



西安交通大学第一附属医院

THE FIRST AFFILIATED HOSPITAL OF XI'AN JIAOTONG UNIVERSITY

从医疗数据生态的角度看医疗数据安全

网络信息部 蔡宏伟



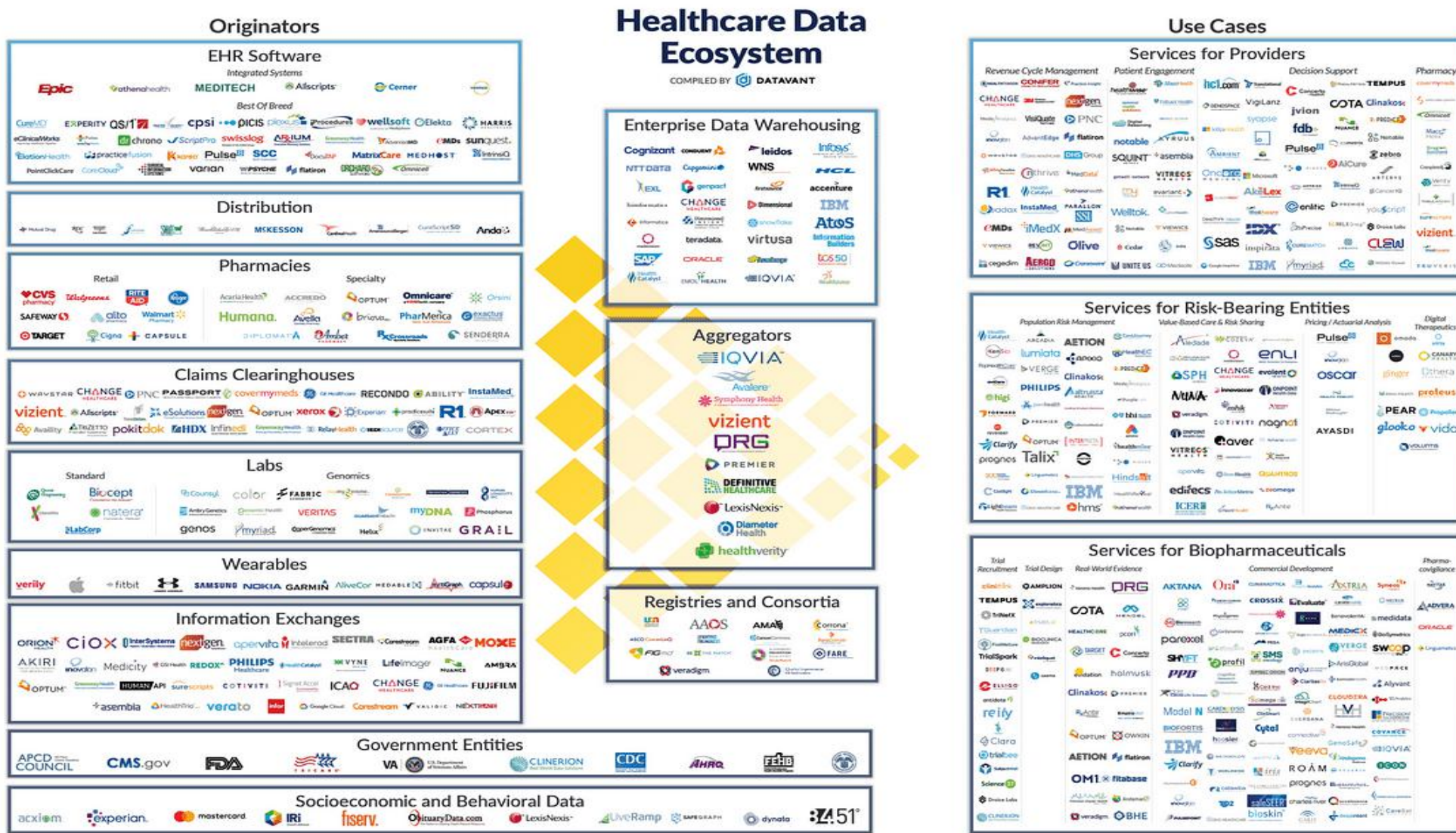
01 医疗健康数据生态体系

02 组织内的数据安全管控

03 组织间的数据安全管控

04 总结

一、医疗健康数据生态体系



医疗数据生态体系中的实体以及数据

1. 医院信息系统数据

2. 供应链管理数据

3. 药品销售数据

4. 医保数据

5. 检查、检验数据

6. 可穿戴设备监测数据

7. 健康注册数据

8. 医疗机构

9. 生物医药公司

10. 医疗器械生产厂商

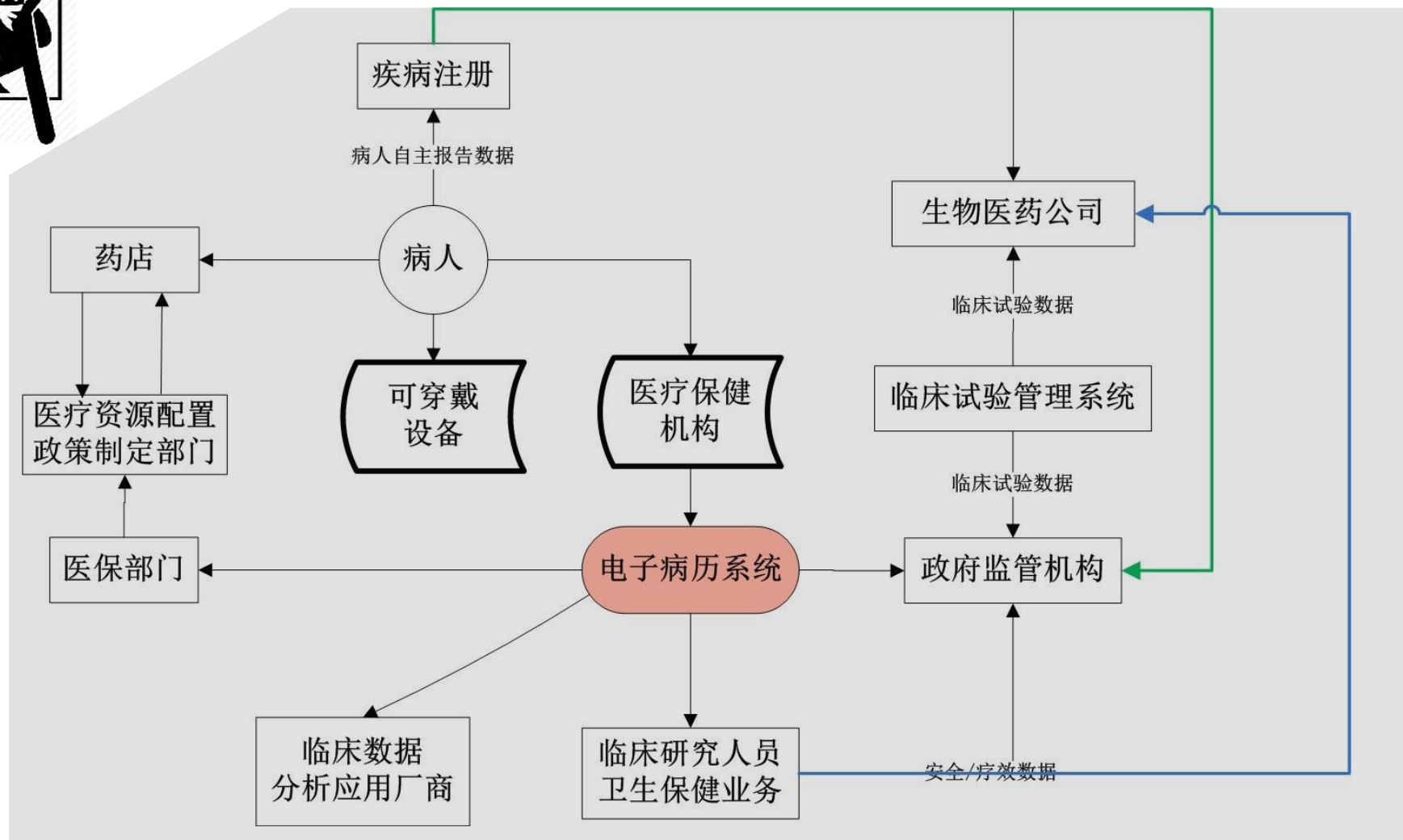
11. 医院信息系统厂商

12. 医疗数据交换厂商

13. 政府监管部门

14. 医保部门

医疗数据生态体系中的实体及相互关系



数据安全管理的目标

- 在“正确的时间”将“正确的数据”交到“正确的人”手中

1. 正确的数据

- 掌握自己拥有哪些数据，通过对数据的分类、分级评估其价值及对组织的敏感程度

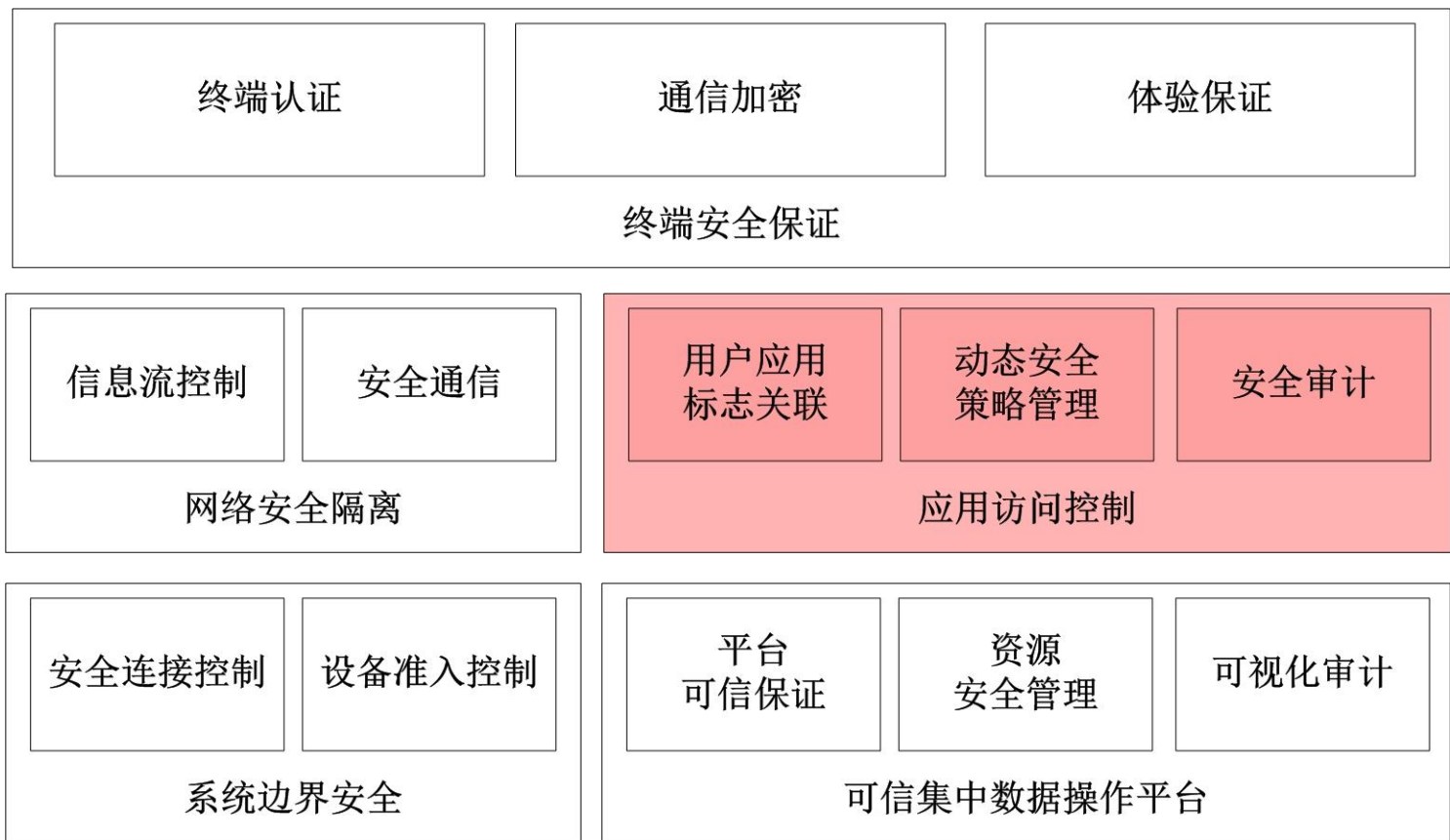
2. 正确的授权控制

- 准确了解数据在医院内部和外部的存储位置和流动方式。确保数据可以安全地从每个数据源传输到授权分析访问人员，同时又保持了隐私信息（病人的以及机构的）。

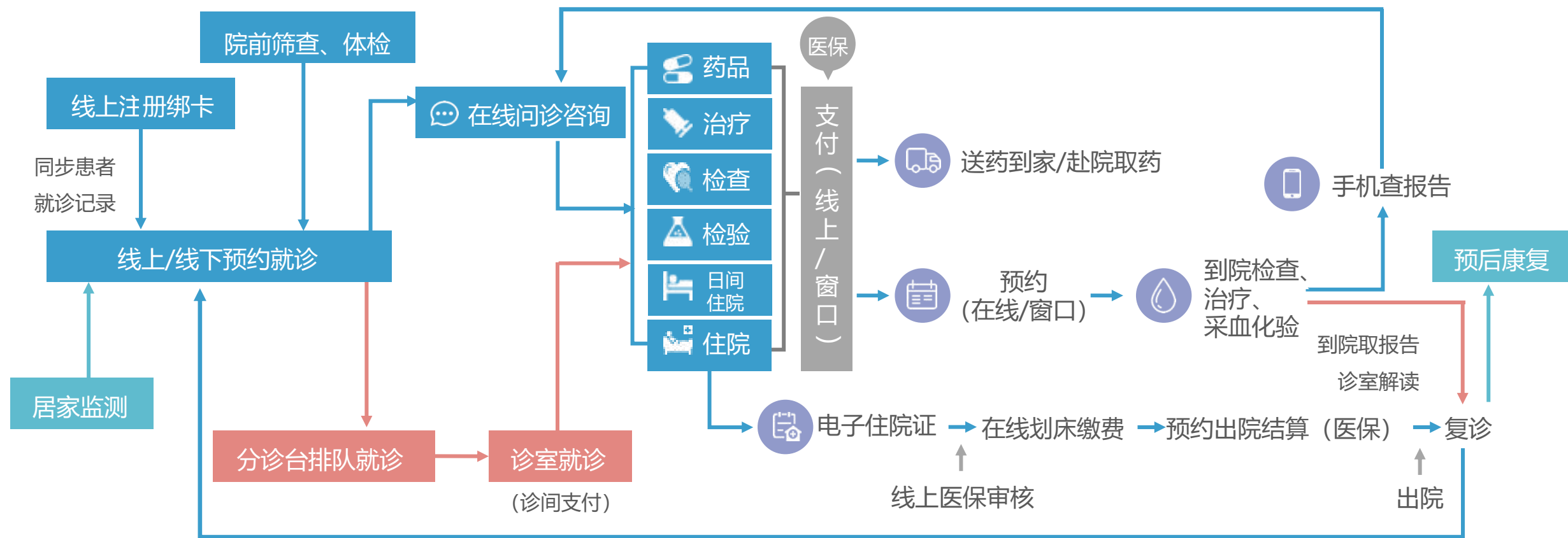
3. 正确的时间

- 拥有授权的时效性。

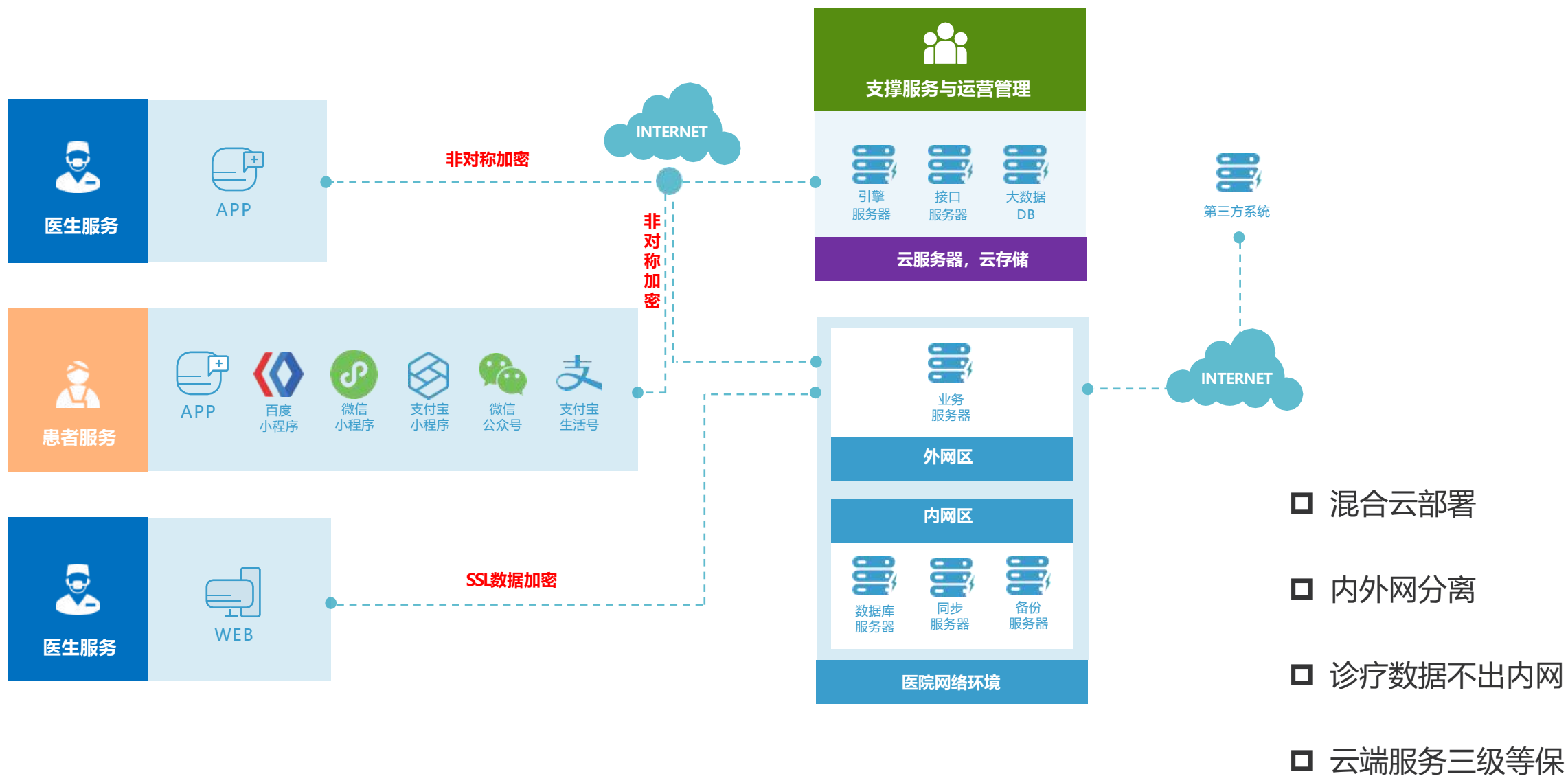
二、组织内的数据安全治理



医院内部业务流程日趋复杂（互联网医院为例）



医院信息系统架构日趋复杂（互联网医院为例）



组织内的主要安全问题及对策

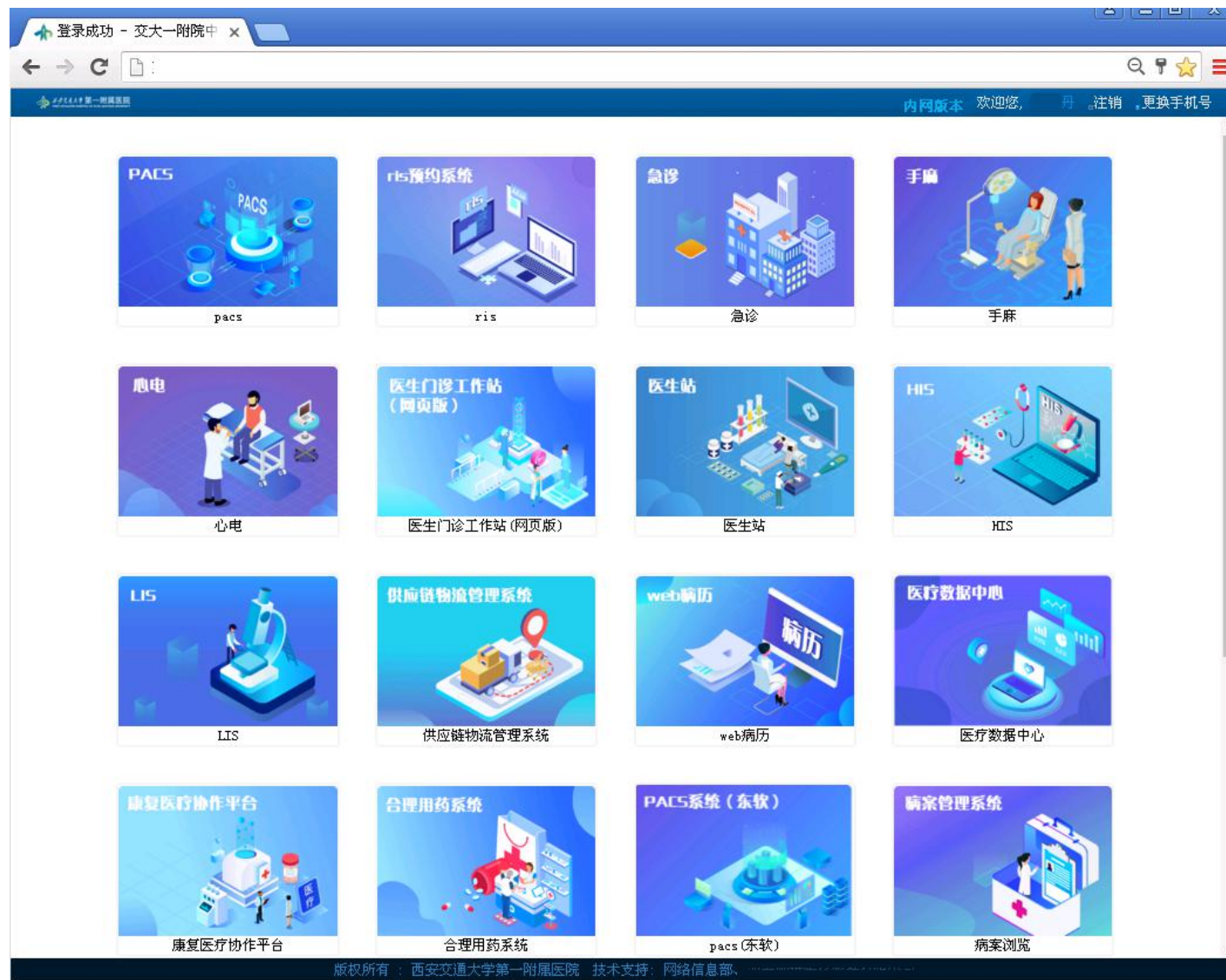
- 非授权访问
 - 系统多而分散
 - 人员流动以及职位的动态调整
- 对策：一般采用基于角色的授权访问机制(RBAC)
 - 数据分类、分级（病人信息，药品，耗材、手术、输血等...）
 - 角色分类（门诊医生、住院医生、检验、病历质控、收费...）
 - 权限分类
 - 角色与权限关联






首先需要明确

1. 确定整个组织的数据是如何产生和流动的。
2. 如何在整个组织的范围内保护数据。
3. 基于角色的，与时间相关的权限分配规则。

医院内部数据安全——统一身份认证



医院内部数据安全——角色的授权



西安交通大学第一附属医院

FIRST AFFILIATED HOSPITAL OF XI'AN JIAOTONG UNIVERSITY

系统管理

西安交通大学第一附属医院 | 通讯录 | 欢迎您! | 退出

平台权限

平台权限类型

平台功能菜单

平台角色权限

平台角色用户

单点登录

职工管理

平台管理

消息中心

平台服务

ETL管理

JOB管理

返回系统首页 / 平台角色权限

角色代码、角色名称

角色代码

角色名称



角色类型

操作

0145

三级公立绩效 (...)



基础角色



0144

三级公立绩效 (...)



基础角色



0143

护士



临床角色



0142

实习医生



临床角色



0141

医生



临床角色



0140

主任医师


临床角色



0139

三级公立绩效 (...)



基础角色



0138

三级公立绩效 (...)



基础角色



0137

数据上报



基础角色



0136

抗体联合


基础角色



0134

三级公立绩效上...



基础角色



0133

报表组


基础角色



0131

运营管理部


基础角色



0127

检验



基础角色



0003

医务科

基础角色



新增角色

主数据管理

医院总线ESB

职工360视图

临床数据中心

操作库管理

商务智能BI

文档中心CDA

知识库

病种库

临床科研

平台监控

平台调度

系统管理

数据上报中心

☒ 360视图

☐ 360页面配置

☐ 闭环流程管理

☒ 360视图

☐ 隐私模板设置

☐ 隐私保护管理

☐ 360访问日志

☐ 个人摘要配置

☐ 闭环节点设置

☒ 临床检索

☒ 我的收藏

保存

医院内部数据安全——用户与角色的关联

返回系统首页 / 平台角色用户

角色代码、角色名称

职工姓名、职工工号

☐ 显示已作废

⊕ 新增该角色人员

⊕ 批量新增该角色人员

角色代码	角色名称	角色分类	职工工号	职工姓名	所属院区	角色范围	操作
0148	三级公立绩效（人...	基础角色	008078	孟		本科室	编辑 作废
0147	三级公立绩效（网...	基础角色	008077	周		本科室	编辑 作废
0146	三级公立绩效（门...	基础角色	008080	许		本科室	编辑 作废
0145	三级公立绩效（药...	基础角色	006662	谢		本科室	编辑 作废
0144	三级公立绩效（护...	基础角色	002783	管		本科室	编辑 作废
0143	护士	临床角色	002627	赵		本科室	编辑 作废
0142	实习医生	临床角色	000967	鱼		本科室	编辑 作废
0141	医生	临床角色	003104	马		本科室	编辑 作废
0140	主任医师	临床角色	009006	阮		本科室	编辑 作废
0139	三级公立绩效（国...	基础角色	000543	张		本科室	编辑 作废
0138	三级公立绩效（医...	基础角色	001484	吴		本科室	编辑 作废
0137	数据上报	基础角色	001526	王		本科室	编辑 作废

共3页 32条数据

«

1

2

3

»

共236页 2831条数据

«

232

233

234

235

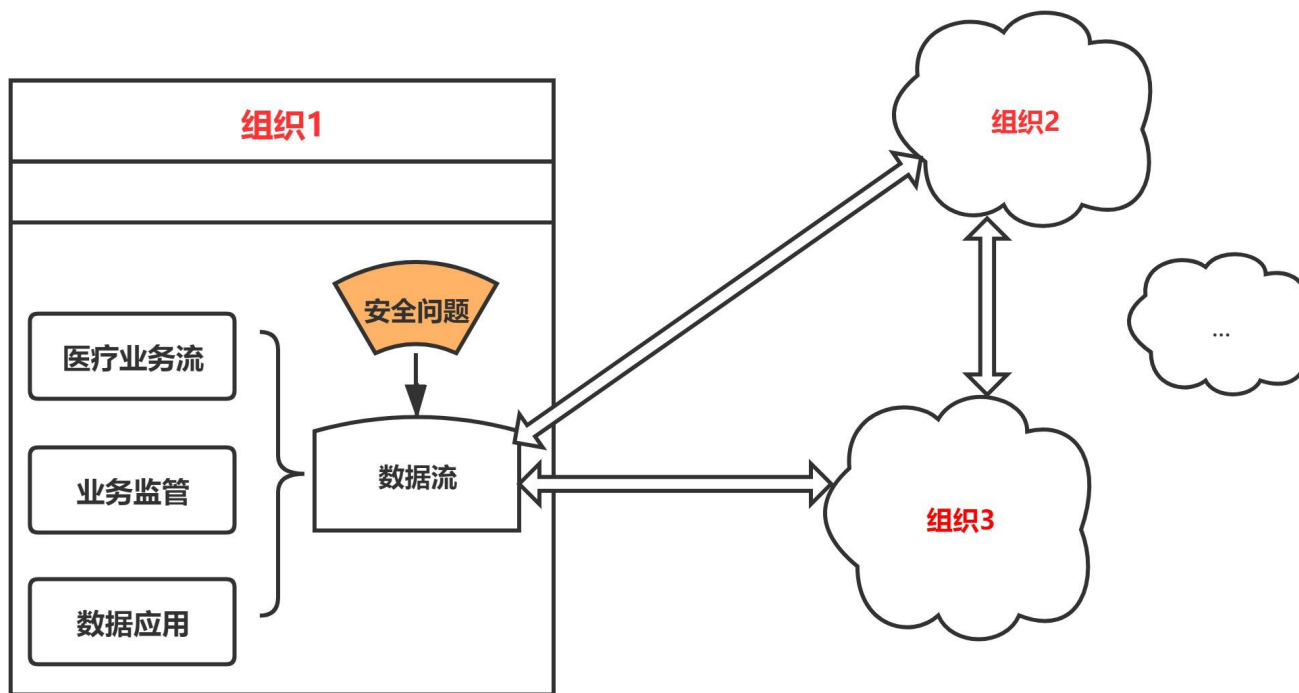
236

»

医院内部数据安全——数据访问日志

返回系统首页 / 360访问日志						
2021/4/22	2021/4/22	模糊查询	Q	今日访问合计: 66	访问总计: 740691	
使用者姓名	IP地址	详细信息	操作时间	访问途径	访问系统	
袁	192.168.106.90	患者主索引^13771464 患者姓名^	2021-04-22 15:23:54	360视图	瑞美lis	
刘	192.168.11.77	患者主索引^12685280 患者姓名^	2021-04-22 15:11:33	360视图	集成平台	
严	192.168.142.125	患者主索引^5175773 患者姓名^	2021-04-22 14:31:37	360视图	医院信息管理系统	
刘	192.168.11.77	患者主索引^12677052 患者姓名^	2021-04-22 12:08:29	360视图	集成平台	
杜	192.168.118.46	患者主索引^13709281 患者姓名^	2021-04-22 11:42:15	360视图	医院信息管理系统	
康	192.168.170.58	患者主索引^13548633 患者姓名^	2021-04-22 11:40:32	360视图	医院信息管理系统	
张	192.168.165.61	患者主索引^6660761 患者姓名^	2021-04-22 11:17:58	360视图	瑞美lis	
赵	192.168.165.249	患者主索引^7548590 患者姓名^	2021-04-22 10:57:02	360视图	瑞美lis	
阮	192.168.106.225	患者主索引^13782785 患者姓名^	2021-04-22 10:53:20	360视图	瑞美lis	
封	192.168.106.4	患者主索引^13782785 患者姓名^	2021-04-22 10:53:01	360视图	瑞美lis	
仵	192.168.116.127	患者主索引^5416706 患者姓名^	2021-04-22 10:13:07	360视图	医院信息管理系统	
仵	192.168.116.127	患者主索引^5416706 患者姓名^	2021-04-22 10:12:37	360视图	医院信息管理系统	
共6页 66条数据				«	1	2 3 4 5 »

三、组织间的数据交换安全管理



- 分级诊疗、远程医疗、健康管理等新业态的产生，必然驱动组织间数据的流动、利用和分析。
- 组织机构间的数据 流出组织边界后，对数据失去控制
- 组织间的数据传输通路和授权访问终端是安全的薄弱环节

数据采集的安全问题及对策

- 问题：

- 医疗数据的采集中直接包含着患者个人信息，如何在保持数据可用的情况下，隐藏用户隐私的内容。

- 对策：

1. 匿名化：既能保证信息的可用性，又能实现隐私保护。
2. 差分隐私技术：在数据集中添加噪声，在保护数据隐私的同时，也确保数据查询的精确性。

数据存储的安全问题及对策

- 问题：

- 很多机构选择云存储；存储在云平台的医疗数据，可能面临着被不可信的第三方偷窥或者篡改的风险。

- 对策：

1. 加密存储技术：以保证数据即使被偷窥也不泄漏其中蕴含的信息。
2. 审计技术：验证数据完整性，以确保数据不被篡改。

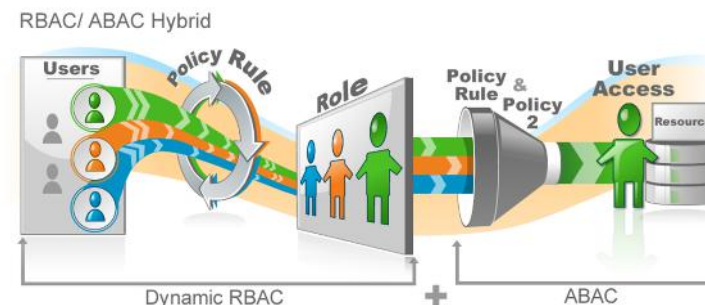
数据共享的安全问题及对策

- 问题：

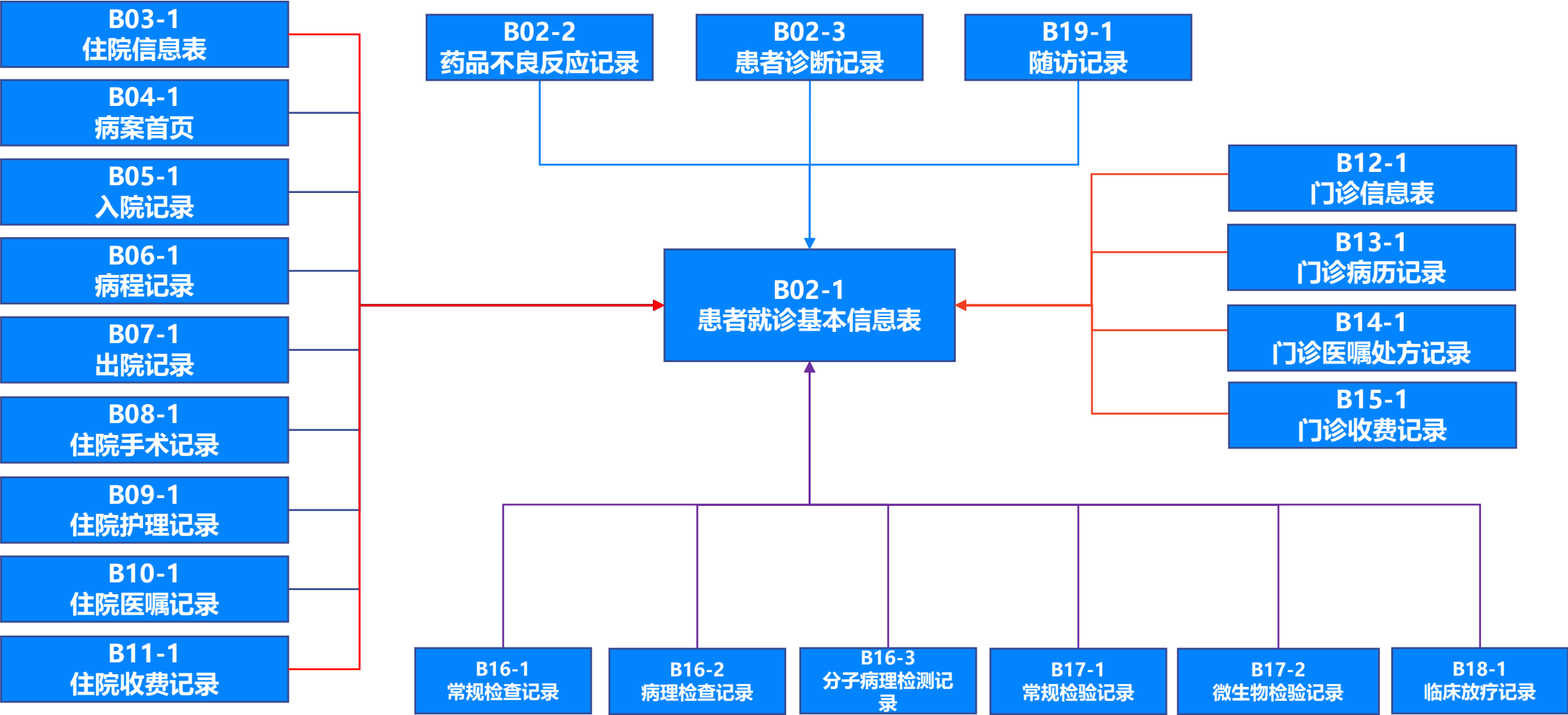
- 当患者的数据存储在云平台上，患者不知道谁访问了共享账户中的数据，因此有很高的数据泄漏风险。

- 对策：

- 访问控制：访问控制技术主要通过给不同的用户分配不同的资源访问权限来确保数据仅被某些有权限的特定用户访问
- 从RBAC到ABAC。ABAC (Attribute-Based Access Control)



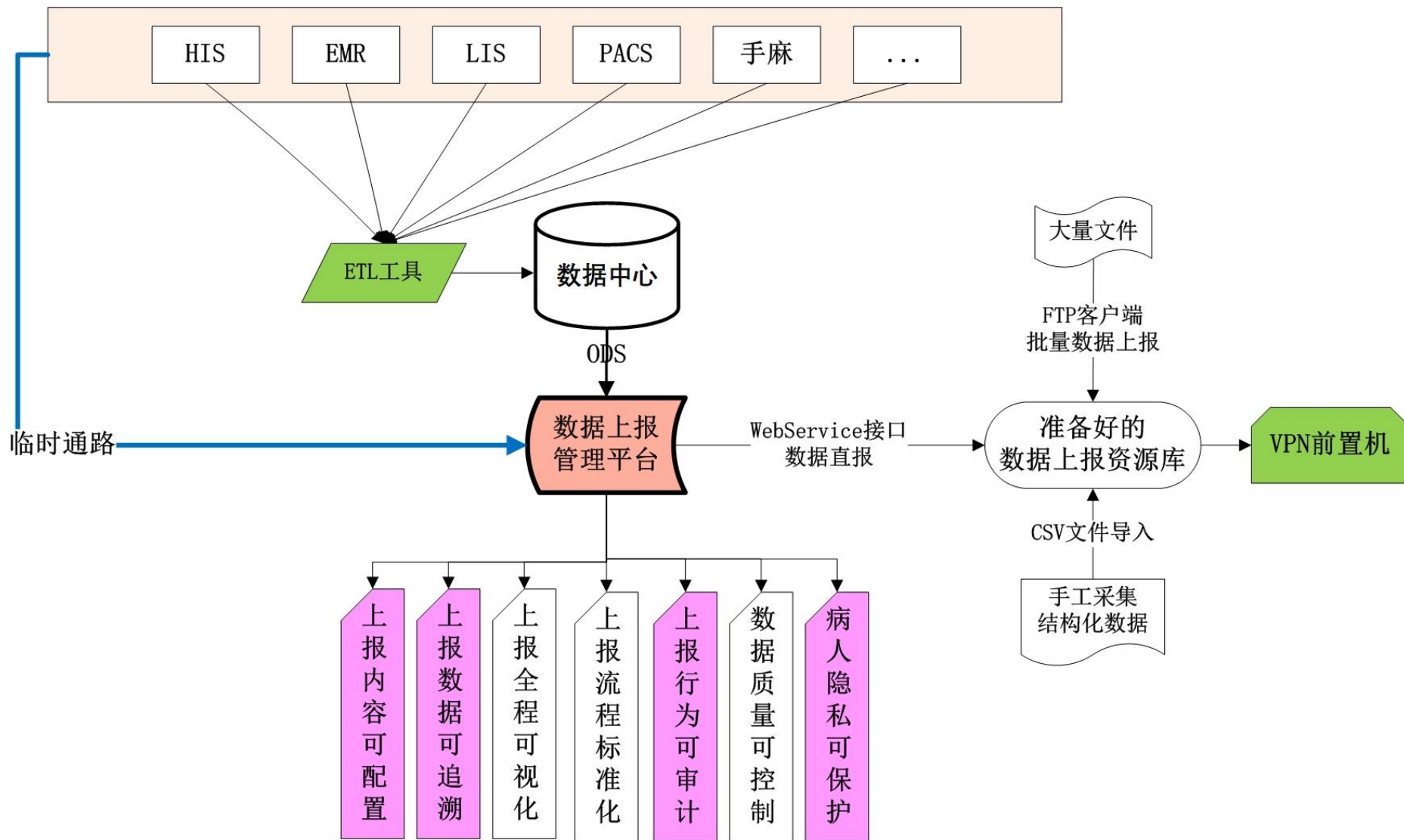
数据上报的安全监管实践



抗肿瘤药物监测数据上报任务分析：7大类，25张数据表（举例）

表单编码	表单中文名	表单分组	表单说明
B01-1	抗肿瘤药物采购记录	药物信息	肿瘤医院：全院药品采购入库记录。综合医院：肿瘤患者治疗所需药品采购入库记录，可参考抗肿瘤药物清单。
B01-2	抗肿瘤药物使用记录		肿瘤医院：全院本周期药品收费记录。综合医院：肿瘤患者本周期药品收费记录，如筛选困难，可参考抗肿瘤药物清单。
B02-1	患者就诊基本信息表	患者信息	肿瘤医院：所有患者基本信息。综合医院：按患者筛选规则（参考上报说明书）进行筛选
B02-2	患者药物不良反应记录		患者就诊期间的药物不良反应记录
B02-3	患者诊断记录		患者就诊期间的诊断记录
B03-1	住院患者信息表	住院信息	肿瘤医院：所有住院患者的出入院登记信息。综合医院：按患者筛选规则（参考上报说明书）进行筛选的住院患者
B04-1	病案首页		患者病案首页信息
B05-1	入院记录		住院患者入院记录
B06-1	病程记录		住院患者所有病程记录：包括首次病程，病程、查房、会诊记录、抢救、手术过程描述等。
B07-1	出院记录		住院患者出院记录
B08-1	住院手术记录		住院手术记录
B09-1	住院护理记录		住院护理记录
B10-1	住院医嘱记录		住院患者所有医嘱信息，包括：长期、临时、检验类、检查类、诊疗类、手术类、治疗类、护理类等。
B11-1	住院收费记录		住院患者所有费用明细信息，包括药品类、医技申请单类、诊疗类（含日间手术等）
B12-1	门诊患者信息表	门诊信息	肿瘤医院：所有门诊患者的挂号信息。综合医院：按患者筛选规则（参考上报说明书）进行筛选的门诊患者
B13-1	门诊病历记录		门诊患者的所有门诊诊断及病历记录
B14-1	门诊医嘱处方记录		门诊患者所有医嘱及处方信息，包括：西药、中成药、中草药、检验、检查、诊疗、手术、治疗、护理等。
B15-1	门诊收费记录		门诊患者所有费用明细信息，包括药品类、医技申请单类、诊疗类（含日间手术等）

统一的数据上报管理平台



1. 新建数据上报任务

字典维护

字典类别

字典值域

值域对照

基础管理

上报平台维护

字典类别

字典值域

值域对照

返回系统首页 / 上报平台维护

输入平台编码或名称

Q

☐ 显示已作废

新增

上报平台编码	上报平台名称	政策文件	上报类型	机构编码	接入系统编码	说明	操作
0004	国家卫生健康委	中国罕见病诊疗服务信息系统接口文档.pdf	接口上报	0004	0004		编辑 作废
02	委属医院上报		接口上报	43523216961011...	3301000001	用于上报国家卫生计生委医院信息服务与...	编辑 作废
肿瘤上报	肿瘤上报		Excel上报	43523216961011...	3301000001		编辑 作废

共1页 3条数据

<

1

>

2. 数据字典值域对照

字典维护

基础管理

返回系统首页 / 值域对照

委属医院上报

字典类别ID字典类别名称

0001身份证件类别代码表

0085ABO血型代码表

0101输血品种代码表

ZDY0002科室字典

共1页 4条数据

东软

输入外部值名称或ID

已对照

未对照

保存

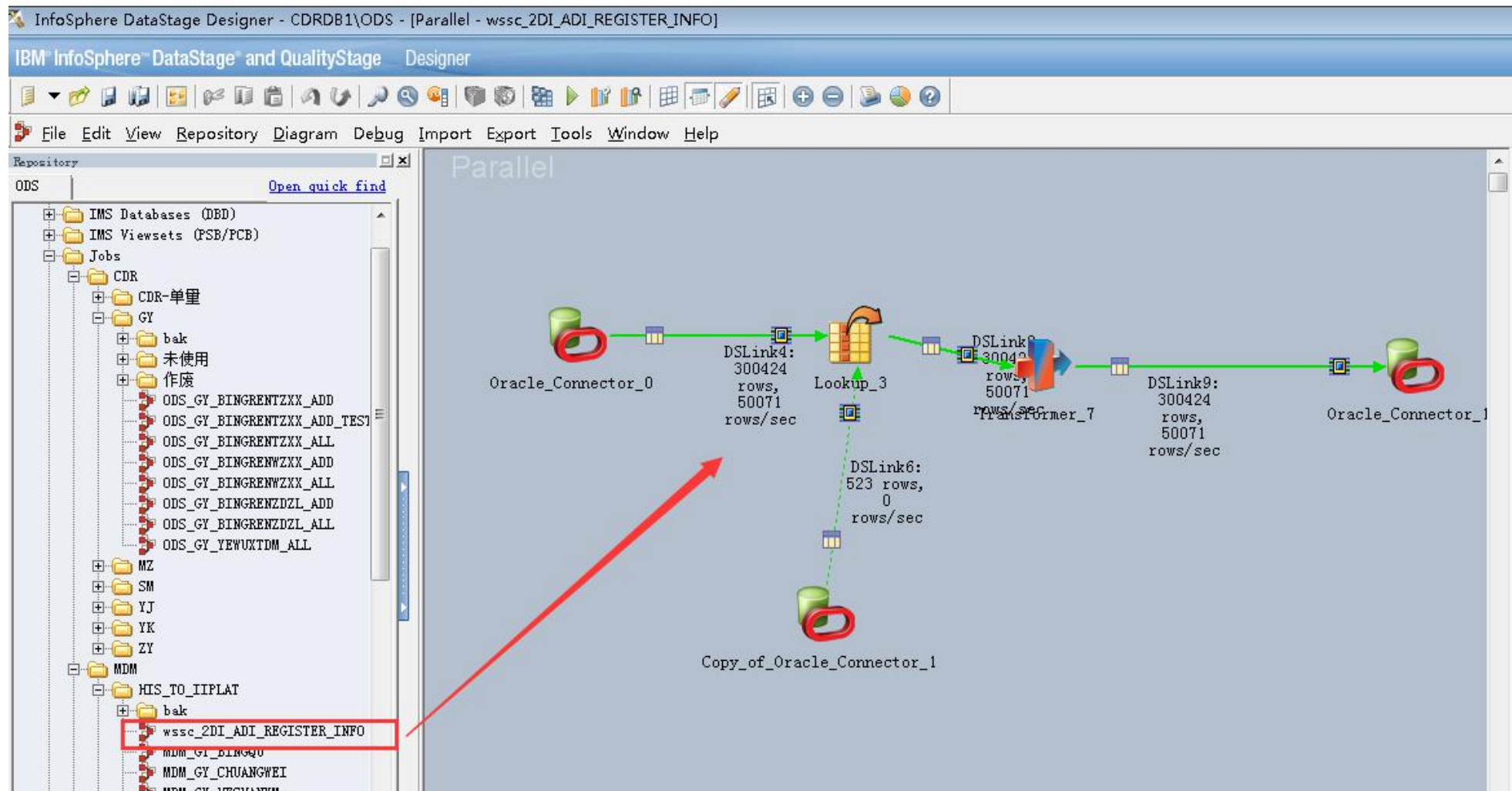
外部值ID	外部值名称	数据源值域	操作
01	身份证	居民身份证	取消对照
02	驾驶证	驾驶证	取消对照
03	军官证	军官证	取消对照
07	护照	护照	取消对照

共1页 4条数据

3. 数据上报脱敏（设置隐私保护）

[illegible]

4. 数据提取



5. 数据自动上报的配置

返回系统首页 / JOB维护

DI_ADI_REGISTER_INFO 🔍 ☐ 显示已作废 ⊕ 新增 🔍

任务分类名称	任务名称	操作	数据开始时间	数据结束时间	执行时间	执行结果	执行信息
IIWEB任务	Job_DRC_DI_ADI_REGISTER_INFO	编辑 作废	2020-04-22 00:00:00	2020-04-23 00:00:00	2020-04-23 14:25:00 至 2020-04-23 14:28:14	✓	成功: 8730/总...
					2020-04-22 14:28:18	✓	成功: 9196/总...
					2020-04-21 18:55:15	✓	成功: 21653/总...
					2020-04-21 17:57:41	✓	成功: 3068/总...
					2020-04-17 14:28:17	✓	成功: 8435/总...
					2020-04-16 14:28:17	✓	成功: 8571/总...
					2020-04-15 14:28:17	✓	成功: 8893/总...
					2020-04-14 14:28:17	✓	成功: 9911/总...
					2020-04-13 14:28:16	✓	成功: 493/总数...
					2020-04-12 14:25:09	✓	

共1页 1条数据

编辑任务控制信息

提交 ×

*任务分类代码

IIWEB任务 × ▾

*任务名称

Job_DRC_DI_ADI_REGISTER_INF(

数据截止时间

2020/4/23 0:00:00

任务开始时间

2020/4/23 14:25:00

任务结束时间

2020/4/23 14:28:14

*任务步长(分钟)

1440

任务描述

门诊诊疗挂号记录 (DI_ADI_REGISTER_INFO) 定时上报任务

6. 上报数据界面化展现

医院运营

门诊分析

门诊月度分析

门诊年度分析

门诊均费分析

门诊均费按科室...

门诊人次报表

门诊收入报表

委属上报2门诊...

住院分析

委属上报2门诊挂号记录

1 / 63

打印[客户端]

打印

输出

邮件

edate: 2020-04-12

sdate: 2020-04-12

查询

序号	人员唯一标识	业务流水号	业务数据产生时间	挂号类别代码	挂号方式代码	挂号费用	预约途径代码	是否退号	是否初诊	是否就诊	挂/退号日期时间	医疗费用支付方式代码	就诊科室代码	科室名称
1	0042398954	29991435	2020-04-21	1	1	12	1	2	2	1	20200421084655	07	A03.04	心血管内科专业
2	0039659313	29991405	2020-04-21	1	1	12	1	2	2	1	20200421084521	07	A09	儿童保健科
3	0000064134	29991407	2020-04-21	1	1	2	1	2	2	1	20200421084524	01	A50.03	妇产科专业
4	0025750913	29991479	2020-04-21	1	1	12	1	2	2	1	20200421084524	07	D99	其他科室
5	0041264259	29991480	2020-04-21	1	2	1	1	2	1	2	20200422103700	07	D99	其他科室
6	0042400259	29991481	2020-04-21	4	1	17	1	2	1	1	20200421084530	07	A06	妇女保健科
7	0041573369	29991410	2020-04-21	4	1	10	1	2	2	1	20200421084533	07	A05.05	生殖健康与不孕症专业

返回系统首页 / JOB维护

DI_ADI_REGISTER_INFO

显示已作废

新增

输入关键词进行搜索

任务分类名称	任务名称	操作	数据开始时间	数据结束时间	执行时间	执行结果	执行信息
IIWEB任务	Job_DRC_DI_ADI_REGISTER_INFO	编辑 作废	2020-04-22 00:00:00	2020-04-23 00:00:00	2020-04-23 14:25:00 至 2020-04-23 14:28:14	✓	成功: 8730/总数: 8730
共1页 1条数据			2020-04-21 00:00:00	2020-04-22 00:00:00	2020-04-22 14:25:00 至 2020-04-22 14:28:18	✓	成功: 9196/总数: 9196
			2020-04-17 00:00:00	2020-04-21 00:00:00	2020-04-21 18:51:56 至 2020-04-21 18:55:15	✓	成功: 21653/总数: 21...
			2020-04-11 00:00:00	2020-04-12 00:00:00	2020-04-21 17:54:27 至 2020-04-21 17:57:41	✓	成功: 3068/总数: 3068
			2020-04-16 00:00:00	2020-04-17 00:00:00	2020-04-17 14:25:00 至 2020-04-17 14:28:17	✓	成功: 8435/总数: 8435
			2020-04-15 00:00:00	2020-04-16 00:00:00	2020-04-16 14:25:00 至 2020-04-16 14:28:17	✓	成功: 8571/总数: 8571
			2020-04-14 00:00:00	2020-04-15 00:00:00	2020-04-15 14:25:00 至 2020-04-15 14:28:17	✓	成功: 8893/总数: 8893
			2020-04-13 00:00:00	2020-04-14 00:00:00	2020-04-14 14:25:00 至 2020-04-14 14:28:17	✓	成功: 9911/总数: 9911
			2020-04-12 00:00:00	2020-04-13 00:00:00	2020-04-13 14:25:00 至 2020-04-13 14:28:16	✓	成功: 493/总数: 493
			2020-04-11 00:00:00	2020-04-12 00:00:00	2020-04-12 14:25:00 至 2020-04-12 14:25:09	✓	
			2020-04-10 00:00:00	2020-04-11 00:00:00	2020-04-11 14:25:00 至 2020-04-11 14:28:18	✓	成功: 7244/总数: 7244
			2020-04-09 00:00:00	2020-04-10 00:00:00	2020-04-10 14:25:00 至 2020-04-10 14:28:16	✓	成功: 8235/总数: 8235
			2020-04-08 00:00:00	2020-04-09 00:00:00	2020-04-09 14:25:00 至 2020-04-09 14:28:17	✓	成功: 8147/总数: 8147
			2020-04-07 00:00:00	2020-04-08 00:00:00	2020-04-08 14:25:00 至 2020-04-08 14:28:17	✓	成功: 8924/总数: 8924

共9页 120条数据

1 2 3 4 5

7. 数据上报的监控和审计



西安交通大学第一附属医院

FIRST AFFILIATED HOSPITAL OF XI'AN JIAOTONG UNIVERSITY

数据上报中心

西安交通大学第一附属医院

通讯录

欢迎您!

退出

返回系统首页 / 数据上报执行

委属医院上报

输入任务名称

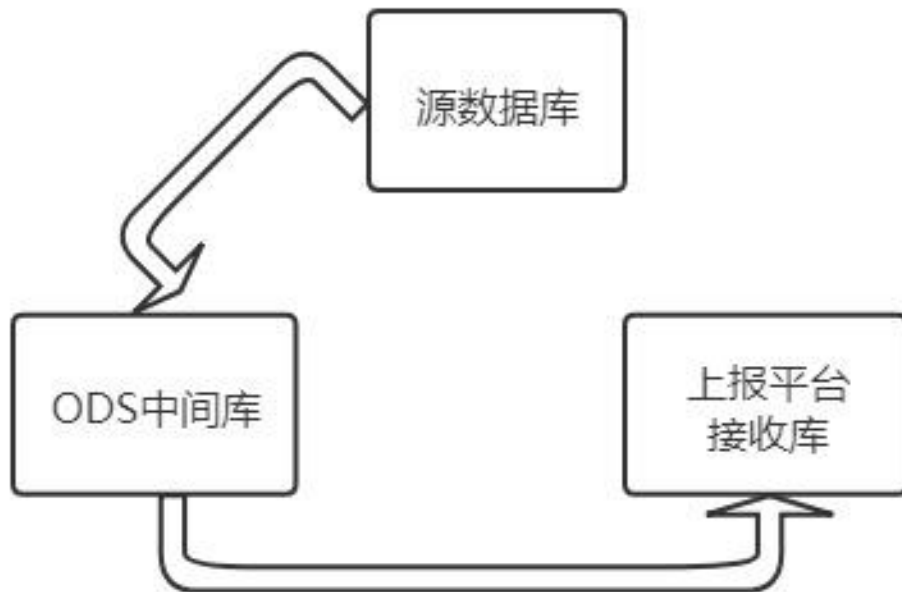
全部状态 成功 失败

批量执行

<input type="checkbox"/>	任务名称	任务描述	视图表名	状态	上次上传时间	下次上传时间	操作
<input type="checkbox"/>	DI_PATIENT_TREAT_IN...	患者就诊基本信息上报	DRC_V_DI_PATIENT_T...	成功	2021-03-31 14:20:00	2021-04-01 14:20:00	执行 查看
<input type="checkbox"/>	DI_ADI_REGISTER_INFO	门诊诊疗挂号记录上报	DRC_V_DI_ADI_REGIST...	成功	2021-03-31 14:25:00	2021-04-01 14:25:00	执行 查看
<input type="checkbox"/>	DI_ADI_RECORD_INFO	门急诊诊疗病历上报	DRC_V_DI_ADI_RECOR...	成功	2021-03-31 14:30:00	2021-04-01 14:30:00	执行 查看
<input type="checkbox"/>	DI_ADI_DIAREC_INFO	门诊诊疗诊断记录上报	DRC_V_DI_ADI_DIARE...	成功	2021-03-31 14:35:00	2021-04-01 14:35:00	执行 查看
<input type="checkbox"/>	DI_ADI_DRUREC_INFO	门急诊诊疗处方上报	DRC_V_DI_ADI_DRURE...	成功	2021-03-31 14:40:00	2021-04-01 14:40:00	执行 查看
<input type="checkbox"/>	DI_ADI_EXPSET_INFO	门诊诊疗费用记录上报	DRC_V_DI_ADI_EXPSE...	成功	2021-03-31 14:45:00	2021-04-01 14:45:00	执行 查看
<input type="checkbox"/>	DI_ADI_EXPSET_LIST	门诊诊疗费用明细记录...	DRC_V_DI_ADI_EXPSE...	成功	2021-03-31 14:50:00	2021-04-01 14:50:00	执行 查看

8. 数据校验

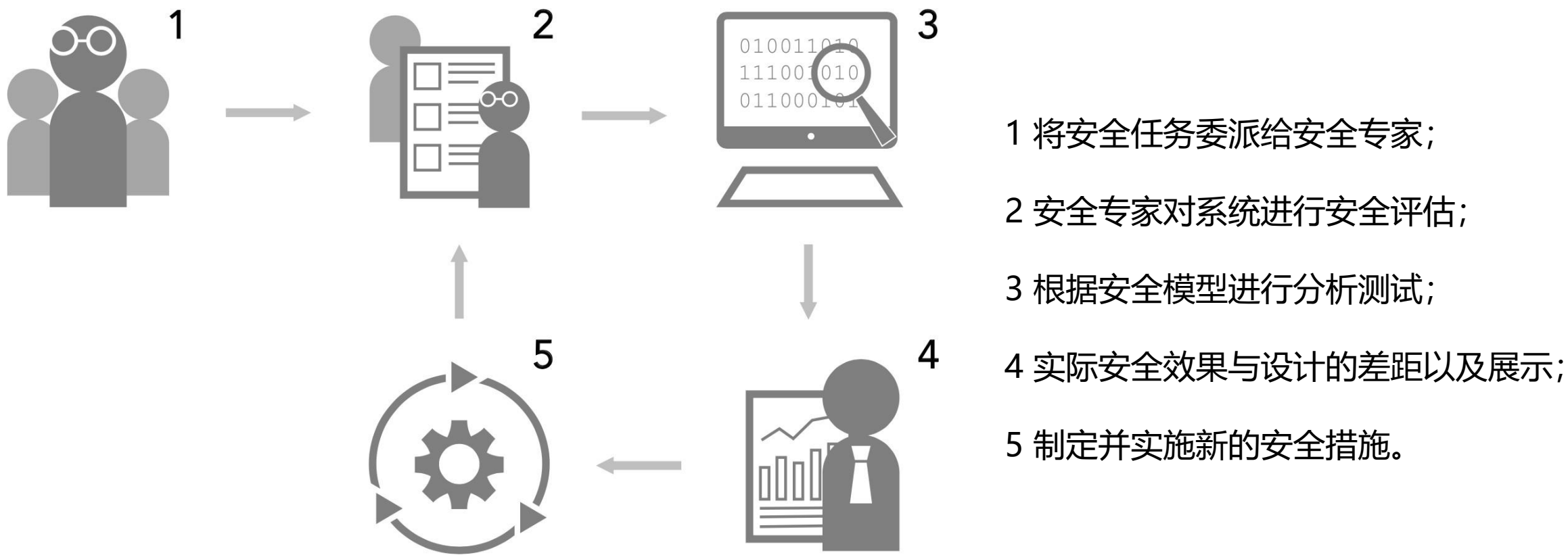
- 源数据库、ODS中间库、上报平台接收库。
- 三者数据总量一致，则校验通过。



四、总结

1. 数据应用与数据安全是**一对矛盾**。
2. 新技术的应用和快速变化的业务对静态安全策略提出挑战。
3. 安全问题是一个系统问题，需要有全局观，需要**安全技术+管理制度+法律法规**的相互配合。
4. 将主要精力放在自己可以把握的安全措施上（如分级授权）。
5. 对于无法把握的安全问题，交给专业的第三方安全服务提供商。

医疗数据安全是一个持续改进的过程





感谢聆听！

