HEALTH AND FAMILY WELFARE DEPARTMENT

2.5 IT Audit of Hospital Management Information System and Stores Management Information System

Executive Summary

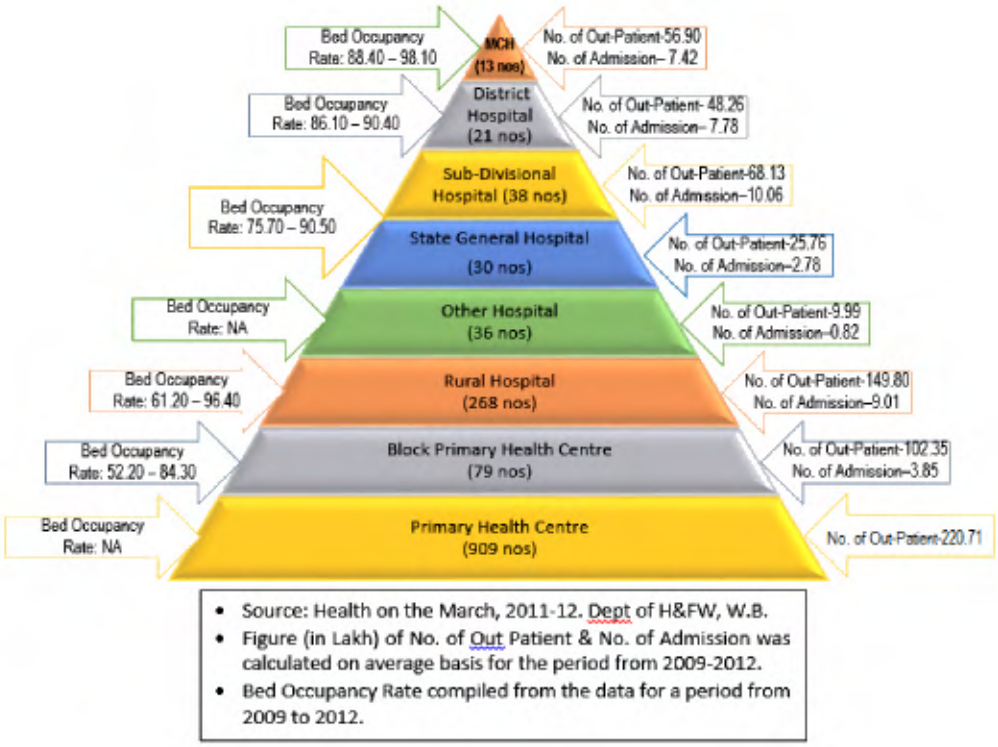
Hospital Management Information System (HMIS) aimed at managing vital patient records encompassing all the administrative and functional aspects of hospital operations. Department also intended to collate critical health related data from the hospitals through HMIS. The department introduced another application named Stores Management Information System (SMIS) for managing drugs and equipment logistics. Both HMIS and SMIS were implemented in all government hospitals down to the level of State General Hospitals. While HMIS was developed using SQL Server 2000 as backend RDBMS with Visual Basic in the front end having a client server architecture, SMIS was a web-based application using MS SQL Server 2000 in the back end and VB.net in the front end.

The IT Audit of HMIS and SMIS was conducted between April and July 2014 covering the period 2009-14 and 2011-14 respectively, which threw light on various issues of control and data integrity as well as instances of unauthorised manipulation of data.

- The desired benefits of improvement of the efficiency of delivery of health care services through introducing HMIS and SMIS remained largely unachieved as the department failed to operationalise these applications in all the intended hospitals. Even where these applications were running, all modules and sub-modules were not put to meaningful use.
- Security of the systems was compromised to a great extent owing to weak logical access controls, physical access controls and absence of password policy.
- It was also a matter of concern that privileges of system administrator were being exercised by support personnel engaged by the maintenance vendor. Lack of supervisory controls was also evident from the instances of manipulation in the system without knowledge of the hospital authorities.
- Deficient controls coupled with absence of security certificate, antivirus, audit trail and logs have rendered the system vulnerable to unauthorised intrusions. These vulnerabilities have resulted in possibility of defalcation of government revenue, as instances of unexplained short collection of revenue were observed in many occasions.
- Ability of the department in continuing its operations in the event of an interruption remains questionable in the absence of business continuity and disaster recovery plans. This issue assumed significance in view of instances of non-maintenance of data back-up.

2.5.1 Introduction

Conceptualised in 2002-03, Hospital Management Information System (HMIS) aimed at managing vital patient records and collating critical health related data from the hospitals, encompassing all the administrative and functional aspects of hospital operations. It was taken up under State Health System Development Project (SHSDP) - II with financial assistance from World Bank. In 2004-05, M/s Semaphore Computers Pvt. Ltd. was awarded the work of development and implementation of the application and it was gradually implemented in all Government Hospitals down to the level[106] of State General Hospitals (SGH) with bed strength of 100 or more. The network of hospitals and patient loads are depicted in the chart below:



The application was developed using SQL Server 2000 as backend RDBMS with Visual Basic in the front end having a client server architecture. It has four main[107] modules *viz*., Out Patient Department (OPD) Management System, In Patient Department (IPD) Management System, Charge Collection (CC) and Pay Clinic Charge Collection.

While HMIS primarily catered to patient data and collection of service charges, the Department introduced another application named Stores Management Information System (SMIS) developed by M/s PCS Technology Ltd. in April 2011, in order to manage drugs and equipment logistics. It was also to be implemented in all hospitals down to the level of State General Hospitals.

---

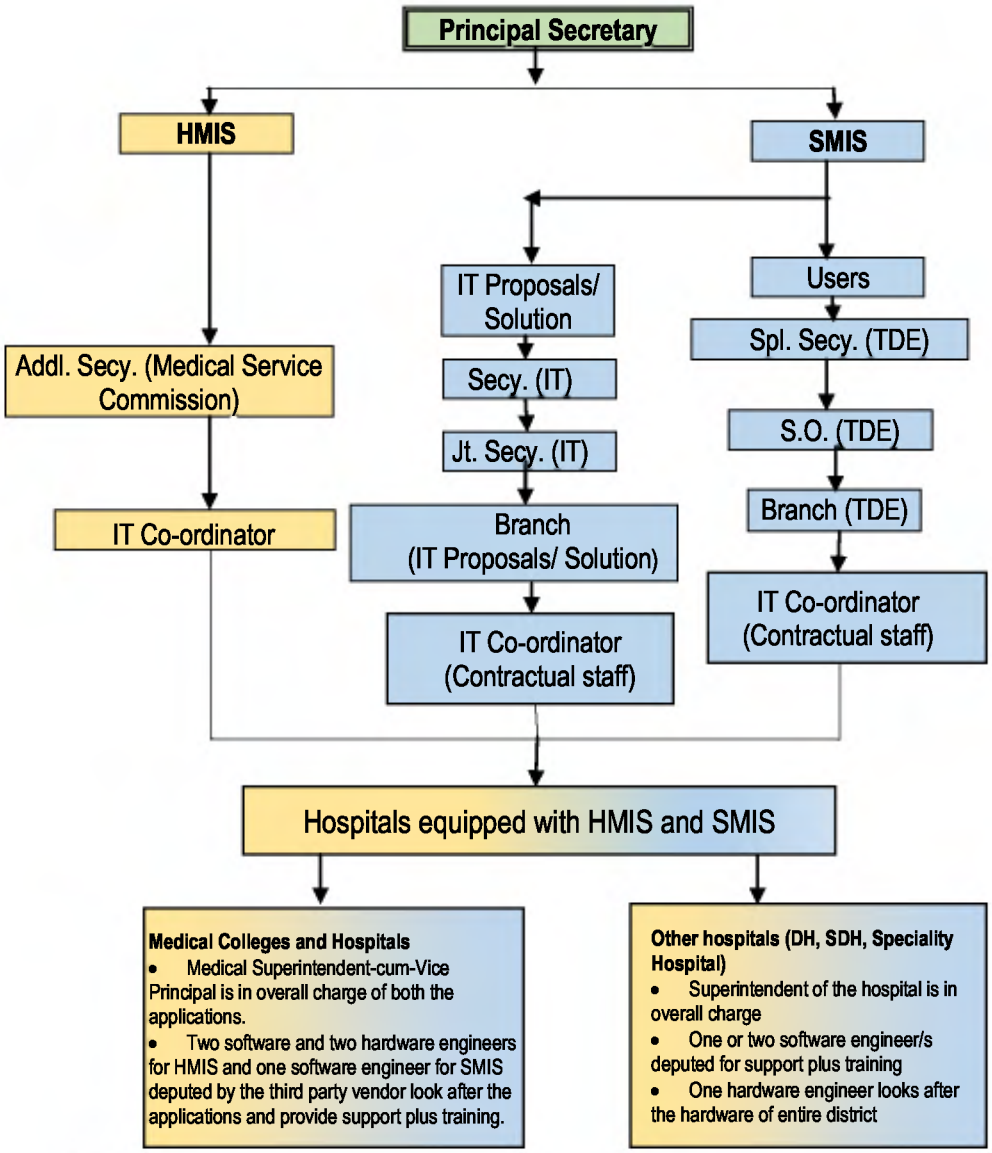
[106] *HMIS has been introduced in the levels of State General Hospitals (SGH), Sub-Divisional Hospitals (SDH), District Hospitals (DH), Medical Colleges and Hospitals (MCH), Speciality Hospitals and Super Speciality Hospitals. Levels not covered under HMIS included Block Primary Health Centres (BPHC), Primary Health Centres (PHC) and Sub-Centre (SC) being the lowest unit of healthcare system in the state*

[107] *Besides four main modules, there were two more modules namely, Blood Bank and Pay Roll, which are no longer in use owing to introduction of other applications*

SMIS, a web-based application was developed using MS SQL Server 2000 in the back end and VB.net in the front end.

2.5.2 Organisational Structure

Director of Health Services under the Health & Family Welfare (H&FW) Department looks after the overall activities relating to HMIS assisted by Joint Secretary (IT), while the Special Secretary (Transport of Drugs & Equipment) is responsible for SMIS. While the Department was unable to plan proper level of hierarchy for operating HMIS, the Departmental hierarchy for operationalisation of SMIS has been chalked out as depicted below:



2.5.3 Audit Objective

The objectives of audit were to examine and assess whether

- HMIS and SMIS have been developed properly mapping the business rules
- Implementation of HMIS and SMIS has resulted in increasing functional efficiency.

- Adequate controls are in place to ensure confidentiality, integrity and availability of data.
- Whether proper measures have been taken to ensure continuity of operations.

2.5.4 Audit criteria

The criteria for framing audit comments were sourced from:

- Rules and provisions issued by the State Government in connection with the H&FW Department from time to time,
- Instructions issued by the Government of India and Government of West Bengal regarding various health Schemes (*viz.* NRHM, RSBY etc.)
- Instructions issued and rates adopted by the H&FW Department for various services provided in the hospitals,
- Best practices for a computerised system as spelt out in COBIT[108] .

2.5.5 Audit coverage, scope and methodology

The IT Audit of HMIS and SMIS was conducted between April and July 2014 covering the period 2009-14 (except for SMIS which was introduced in April 2011) through test-check of records/ data of the department and 22 hospitals ***(Appendix 2.5.1)***selected on the basis of stratified sampling. These 22 hospitals included four Medical Colleges and Hospitals (MCH) out of 13 in the State, three major hospitals (Speciality Hospital) out of nine, seven District Hospitals (DH) out of 21 and eight Sub-Divisional Hospitals (SDH) out of 38. Data was collected from each of the seventeen hospitals where HMIS was found running in DVDs after the same were authenticated by the authorities and data back-up of SMIS was centrally collected from the department. All these data were restored in SQL Server 2008 and analysed using IDEA 9.1 software.

An entry conference was held in April 2014 with the Principal Secretary, H&FW Department and other functionaries of the department wherein audit objectives, scope, criteria and methodology were discussed.

Findings of audit, conclusions and recommendations were discussed with the Department in an Exit conference held in December 2014. The department also communicated its formal replies to audit observations in January 2015, which have been duly incorporated at appropriate places.

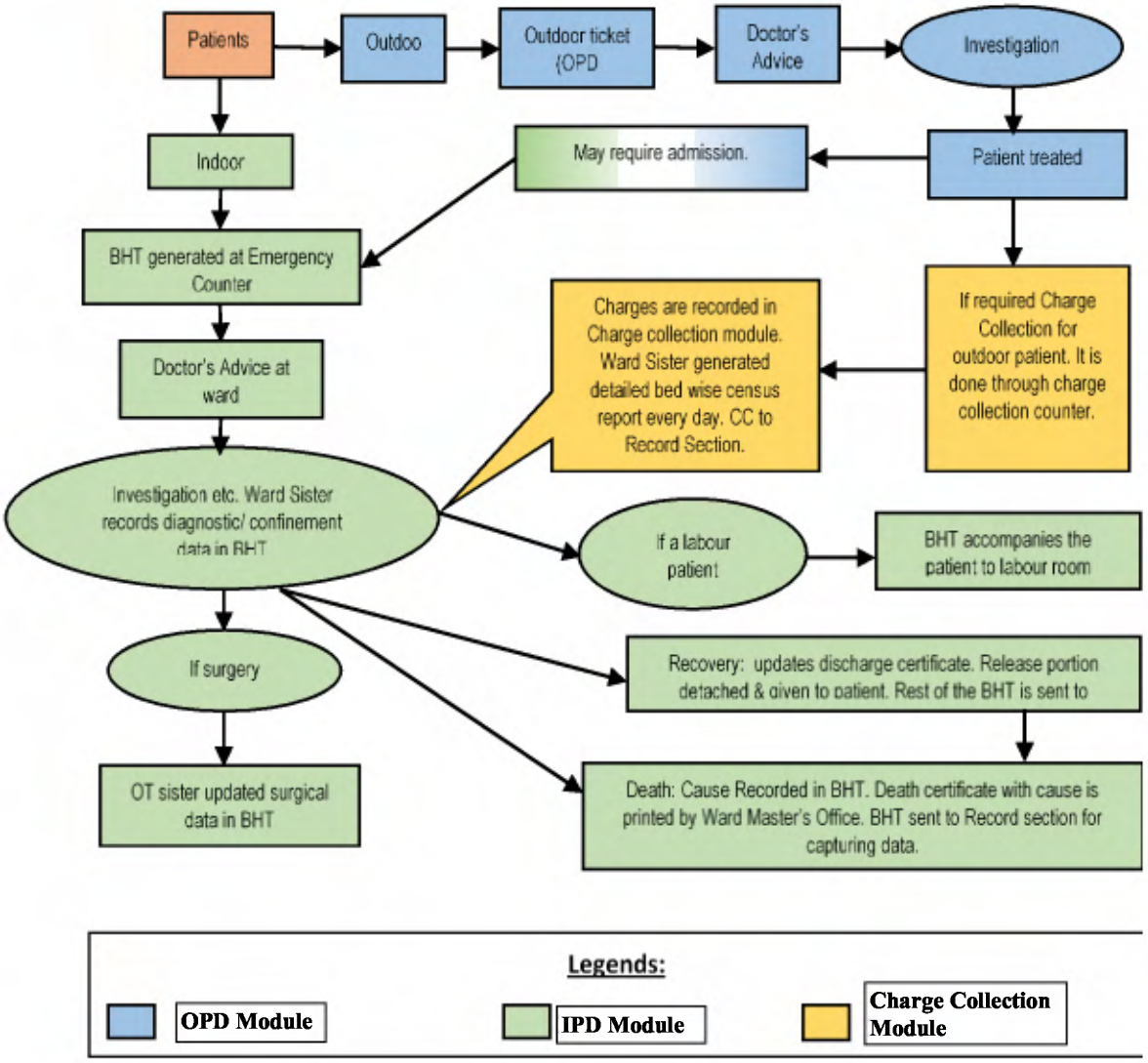
2.5.6 Process flow diagrams of HMIS and SMIS

2.5.6.1 Process flow of HMIS

As per system followed in Government hospitals, a patient gets registered for treatment by paying ₹ 2 and acquiring an OPD registration card. The doctor at OPD enters prescriptions on this OPD card. If the doctor recommends the patient to undergo any procedure/ test, the patient is directed to pay requisite charge through prescribed form to the cash collection center of the hospital. A form is also issued to the patient from the OPD which shows the type of test to

[108] *Control Objectives for Information and Related Technology (COBIT) is a framework supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks*

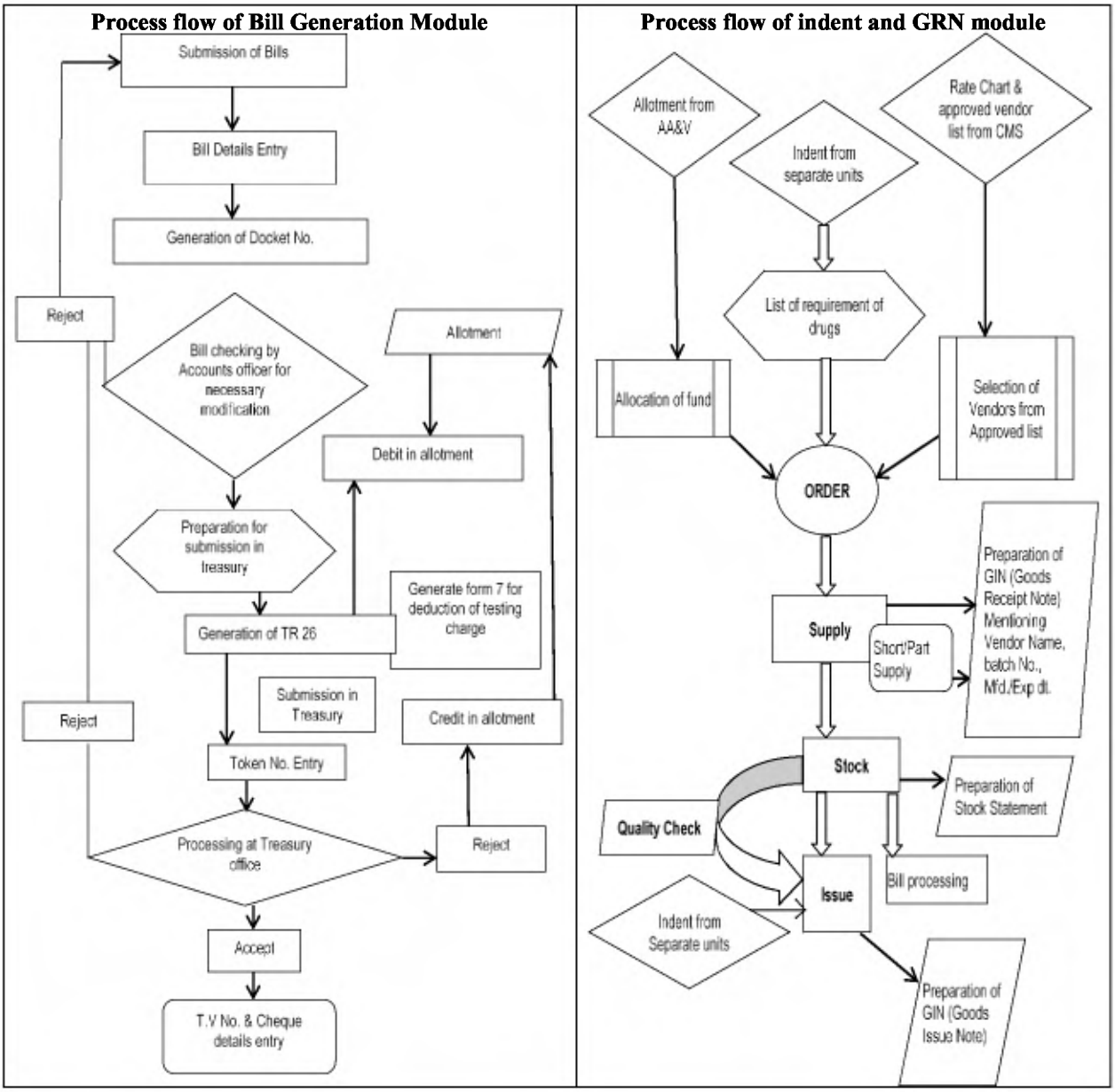
be conducted and amount to be paid apart from name and other details of the patient. On payment of requisite amount, a charge serial number is generated and a computerised money receipt is issued to the patient. In case multiple tests/ procedures are prescribed for a patient, all are booked under a single charge serial number, though multiple money receipts may be generated. Similar process of collection of charge is followed for in-patients also. The process flow diagram is depicted below:



2.5.6.2 Process flow of SMIS:

As regards SMIS, requirement of drugs, equipment and other hospital consumables (OHC) are received from various wards and departments of the hospitals in the Store. The compiled requirement of the hospital is then forwarded to the respective CMOH for allotment of funds and procurement of drugs, equipment and OHC for a particular period. Accordingly drugs (from DRS) and funds are provided to the hospital. The process flow of SMIS has been designed for indenting of requirements by respective wards and issue of the same from stores, as shown in the process flow diagram. Moreover, consumption of the issued drugs, equipment or OHC should also be entered into

the system by the end-users. The process flow is depicted in the following diagrams:



Audit Findings

2.5.7 Status of running of the systems

2.5.7.1 HMIS:

No centralised information on implementation schedule: HMIS aimed to computerise all hospital activities down to the level of State General Hospitals. However, neither was any centralised information on target date for HMIS Project development on record nor was any stage-wise schedule of implementation of the application available.

Deficient training: Though the Department had chalked out training program for its staff to operationalise HMIS, the same was not followed up

properly. The department also accepted (January 2015) that dearth of trained manpower was a factor behind under-performance of the applications.

Non-running/ partial running of the application: Absence of stage-wise implementation schedule coupled with insufficient training to the staff and non-implementation of various sub-modules had adversely affected introduction of HMIS, as would be evident from the fact that out of 22 test-checked hospitals, HMIS was not running in four[109] (18 *per cent*) though all these hospitals had bed strength of 100 or more[110]. Out of these four hospitals, in three, the application is yet to be introduced. In the remaining one hospital (Haldia SDH with bed strength of 300), though the Emergency sub-module under IPD module of the application was initially introduced in 2004-05, it was discontinued after a few months of operation.

Non-functional modules: Moreover, more than half of the total 24 sub-modules under three main modules of HMIS, *viz.* OPD, IPD and Charge collection were found to be non-functional in eleven test-checked hospitals whereas one module, namely Pay Clinic Module were seen operational in only two out of eighteen test-checked hospitals where HMIS were running (***Appendix 2.5.2***). The hospital authorities attributed (July 2014) this to shortage of hardware and skilled manpower.

Effects of non-functioning/ partial functioning of modules: As all the modules and sub-modules were not being utilised, details of the admitted patient in respect of their diagnosis, medications, diets, diagnostic tests, etc. prescribed for a patient, movement of patients from/ to different wards, discharge, death, deployment of personnel, etc. were not available in the system. As a result, the department was not in a position to get vital information like total vacancy of bed in IPD in a hospital on a particular day, total discharge/ death, bed occupancy rate, disease cycle, etc. from the system. The citizens were also deprived of benefits of vacant beds, better managed hospital services etc.

The department admitted (January 2015) that insufficiency of computer literate persons was a factor attributable to this and stated that the existing staff could not be persuaded to run the system in most hospitals.

2.5.7.2 SMIS:

Status of introduction vis-à-vis target: SMIS was to be introduced in all hospitals down to the level of SGHs. However, it was noticed that, SMIS could not be introduced in six[111] out of 22 test-checked hospitals due to absence of connectivity, non-deployment of skilled manpower and non-assignment of user id/ password.

Absence of computer terminals in wards restricting implementation: Test-check also revealed that in none of the 22 sampled hospitals could department provide computer terminals and internet connection in wards so that indenting of stores would originate from wards/ concerned departments. Consequently, in all the test-checked hospitals, indents and issues from/ to various wards and

[109] *Baruipur, Raghunathpur, Haldia and Chanchal SDHs*
[110] *Bed strength: Baruipur Hospital-160, Raghunathpur Hospital – 150 and Chanchal Hospital - 100*
[111] *Regional Institute of Ophthalmology Kolkata, Gangarampur SDH, Kalimpong SDH, Chanchal SDH, Baruipur SDH and Bolpur SDH.*

departments are entered consolidating the indents/ issues for a period of time utilising 'Issue Clearance' facility in the system so as to equate the stock balance in system with the manual store ledger.

Bill payment facility not being utilised: Moreover, in nine[112] hospitals, bill payment facility was not utilised even after 39 months of implementation of the application for reasons neither on record nor intimated when called for.

Thus, the Department was unable to implement the system fully to computerise the store operations. Only indenting from District Reserve Stores (DRS) and issue clearance were being done through SMIS by the hospitals but other modules like indenting, issuing of stores articles, maintenance of stores ledger, budgeting, requirement analysis and generation of bills through TR 26 for payment to medicine suppliers were not used by the hospitals audited.

Various issues of deficient utilisation/ non-utilisation of application modules and dilution of IT security controls giving rise to instances not only of lacunae in the data base but also cases of suspected pilferage of hospital receipts were observed in audit which are discussed in the subsequent paragraphs.

2.5.8 Non-routing of transactions through application

2.5.8.1 HMIS

Having been developed to encompass all hospital related activities in a computerised environment, HMIS necessitated entry of all data relating to patients into the system to generate reliable reports on hospital activities. Audit, however, noticed instances of transactions not being fed into the system rendering the data captured by the system unreliable.

- ***Hospital collections not routing through HMIS:*** Out of 18 test-checked hospitals (where HMIS was running), in eleven, collections of various charges were made through general money receipts without routing them through HMIS. The department attributed (January 2015) the same to absence of trained manpower, but stated that the problem would be addressed in near future by gradual increase of trained manpower.
- ***Non-capturing of data of free patients:*** In the State, certain categories of patients are eligible for treatment free of charge. Despite the system having provisions for entering this data, none of the 18 test-checked hospitals captured data on free patients in the system. The hospital authorities either expressed their ignorance of the provision or attributed non-capturing of relevant data to dearth of manpower. The department also did not give any directives to capture such data. Thus, captured data was not complete.

Irregular exemption of charges: In this connection it was seen that though no exemption of charges for various services was to be allowed to the patients unless they belonged to the BPL category, analysis of data revealed that in eight hospitals, ₹ 92.36 lakh was exempted to patients not belonging to BPL category in 46672 cases. Such cases revealed that proper validation controls were not existent in the system which has resulted in loss of hospital receipts.

[112] *BC Roy Post Graduate Institute of Paediatric Science, Regional Institute of Ophthalmology, Purulia Deben Mahato DH, Raiganj DH, Barasat DH, Asansol DH, Bolpur SDH, Arambag SDH and Haldia SDH.*

Thus, partial automation of charge collection coupled with deficient capturing of relevant data has made it difficult to vouchsafe veracity of amounts shown to have been received as hospital revenue leaving substantial scope of malpractice.

2.5.8.2 SMIS

Procurement operation by-passing SMIS: Drugs not available with the hospital stores can be procured locally. These medicines are to be entered into SMIS through Goods Received Notes (GRN) module or 'Purchase through Fair Price Shop Entry' before issuing to indenting units. The department also mandated (March 2012) the use of SMIS for procurement and distribution of drugs, equipment and other consumables, without which all procurement would be treated as suspected defalcation of Government funds. Inspite of such stipulation none of the 16 test-checked hospitals where SMIS was running, followed the same. Though the department had further stipulated (March 2012) that non-use of SMIS would invite stopping of allotment of funds to hospitals for procurement from the second quarter of Financial Year 2012-13, no such measure was resorted to. Thus, due to lack of monitoring by the Department, the application had not been running meaningfully.

Security and adequacy of controls

IT controls in a computer system represent policies and procedures that ensure the protection of the entity's assets and accuracy and reliability of its records. Access to an IT system is twofold. The first is physical access where an individual could come in physical contact with the IT assets. The other is logical access which represents access to the application/ data by individuals using user-ids and passwords.

2.5.9 Logical access controls

Necessity of password policy and hierarchical access privileges: As per the contract between the Department and the vendor, the maintenance personnel was supposed to provide only hand held support and impart training to the departmental officials in running HMIS and SMIS smoothly. Though there was clause of confidentiality[113] in the contract, the support personnel were not supposed either to enjoy independent/ unrestricted access to the applications/ data base or to create user ids without written permission from the competent authority. They should not know the passwords of various users either. This calls for clear password policy and hierarchical access privileges among the users of the system spelt out by the Department.

However, various system deficiencies like, absence of password policy, privileges of system administrator[114] with vendor personnel, inadequate access and validation controls, absence of antivirus, etc. were noticed, which jeopardised the security of the system as explained in the subsequent paras:

---

[113] *The clause inter alia stipulated*

- *All knowledge and information which are not supposed to be hosted in the public domain should be treated as confidential*
- *The information relating to the systems should be disclosed by the third party to its officials strictly in a "need-to-know" basis*

[114] *A system administrator is a user of a computer system with special privileges needed to administer and maintain the system.*

2.5.9.1 Password policy

Absence of password policy and mapping of privileges: Scrutiny revealed that the Department did not have a well documented password policy in vogue to prevent any unauthorised access to the system. Though it was expected that every user would be assigned certain level of privilege as per designation beyond which, he cannot access any part of the system, scrutiny revealed that this mapping of privilege was not well defined.

Privilege of system administrator (super-user) enjoyed by support personnel: The third party service provider was only meant to provide hand holding support and training as per the agreement with the department. It was observed that both in cases of HMIS and SMIS, the third party support personnel had complete access to the system not only with their own ids but also using hospitals' staff ids as discussed below:

HMIS: ***Outsourced agency enjoying un-restricted access in the absence of privilege policy:*** Out of 18 test-checked hospitals where HMIS was operational, in 10, the outsourced agency in charge of the maintenance had full access to the administrative password without any documented privilege policy. This assumes significance in view of several instances observed by audit where the system was deliberately modified leading to pilferage of hospital receipts.

Instances of duplicate user id and ghost user id: Analysis of data revealed that in the aforesaid eight hospitals there existed 21 duplicate user id (varying from two to five user id) against one user and in eight[115] cases, there existed ghost user id (no user id assigned but the user entered into the system for data entry/update). The system also allowed the character of space as user id (which should, ideally be of minimum eight characters) due to lack of validation control.

SMIS: ***No departmental directive on confidentiality of passwords:*** Under SMIS, all store purchase related activities like placing of order, receipt of items, generation of bill, quality checking etc. are to be processed through the system, necessitating several levels of administrative involvement/ check, including confidentiality of every user's password. The department had also not issued any directive in this regard.

Vulnerability of the system from weak user access control: Due to inadequate privilege mapping, it was observed that a Store keeper who was in charge of equipment in any hospital could execute the function of the Store keeper in charge of drugs through the system. This made the system vulnerable to misuse or manipulation. Thus, the system lacked user access control.

Non-encryption of passwords of hospital officials: Scrutiny of data revealed that out of total 2394 users created for using SMIS, as many as 934 users had not accessed their account. Moreover, data analysis revealed that the passwords of the users of the private vendors who developed and are maintaining the application were encrypted but those

[115] *Seth Sukhlal Karnani Memorial MCH, Calcutta MCH, Darjeeling DH, Hooghly DH, Raiganj DH, Lady Dufferin Victoria Hospital, Barasat DH and RIO.*

of the departmental staff were not encrypted thus making the application extremely vulnerable to external unauthorised access due to use of selective encryption. It was also noticed that, the entire application was hacked in March 2013 and the department had to temporarily shut the application for three days. Thus lack of access control policy rendered the application extremely vulnerable to external threat of hacking.

Thus, privilege of super-user is being enjoyed by the personnel of the firm maintaining the hardware/ software. They can enter, modify, commit and save any data compromising the data integrity.

The department, in its reply, stated (January 2015) that it had since implemented an interim password policy for modified on-line HMIS. It was further intimated that a more streamlined password policy with multi-level checks was being developed. Regarding undue privilege enjoyed by the support personnel, the department stated that administrative passwords were handed over to the support personnel as administrative heads did not find time to handle the system and there was no regular hospital employee who could be made accountable and available round the clock.

2.5.9.2 Impact of deficient controls in logical access

Generation of registration number: Patient Registration Number was a system generated number assigned to each patient entering in a hospital for any kind of treatment in OPD or IPD. A patient can be tracked in the system through this number. The number is unique in nature and any gap in the serial number might have indicated loophole in the system. For OPD purpose, a patient needed to deposit ₹ 2 irrespective of their status of being BPL or not and a system generated blank prescription with OPD number and Registration number was printed and handed over to each patient. In case of emergency/ IPD admission, a system generated Bed–head ticket was generated before admitting the patient.

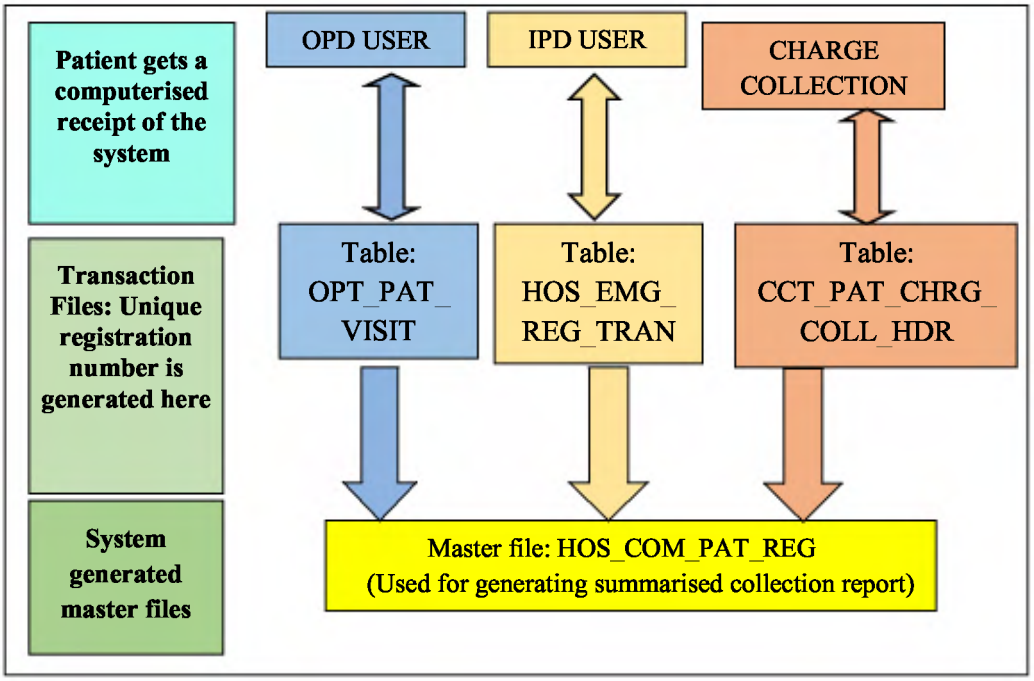
- ***Duplication of registration numbers:*** However, analysis of data relating to IPD and OPD module revealed that in 18 hospitals, in 74215 cases, same Registration number were issued to different OPD patients indicating not only flaws in database design but also possibility of pilferage of hospital receipts.
- ***Multiple registration numbers generated against a single patient:*** In North Bengal MCH, there existed more than one registration number against a particular patient on a particular day for collection of hospital charges viz. x-ray charges, OT charges etc. Analysis of the data revealed instances of multiple registration numbers being generated against a single patient on a single day indicating flaw in the database designing. Data analysis showed 76273 registration numbers so generated against 31749 patients with two to nine registration numbers against each of them. Possibility of intentional tampering of the database by accessing administrative password could not be ruled out.
- ***Stop-gap arrangement of server without knowledge of system administrator:*** In North Bengal MCH, on comparing the HMIS data for the period from June to August 2013 with relevant manual documents *viz*., cash book, IPD patient registers, departmental registers etc., it was seen that there

was no data in the server for the period from 18June 2013 to 16July 2013. It transpired that due to faults in the server during the period, the third party support personnel ran HMIS through a stop-gap server by temporarily configuring another PC as a server. However, no data back-up was taken during the temporary arrangement. The MSVP expressed ignorance of the fact. This also pointed to the fact that a very sensitive function like revenue collection was being managed without the supervision of the MSVP. Given the fact that as compared to revenue collected in August 2013 fully through HMIS module, collection figures of June 2013 (manual collection for 11 days) and July 2013 (manual collection for 14 days) fell short by 39 *per cent* and 63 *per cent* respectively, absence of back up data assumed seriousness. Scrutiny further revealed similar instances in NBMCH when system remained shut down in seven different spells ranging from 15 days to 151 days.

- ***Numeric gaps in registration numbers indicating manipulation in master table by support personnel:*** Scrutiny of data of Bolpur SDH pertaining to 69 working days from 2 May 2014 to 21 July 2014 revealed that on ten days, there were numeric gaps varying from one to 602 in patient registration number. Further enquiry revealed that when the system was down, the hospital switched over to manual OPD tickets. In order to keep continuity in numbers, the third party support personnel edited the master tables from the backend by increasing the OPD ticket serial number. This was, however, done without the knowledge of the hospital Superintendent indicating violation of logical access control to the data table.

2.5.9.3 Process of entry and storage of patient data

HMIS was designed to record all patient activities inside hospitals. The process flow diagram of entry and storage of patient data is depicted below:



Registration number is generated by the system either from OPD module or from IPD (Emergency) module or from Charge collection module (when a patient is issued manual OPD ticket due to system failure and then proceed for

any service at Charge collection counter). Data thus entered into the system is automatically stored in one of the three transaction tables[116] attached to these modules. All these data finally get stored in a Master file. Thus, total number of registration numbers generated in the aforesaid three transaction tables must reconcile with that stored in the master file.

At the end of the transaction hours, each user generates a summarised collection report from the system using master table and deposits the amount in Cash Section.

Mismatch between transaction tables and master tables: Analysis of the aforesaid four tables in respect of 17 test-checked hospitals (excepting Bishnupur SDH, where the charge collection module has been discontinued) revealed that

- There was no mismatch of records of the tables in respect of Kalimpong SDH and Gangarampur SDH;
- In the remaining fifteen hospitals, master table contained 77263 less number of registration numbers as compared to those recorded in the transaction files. Number of such registration numbers missing from the master file in each hospital ranged from five (in Bolpur SDH) to 69103 (NBMCH).

Such mismatch in records is indicative of possibilities like

- Either the data was wilfully deleted from the master table or
- the master table was temporarily delinked from the transaction tables

2.5.9.4 Possibility of pilferage of revenue through missing registration numbers

Given the fact that the missing registration numbers accounted for total revenue of ₹ 92.92 lakh and there was no supervisory check on collection amount deposited to the cashier, the matter assumes seriousness. This may further be viewed with the fact that in absence of any logical access control policy for access to the data table, the administrative privilege was being enjoyed by the lower level of maintenance personnel deputed by the third party maintenance agency.

Though this *prima facie* indicated unauthorised access to the system, the Superintendents were unable to explain the reason for users accessing the system beyond hospital hours. They attributed the same to system failure.

The reply was not tenable as it evidenced lack of physical access control in the system and might even point to attempts for unauthorised and intentional entry in the backend software. Further, instances of non-logging out indicated that access security was compromised exposing it to the risk of unauthorised access.

[116] *Table names being OPT_PAT_VISIT for OPD or HOS_EMG_REG_TRAN for IPD and CCT_PAT_CHRG_COLL_HDR for Charge Collection*

2.5.10 Supervisory control

Audit came across several instances pointing to deficient supervisory controls which could potentially affect the reliability of the data being captured and maintained in the system. These have been indicated below:

2.5.10.1 Control over refund of hospital charges: In hospitals where HMIS was running, any refund to be made to a patient should also be done through the system. Normally, patients, who had earlier been referred for some clinical investigation or operation and later advised not to do the same, would be allowed the refund in full provided they claimed the refund with copy of the advice after approval of higher authority in the hospital. Since refund of government money is sensitive in nature, proper checking should have been in place to validate and authenticate such refund. It was, however, seen that different hospitals followed different system of refunds. While in 13 hospitals, refunds were recorded both in manual and electronic records, in five, refund was found to be done manually only and no records of such refund were entered in the application.

2.5.10.2 Irregular handling of refund cases: In one hospital (Kalimpong SDH), it was observed that refunds were made by taking back the system generated charge collection receipts from patients and the same charge collection receipts were re-issued to other patients having advice for same clinical test just by changing the name on the receipt without any approval of the hospital authority. Thus, part of the collection was not being captured in the system. Moreover, there was a high chance of defalcation as these refunds are not getting reflected anywhere.

2.5.10.3 Control over printing of receipts: As charge collection receipts represent revenue, adequate controls are essential to ensure that duplicate receipts are not issued and resultant leakage of government revenue is avoided. Thus, the system should have ample control over the printing of receipts, serialising the receipts by generating system number and number of copies be restricted to one only at user level. Accordingly, system should have generated and printed only one copy of receipt against any charge collection.

In HMIS, however, any number of copies of receipts can be printed against a given charge collection.

2.5.10.4 Misutilisation of pre-printed receipts: Taking advantage of this lacuna, in one test-checked hospital (SSKM MCH), charges were collected manually against this pre-printed receipt without routing the collection through the system indicating chances of defalcation of government revenue. This came to notice of the hospital authorities in February 2012 consequent upon a complaint received from one patient. It was found that receipt issued against one patient was re-issued against the complainant after manually deleting the patient's name and adding the latter's name. Analysis of database design showed that the application was designed to restrict print of receipts to a pre-defined number but since the same was not mapped properly in the application, the same could not be applied in this case.

Thus, there was vulnerability to government receipts taking advantage of the loop hole in the system.

2.5.10.5 Control over amounts deposited to Cashier: Hospital revenue collected from various points of collection in the hospital is to be deposited to the Cash section at the end of the day for entry in cash book and further remittance to government account. In support of the amount of collection, the collecting personnel have to produce a system generated collection summary while depositing the amount to the cash section. The cashier should have another set of system generated MIS report of daily collection statement which should match that deposited by the users. Any mismatch in these two system generated report should be reported to and checked by authority to do away with possibility of fraud.

2.5.10.6 Systemic observations on deposit of collection to cashiers in test-checked hospitals: This aspect was put to audit verification in three medical colleges and hospitals (namely Calcutta National Medical College & Hospital, NRS Medical College & Hospital and North Bengal Medical College & Hospital) in Kolkata, apart from the test-checked ones and the following was observed

- ***Inherent system deficiency in deposit of collection:*** At the end of each day's transactions, the cash collecting officials deposit the collected cash to the cashier alongwith a computer generated user-wise and date-wise collection summary. The collection summary[117] does not contain the details of procedure for which charge was collected. The cashier enters the amount as per the collection summary in cashbook and remits it to Government account without any cross-checking from the system.
- ***Absence of cross-checking of amounts deposited:*** In the remaining test-checked hospitals, there was no system of cross checking the amount collected and the amount deposited by the various collection point users as there was no terminal of HMIS available with either the Accounts Officer or the Assistant Superintendent or the Cashier. Therefore, there was no compensatory control and this left the system vulnerable to revenue leakage. The authorities were not fully cognizant of such discrepancies. This pointed to lack of supervisory control over revenue collection.

2.5.10.7 Instances of manipulation of database facilitated by the control weaknesses

The systems of collection of revenue, issue of receipts and depositing of the receipts with cashiers in respect of some high value procedures/ tests[118] in two medical colleges and hospitals (namely Calcutta National Medical College &Hospital and NRS Medical College) were subjected to audit verification which threw light on various control weaknesses, lack of transparency as follows:

---

[117] *Collection summary contains patient referring point (OPD/ IPD), collection bill number, patient ID, patient serial number, name, amounts received/ refunded etc.*

[118] *Calcutta National MC&H: Extra Corporal Shock Wave Lithotripsy (ESWL) (₹6000 per test) done in Urology Department; NRS MC&H: ESWL (₹6000 per test) and Urodynamic study test (₹500) done in the Urology Department; Percutaneous Transluminal Coronary Angioplasty* (PTCA) (₹ *2000 per test) and Balloon Mitral Valvuloplasty (BMV) (₹1000 per test) both carried out at Cardiology Department; North Bengal MC&H: CT Thorax(₹1500 per test) and CT Scan (₹800 per test) done in CT Scan Department.*

- ***Manipulation of data leading to under recovery of government revenue:*** There were discrepancies in amount to be collected and amount actually shown as collected indicating short collection of revenue and possible manipulation of data:

Table 2.5.1: Instances of mismatch between HMIS database and records of hospital departments

Name of the hospital	Name of test	Period	Number of test conducted				Number of tests not traceable in database	Short collection of revenue
			as per concerned department	Amount to be collected	Collection database of HMIS	Amount actually collected		
Calcutta National MCH	ESWL@ 6000 per test done by Urology Department	January 2007 and September 2013	1708	₹ 102.48 lakh	920	₹ 55.15 lakh	788	47.28 lakh
NRS MCH		October 2011 onwards	62	₹ 6.32 lakh @ ₹ 6000 per test	62	₹ 3.42 lakh	--	₹ 0.30 lakh[119]
	PTCA (₹ 2000 per test) done by Cardiology	January 2012 and September 2013	605	₹ 12.10 lakh	584	₹ 11.68 lakh	21	₹ 0.42 lakh
	BMV (₹ 1000 per test) done by Cardiology		78	₹ 0.78 lakh	64	₹ 0.64lakh	14	₹ 0.14 lakh

Source: records of respective hospitals

- ***Tampering of master database deleting data:*** Data analysis further revealed that, master databases were tampered in Calcutta National MCH by deleting records relating to charge collection from patients as evident from the fact that records of 3485 cases of charge collection were untraceable in user login details master table.
- ***Mismatch of charge collection data:*** Analysis of data of CN MCH also revealed that in 38 cases during the period as stated above, amount paid as per charge collection master table differed from the amount paid as per user login details master table.

2.5.10.8 Control over creation of user id-s

- ***Multiple user id-s against single user*** In eight test-checked hospitals[120] there existed more than one username against each user under HMIS. This was attributed to a loophole in the software which did not permit the user to login again on the same calendar day if the computer gets shut down before the user could log out. Consequently, if the computer gets turned off due to reasons like power failure, users were provided with new user ids by the third party support personnel without the permission of the higher authority. Authorities were not fully cognizant about this problem.

[119] *In five cases of ESWL, against ₹30000 receivable, only ₹70 were deposited in account resulting in short deposit of ₹29930.*

[120] *Seth Sukhlal Karnani Memorial MCH, Calcutta National MCH, Asansol DH, Darjeeling DH, Hooghly DH, Raiganj DH, Purulia DH and B.C. Roy Hospital.*

2.5.11 Physical Access Control

2.5.11.1 Access to the system beyond working hours

In hospitals, OPD services are available from 9.00 AM to 2.00 PM. Accordingly, the OPD module of HMIS should have remained operational during this period only. However, in all test-checked hospitals analysis of data for the period from June to August 2013 revealed that there were numerous instances of system being logged-in/ logged-out before/ beyond functional hours of OPD. Analysis of data revealed that in around ten *per cent* of total user login cases, there was no logout time captured in the database.

2.5.11.2 Access to server and client PCs

No restrictions on external memory: Audit observed that the department had not framed any policy for by its staff or the third party service providers to restrict access to servers and client PCs by pen drive, HDD, external drive etc.

USB ports not deactivated exposing the system to risks: Test-check showed that the USB ports of servers and clients in any test-checked hospitals were not blocked. Consequently possibility of obtaining unauthorised and sensitive data or attack of malware through USB drives and other external devices cannot be ruled out.

Hard disk removed without knowledge of system administrator: In Arambagh SDH, the hard disk of the computer server crashed in November 2013. It transpired that the hardware engineer of the third party firm had taken out the hard disk for data retrieval without the knowledge of Superintendent. This indicated that the third party personnel worked on their own volition without seeking necessary permission from the Superintendent, who was the system administrator. This compromised security of the system.

The department stated (January 2015) that physical access to and control over data base would be withdrawn from the support staff as soon as on-line HMIS is implemented.

2.5.12 Application control

2.5.12.1 Deliberate entry of wrong data to circumvent application deficiency: Instances were noticed where data integrity of SMIS was sacrificed to circumvent the application deficiencies which in turn compromised effective management of stores.

2.5.12.2 Entry of medicines with incorrect expiry dates/ batch numbers

- There existed no validation rule in the SMIS for entering the shelf life of a medicine purchased through the application. As a result, in 20 cases, expiry dates of medicine/ equipment preceded the respective manufacturing dates. In eight cases, the manufacturing dates and expiry dates were same.
- On the other hand, in case of 260 medicines, it was observed that the shelf life was shown to be more than 100 years.
- Moreover, items not having batch number[121] could not be entered into the system though the application had provisions for entry of these items.

[121] *viz. Jute Swab, Cotton Swab , Bed Sheet, Draw Sheet etc.*

Consequently, these items were taken into the system by giving a junk batch number or by numerically entering zero.

Thus, due to faulty logic embedded into the system designing left the application less dependable when it came to the shelf-life of medicines.

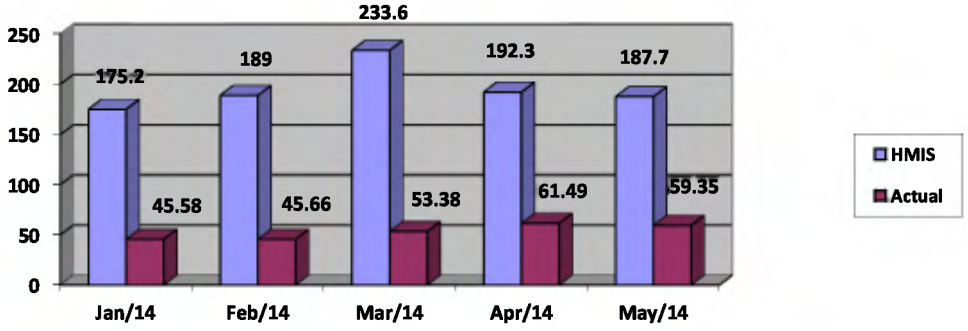
The department stated (January 2015) that the issue has already been resolved by separating Good receipt Notes (GRN) of drugs and equipment.

2.5.12.3 Faulty calculation by the system: The application had a system of Goods receipts notes (GRN) where the hospital authorities were supposed to enter all data relating to the procured medicines/ equipment including their rate and quantity. There was also a column for calculating the total price of the medicines/ equipment. It was designed in that manner to initiate bills for payment to the suppliers. It was observed that in 108 cases, the system calculated the price of medicine/ equipment in excess of payable amount by ₹ 1622740. On the other hand, in 172 cases the system erroneously undercalculated amounts payable by ₹ 39453965.

2.5.13 Validation control

2.5.13.1 HMIS: The department is dependent on HMIS for calculation total out patients, total emergency admission, bed occupancy rate, etc. for incorporation in annual health report of the department which were extremely important for policy making of the health department. So there should be proper controls in place to ensure completeness and authenticity of the data captured. As data on hospital activities captured in the system were not complete (as already discussed), authenticity of reports generated using HMIS database was doubtful. Moreover, instance of system generating irrational figures was noticed.

Chart 7: Comparison of actual Bed Occupancy Rates with those generated by HMIS



Irrational data being generated by HMIS: In Kalimpong SDH, admission rate[122] calculated by the system (IPD module) ranged from 175 to 234 *per cent* during January 2014 to May 2014 though bed occupancy rate[123] during the same period was between 46 *per cent* and 62 *per cent* as shown in **Chart 7**.

[122] *Emergency admission rate = (Total number of patients admitted in the hospital from emergency during the month*100)/ (Number of patients attending emergency)*

[123] *Bed occupancy rate = (Total number of patient days in the hospital during the month*100)/ (Bed strength * number of days in the month)*

2.5.13.2 SMIS: Audit observed that SMIS was deficient in validation controls as would be clear from the following instances.

Incorrect balance position generated by the system: In National MCH and Asansol DH, discrepancies between closing balance and opening balance were observed. In National MCH, in case of 49 drugs, the opening balance of 1 April 2014 differed from actual stock. In 39 cases, the opening balance as on 1st April 2014 in the system was more than the closing balance in hand though no drugs were received and entered into the system during this period and in nine cases, there was decrease in the opening balance. In Asansol DH, stock of 39 items of drugs, the opening balance was more and in six cases, the stock was less. Thus, the stock position as indicated by the system was incorrect thereby indicating inadequate processing control.

SMIS was designed to make procurement of drugs only if there is adequate allotment of funds. The funds are allotted by the department and entry to this effect is also made from the department. When orders are placed for procurement by the hospitals, the value of orders gets deducted from the available balance. Once the funds are exhausted, the hospitals would not be allowed to make any further procurement. Scrutiny revealed that in Darjeeling DH, the system was unable to deduct the expenditures correctly when hospital made purchases.

Incorrect calculation of allotment position by SMIS: Analysis of transactions for the period from June 2013 to October 2013 revealed ten instances of incorrect deduction where the system wrongly calculated the available allotment after deducting order value from the total allotment as detailed in ***Appendix 2.5.3***.

It was also observed in one case that the system wrongly calculated not only the available balance but also the order value. The order value as calculated by the system did not match with the manual records. In place of order value of ₹ 23.40 lakh, system was showing ₹ 95.39 lakh.

It transpires that either the program language was wrongly designed to calculate available balance after deducting the order placed or the administrative privilege was tampered with to make intentional modification leaving scope for placing excess order.

Department stated (January 2015) that in the upcoming version of the HMIS, the validation control deficiencies would be rectified, while those of SMIS were being addressed

2.5.14 Other security issues

2.5.14.1 SMIS operating without security certificate

For security through use of encryption, any website needs to obtain a certificate from a trusted organisation. This will ensure that the site is protected against attackers who create malicious sites to gather information. It was seen that the website of SMIS lacked such security certificate. Absence of security certificate left the system, extremely vulnerable to hackers and malware attacks. Besides, whenever an attempt was made to enter the webpage, it showed a warning message stating that the page was potentially harmful to open.

Department stated that initiatives have been taken to get the SMIS application audited through third party security audit.

Operationalisation of the system without mandatory testing: oreover, the Department did not test the application with the Standardisation Testing and Quality Certification (STQC) of Department of Electronics and Information Technology (DEIT)[124] which was mandatory for any e-governance programme developed by Government agencies before making the application operational. Thus, not only did the system lack proper validation rules but also the Department failed to conform to extant rules of Government in introducing new software.

2.5.14.2 Lack of Antivirus

HMIS was developed to be operated in a LAN environment whereas SMIS was developed in a web-based platform. In order to safeguard the data relating to the application, the department should have chalked out very strong and secure antivirus policy. Moreover, there should have been proper firewall installed in all PCs used for operating SMIS and restrictions should have been in place on access to internet through earmarked computers. There should have existed well defined policy to restrict use of external storage devices. However, it was found during audit that the department had not issued such directives nor had it chalked out any security policy for safeguarding the data. In 11 hospitals out of 18 test-checked, there was no antivirus. Thus, due to absence of proper antivirus and system security policies, the entire system of SMIS and HMIS was vulnerable to unwanted intrusion and even loss of data.

2.5.14.3 Absence of audit trail and log

Audit trail is the evidence that demonstrates how a specific transaction was initiated, processed and summarised. Similarly, log files are used to record the actions of users and hence provide the system administrators and organisation management with a form of accountability. A system log can record who logged onto the system and what applications, data files or utilities they used whilst logged on. Thus, these facilities will aid the management to keep track of unauthorised access and amendment made in the system. It was seen that audit trail was available neither in HMIS nor in SMIS. Though log files were there in both the applications, those were not checked by the system administrators in cases of HMIS and log file relating to SMIS was wrongly designed without any column to capture log-out time thus compromising the security of the system.

2.5.14.4 Non-employability of the system for departmental oversight

One of the major objectives of HMIS was to collate and use hospital data for planning and monitoring of health care services. However, as the system was found running in individual hospitals through LAN without any system to feed data in a central server on a regular basis (either real time or periodically), it was not possible to monitor the activities centrally from the Department. Consequently, the department had to rely on manual reports sent from the

[124] *In order to provide state-of-the-art technology based quality assurance services to its valuable clients and to align with DEIT mandate-to focus on IT and e-governance sector, STQC is providing quality assurance and conformity assessment services in IT and e-Governance Sector since 1999. STQC supports Government of India's National e-Governance Plan (NeGP) for overall growth of e-governance within the country. STQC has developed e-Governance Conformity assessment and Quality Assurance framework.*

hospitals. Though the Department had earlier envisaged that the reports generated from the system would be utilised to take several management decisions including access of same data by the citizen like live status of vacant bed in any hospital, the same could not be achieved by the Department.

In contrast, SMIS was working through a central server located at the Departmental headquarters.

Department stated (January 2015) that the issue would be addressed in the online HMIS.

2.5.14.5 Competence of personnel

Though one software support personnel from the maintenance agency was posted at each hospital having functional SMIS and HMIS, it was observed that these personnel attached with test-checked hospitals had no operational knowledge of SMIS/ HMIS (in case of four[125] hospitals) or had been imparted with inadequate training (Haldia SDH) or no training (Asansol DH) in SMIS.

It is thus evident that there is a need for the department to be more vigilant on the quality of software support personnel posted by the support agency.

2.5.15 Business continuity

Business Continuity and Disaster Recovery Plan aims to ensure that an organisation is able to accomplish its mission and is able to process, retrieve and protect information maintained in the event of an interruption or disaster leading to temporary or permanent loss of computer facilities. This calls for well documented, tested and updated continuity and disaster recovery plans, regular back-up of systems software, financial applications and underlying data, etc. However, deficiencies in these areas were noticed in audit as discussed below.

2.5.15.1 Absence of Business Continuity and Disaster Recovery Plans

The department did not have any business continuity and recovery plan. As such capability of the department to resume its operations after an event of an interruption was doubtful.

Irregular data back-up in absence of policy: The department had not chalked out any well-defined back-up policy for HMIS. The back-up was found to have been taken in irregular intervals at the whim of the third party supporting staff. In test-checked hospitals, it was found that back-up of HMIS was taken in an interval varying from two days to five months while in Kalimpong Hospital, no data back-up was taken as third party support personnel did not know how to take a back-up in SQL Server. The last back up was taken in Kalimpong Hospital in September 2011.

Reduction of revenue not investigated in absence of data back up: Absence of data back-up assumed further seriousness from the instance of North Bengal MCH (*as already discussed in para 2.5.9.2)*, where another PC had to be configured as a temporary server due to occurrence of fault in the existing server. Substantial fall in collection of revenue during that period could not be sufficiently investigated into in the absence of data back-up during the

[125] *Personnel attached with Bishnupur, Haldia and Arambagh SDHs had no operational knowledge of both HMIS/ SMIS while the one posted to Asansol DH lacked operational knowledge of SMIS.*

temporary arrangement coupled with ignorance of the MSVP of the whole event.

Department, while admitting (January 2015) that the Disaster Recovery Plan could not be successfully implemented over distributed data base; stated that this would be automatically addressed once online centrally hosted HMIS is introduced. Regarding absence of data back-up it has been intimated that the Deputy Project Managers have been entrusted with administrative jobs and a Standard Operating Procedure is being prepared to bring uniformity across the state.

2.5.15.2 Non-utilisation of computer infrastructure in wards

With the introduction of HMIS, 19 out of the 22 test-checked hospitals were provided with LAN connectivity in OPD ticket counters, charge collection counters, Emergency admission points, all departments and wards. The respective staff was to capture data through these nodes. It was observed that in none of the 19 test-checked hospitals did such connectivity exist at the time of visit of the IT Audit team. Audit came across instances where the hubs, switches, UPSs, PCs, printers were found abandoned in a dilapidated condition. The hospital authorities agreed to the fact that the process of recording all information relating to HMIS in various departments, Wards and stores had not been done. This indicated that even after putting the infrastructure in place, continuity of operations was not ensured by the hospitals.

PC earmarked for running HMIS (May 2014) and switches and hubs (June 2014) were lying in dilapidated condition in North Bengal MCH

The department attributed (January 2015) the same to acute shortage of computer literate manpower at various levels of hospitals and added that initiatives have recently been taken to provide adequate computer literate manpower and impart functional computer training.

2.5.16 Conclusions

Thus, the desired benefits of improvement of the efficiency of delivery of health care services through introducing HMIS and SMIS remained largely unachieved as the department failed to operationalise these applications in all the intended hospitals. Even where these applications were running, all modules and sub-modules were not put to meaningful use. Instances of transactions not being captured in the system or wrong data being fed into the system to circumvent deficiencies have led to compromise in completeness and reliability of the database. The department could not do away with its dependence on manual data for monitoring, as HMIS was not a centralised system.

Security of the systems was compromised to a great extent owing to weak logical access controls, physical access controls and absence of password

policy. Lack of supervisory controls was also evident from the instances of manipulation in the system without knowledge of the hospital authorities. It was also a matter of concern that privilege of Super-User was being enjoyed by support personnel engaged by the maintenance vendor. Such deficient controls coupled with absence of security certificate, antivirus, audit trail and logs have rendered the system vulnerable to unauthorised intrusions. These vulnerabilities have resulted in possibility of defalcation of government revenue, as instances of unexplained short collection of revenue were observed in many occasions.

Ability of the department in continuing its operations in the event of an interruption remains questionable not only in the absence of business continuity and disaster recovery plans, but also in view of instances of non-maintenance of regular data back-up.

2.5.17 Recommendations

Audit recommends for consideration that

- ***The department switch over to a web-based platform integrating both HMIS and SMIS for better management, proper monitoring and overall control over the entire system.***
- ***The department ensure that all the modules in the applications are optimally utilised so that all hospital activities are computerised for efficient delivery of health care.***
- ***Comprehensive password mechanism with well-defined privilege policy be introduced immediately to ensure that the system captures and maintains complete and reliable data and to do away with possibilities of unauthorised manipulations in the system.***
- ***The department revamp the IT infrastructure in hospitals as well as formulate proper training programme in a planned and time bound manner to existing manpower for successful operation of HMIS and SMIS.***
- ***The department formulate a business continuity and disaster recovery plan and ensure its strict compliance so that it can smoothly resume its operations in the event of any interruption.***

During exit conference (December 2014), the Principal Secretary of the department, while accepting all the findings and comments of audit, assured to look into the matters and comply with the recommendations.