted if more information is required to complete request.
4. User is contacted with anticipated completion date.
5. If initial technician cannot resolve request, reassign request to a Level 2 technician
6. Technician completes request.
7. Technician resolves ticket.

Creation of User Accounts for new staff

1. Receive signed Acceptable Usage Policy from Human Resources.
2. Ticket created and assigned to System.
3. Account created and account information sent in ticket.
4. Email sent to immediate supervisor with requested account information.

Termination of User Accounts

1. Receive notification from Enrollment Services that an employee is no longer active.
2. Generate a help desk ticket.
3. Assign ticket to Network Support Team.
4. Generate a help desk ticket. Assign ticket to IT Support Team

Computer Moves

1. User fills necessary details and gets signatures on Movable Property form.
2. User submits form to helpdesk.
3. Helpdesk request is generated and assigned to appropriate personnel.
4. Computer is moved and completed Movable Property form forwarded to Property Control.
5. Helpdesk request is resolved.

Request for new software

1. User submits helpdesk request with required specifications/software titles.
2. Request is assigned to appropriate personnel.
3. Technician requests quotes from vendor(s).
4. Once quote(s) is received, technician attaches quotes to request.
5. Helpdesk request is resolved.

Custom Report Request

1. User submits helpdesk request with required specifications for report.
2. Report request should include: a. Format b. Required fields c. Sort order d. Group order e. Point of contact f. Source of information (form names)
3. Request is assigned to appropriate personnel.
4. Technician contacts user to review report requirements.
5. Create report.
6. Report attached to helpdesk request for user review.
7. If user approves report, request is resolved.

Multimedia Request

1. User submits helpdesk ticket or email with meeting room requirements with a minimum of one-week prior notice.
2. Ticket/email should include:
   Date and time of meeting
   Location
   Equipment requirements (i.e. laptop, video, audio)
   Type of meeting

3. IT coordinates with Facilities Services for setup requirements (if needed).
4. Multimedia requirements are setup.

Suspected security violation

1. User submits helpdesk request with detailed information
2. Request should include
- Time
- Error message
- Computer name
3. Request is assigned to appropriate personnel
4. Validity of request will be determined
5. If valid, investigation will occur
6. Helpdesk request is resolved.

Software

The IT Program will maintain all software, which is located on VSPM AHE's system. As it pertains to software, the following procedures will be followed:

a) The IT Program will maintain a current list of standard and recommended software
b) To ensure software is compatible and not destructive to the computer systems, the IT Program will approve any and all software programs.
c) If a user is interested in software that is not on the maintained list, the user will need to complete an IT Work Order to request assistance in determining if that software is sustainable on computer systems and network.
d) The IT program will determine if software is qualified as being compatible with VSPM AHE's system.
e) If software is not qualified as being compatible with the standard software or system, software cannot be installed on the system.
f) If a software program exceeds the specifications of the user's computer system, the user will be notified to look for alternative software or to find program funds to upgrade the system.
g) All software installed on computers or on the servers must have a valid license.
h) Should sever-based software make a server unstable, the IT Program will be responsible for restoring any data that was stored on a sever is backed up by the IT Program's backup server.
i) The IT Department must monitor all software licenses in order to ensure compliance with the vendor's license agreements.
j) Users may contact the IT Department to obtain additional guidance, quotes and advice on any software.
k) Typesof software used:

NKP Salve Institute of Medical Sciences & Lata Mangeshkar Hospital
Digdoh Hills, Hingna Road, Nagpur
Contact 07104-66500

Project Management Process:

A formalized project management process will ensure that projects are documented, that users have a single point of contact, and that limited personnel resources are used to the best advantage. The Project Manager is the key to project management and will be responsible for the analysis, design, workload planning, testing and implementation of projects. The Project Manager will review project requests and assign the project to the staff member whose talents are the closest fit.

A. Request For Services:

The first step in project management is generating a formal request for a project based on VSPM AHE's requirement. Requirements may come from any level in the organization, including from within Information Technology itself. Requirements that are substantial enough to become projects must be formalized before being acted upon. The reason for the formality in this process is to document the workload in the IT Department and to obtain a written description of the user's request. A standard Project Request Form to assist the user in documenting their request. It also ensures that department heads are aware of the projects that the IT Department is working on for them, and will enable them to prioritize projects if necessary.

Each request must be submitted through the requestor's chain of command via his/her Department Head or Chair to the IT Department. The IT Department will respond via email to all requests within ten (10) working days. The response will include whether the request is accepted or rejected, and a projected time line for the project based on the current workload.

B. RequestForServicesApprovalProcess:

When a request is received on a Project Request Form, the Project Manager assigns a number and logs the request. At weekly meetings, the CIO will evaluate any new requests. The Project Manager evaluates the problem identified in the request and make recommendations on an appropriate course of action and possible alternatives. Other staff members are consulted as necessary to complete the initial review. The CIO then evaluates the review and forwards the request back to requester with any additional comments. Within two (2) working days, the CIO receives the review and approves one of the following three actions:

- Approve the request and assign it to the appropriate Group with its original priority or adjusted priority.
- Reject the request, identifying the reason, and arrange a meeting with the requestor to discuss the issue.
- Delay the request until a preliminary feasibility study is completed. At that time, the project is approved or rejected.

The CIO must respond within ten (10) working days from the receipt of the request to all formal requests for services.

C. Project Management Steps:

Each project must be planned in detail and controlled by the Project Manager. Control is involved with comparing actual progress with the plan and taking corrective action when the two do not correspond. The project plan will be prepared by the Project Manager and will detail all the work that will need to be done. The plan also lists the individuals whose skills are needed to work on the project, a work breakdown chart for the project, and a projected time line with milestones. The Project Manager may find it necessary to revise the plan during the process due to additional user input or discovery of new information. However, before beginning the development step, a plan must be laid out and users kept informed of changes, especially time line changes. The CIO will be available to the Project Manager to assist in developing the plan. The Project Manager should keep all informed of changes to the project plan as they occur.

Below is a list of steps that a Project Manager typically follows while constructing a project plan. The steps below are guidelines that every Project Manager should follow when developing their plan, and designing and implementing their project. Some steps may require more or less time, and may involve only the Project Manager or both the Project Manager and Project Team Members depending upon the scope of the project. The user who requests the project should be heavily involved in the project management process.

1. *Problem Definition* - After a user's request is received the CIO to makes a decision whether to accept or reject a project. The user's request and any comments by the CIO becomes the basis for the Project Manager to begin the project. Once assigned, the Project Manager reviews all documents with the project and begins to develop a plan.

2. *Process Analysis* - The Project Manager will begin the project with a thorough understanding of the business process being modeled.

The Project Manager must become familiar with the user's business processes before developing the discrete tasks to accomplish the project. This includes determining problems that exist in the current system, specifying objectives and goals, and listing possible system constraints or limitations. A determination and definition of interfaces with any other existing system, and requirements within or between departments, must also be completed. This involves all organizations that either are sources of data or users that require information from this particular system. Full analysis of the system must be conducted to produce the functional requirements of the entire system.

3. *Functional Description* - After conducting a process analysis, the Project Manager will develop a functional description. The functional description defines the system requirements and provides the requestor with a clear statement of the operational capability to be developed. If the requirements change at any point, the functional description should be updated and receive concurrence from the user. The functional description is the basis for mutual understanding between the user and IT Department.

4. *User Requirements* - After the functional description is developed, the Project Manager must determine exactly what is to be included in the system design and define these elements. A list of every single necessary requirement that the new system must accommodate as well as those features that are desirable must be prepared. System features that the user would like to have incorporated in the new system must be recorded. Specifications must be based on what the user wants, not on what the Project Manager wants.

5. *System Design* - In the design phase, the functional requirements are further developed and refined. Possibly, several alternate approaches may be conceptualized and compared from the standpoint of best cost and benefit factors. Mock-ups of new forms, reports, screens, and other systems documents may be prepared, if the project is a software project. Physical and logical diagrams will be prepared if the project is a system or network. Prototyping is encouraged so that the user has an opportunity to approve the design. For software design projects, the file structures and report design must be accomplished. For all projects, the impact on systems and networks must be determined before a design is approved.

Once an acceptable design has been developed, the Project Manager will develop a Plan of Action and Milestones (POAM) and a workforce loading plan. Normally when developing a POAM and the workforce loading plan, the Project Manager should plan on team members being available to work on projects no more than 28 hours per week. The Project Manager must consider the project team members' other commitments to develop a realistic time line. The CIO will approve the project team, and the supervisors of the project team members must be kept notified of project time requirements. The workforce-loading plan can be in any format, but the Project Managers may find it useful to develop a matrix of tasks and project team members with the number of hours each team member should expect to work on a task. Critical tasks, tasks that must be completed before other work can be done, should be defined. During the design phase the Project Manager should develop the Life Cycle Management and obtain LCM approval if it is required.

6. *System Development* - During this phase, the system design is implemented. If design changes are required, it may be necessary to revisit earlier steps to ensure that the system is designed properly. Operation, use and maintenance information is developed.

7. *Acceptance Testing* - A test plan must be devised that states which tests will be conducted to verify that the system complies with the requirements identified in the user requirements specification. The test requirements are developed, the scope of the test is identified along with pass/fail criteria, and the system is tested. The entire integrated system must be tested to ensure that the hardware and all software components work as designed. All testing must take place in a controlled environment before the complete project is introduced to users. A functional configuration audit is performed to ensure that system performance complies with requirements specifications and any approved changes. A physical configuration audit is performed to ensure all deliverables have been in fact produced, procedures were followed, and standards were adhered to.

8. *User Training* - Any change in a system requires at least new knowledge and usually new skills on the part of operators, administrators, users, and managers. Orientation on the system is required for everyone in the organization affected by the new system. If the project was not to create a new system, but to revise a system, modify a network, or release a new version of software, somewhat less training may be required. For some, orientation may require only a short memo, for others several hours of briefings.

Training requires the teaching of new skills and may include techniques such as formal classroom training sessions, training aids, practice sessions, and assistance on the job. The Project Manager is responsible for developing training plans based on system requirements.

9. *Documentation* - Documentation must be prepared as required. At a minimum, there must be sufficient documentation to fully describe and explain all system programs and operations, or changes and the reasons for the changes. A maintenance manual must include, at a minimum, the production environment, location of all external files used, and a list of all files needed by the system with a summary of information on each. This type of document is essential for trouble-shooting purposes, for modifying or upgrading the

existing system, and for designing a new one. It is also essential to prepare guidance to the people who will operate the system. Documents must be readable and understandable to the user who must approve them. LCM documentation developed during the design phase should be included as part of the documentation.

10. *Operation* - The system is implemented and turned over to the user. Data creation and data conversion from the old system to the new system must be accomplished, if necessary. If the system is a replacement for an existing system, phase out of the old system must be planned.

11. *Evaluation* - All team members will contribute lessons learned on the project and send them to the Project Manager for consolidation. These will be compiled into a written record for future reference and maintained with other documentation for theproject. If applicable, the Project Manager will prepare a Future Action Plan on possible upgrades and enhancements.

Guidelines for Preparing an Information Technology Services Project Request

A response is due within 10 working days to all requests received by the IT Department. The following are guidelines for preparing the Project Request Form:

- *Project Name:* To be filled in by the IT Department.
- *Department:* Provide the name of the requesting department.
- *Date of Request:* Enter the date of the request.
- *Requesting Individual:* Provide the name, title and phone number of person initiating the request.
- *Contact/Liaison:* Provide the name, title, and phone number of person who is the principal contact on all matters relating to the project for the requestor.
- *Nature of Request:* Describe in as much detail as possible the nature of the request:
- *Priority Requested:* Indicate priority needed and justify why. Priorities changed by Information Technology Services will be marked in the priority-approved space.
  - Emergency Priority. (Emergency fix or change required. Immediate response required. This priority is only available for operational systems.).
  - High Priority. (Impact on operational readiness, development schedule, or significant cost impact, if not fixed immediately.)
  - Normal Priority. (All other.)
- *Critical Date:* The latest acceptable date for satisfying the Project Request. Enter the critical date and justification.
- *Basic Purpose/Objective:* Describe in a brief but specific manner the basic purposes or objectives of the project.
- *Reason for Request:* Provide reasons for the request (e.g. to comply with changes in policies/procedures).
- *Identify Source of Funds:* Identify potential source of funds or alternate resources for the project in the event Information Technology Services resources are not available.
- *Department Head Signature:* The Head of Department (HOD)must sign and date the request.
- *Management Signature:* Management signature indicates approval. Paper copies must be signed.

2.9 Feedback & Complaint Management

Customer Feedback

a. Filled Customer Feedback forms are to be collected on a daily basis from clients.

b. Customer feedback Form shall be reviewed periodically and report on Customer Satisfaction index shall be generated quarterly.

c. Customer Satisfaction Report shall be checked/reviewed for continual improvement.

Complaint

d. In case of the Customer Complaint, Customer is cordially heard first and complaint is logged in the Complaint Register.

e. Complaint recorded by the customer is reviewed and accordingly correction and/or complaint are redressed through internal discussions.

f. In case the complaint falls in the severe category, e.g. Expired Goods, Goods not as per prescription post correction and/or complaint redressal, Corrective Action is initiated by identifying the root cause, taking action to avoid recurrence and finally reviewing the Corrective Action taken for effectiveness.

g. Records of correction and Corrective Action (if applicable) is established and maintained in the Corrective Preventive Action Report.

h. Corrective Action Report shall be also generated in case of Critical customer feedback and/or suggestions and/or in case of any product/service non-conformity internally identified.

i. Preventive Action Report shall be generated in case of potential problem with the action flow similar to the Corrective Action.

DR. KAJAL MITRA
DEAN

DEAN
N.K.P. Salve Institute
of Med. Sciences
NAGPUR

Appendix 1

Project Request Form

ECT NAME:

RTMENT:

OF REQUEST:

E OF REQUESTOR:

:

IE NO:

E OF CONTACT/LIAISON:

:

IE NO:

OF REQUEST:

RITY REQUESTED:

RITY APPROVED:

IFICATION FOR REQUESTED PRIORITY:

ICAL DATE:

SON:

IC PURPOSE/OBJECTIVE: