

LIÇÕES DO SISTEMA DE GARANTIA DE PRIVACIDADE E SEGURANÇA AMERICANO - HIPAA - PARA O SISTEMA NACIONAL DE SAÚDE PORTUGUÊS

HENRIQUE CURADO e LUÍS VELEZ LAPÃO

Lisboa, 3 Novembro 2005

Henrique Curado [1], Luís Velez Lapão [2]

[1] DPS, Escola Superior de Tecnologia da saúde do Porto - Instituto Politécnico do Porto

[2] DID - Instituto Nacional de Administração


AGENDA

1. Realidade actual dos SI nos hospitais como resultado de anos de desnorte
2. O equilíbrio possível dos distintos interesses em confronto – pessoais e público.
3. O equilíbrio possível entre privacidade e segurança.
4. Estado actual do tratamento dos dados pessoais pelo Sistema de Saúde português.
5. Lições que se podem retirar do sistema de garantia de privacidade e segurança americano - HIPAA - para o Sistema Nacional de Saúde Português.
6. Conclusões.

REALIDADE ACTUAL DOS SI NOS HOSPITAIS COMO RESULTADO DE ANOS DE DESNORTE

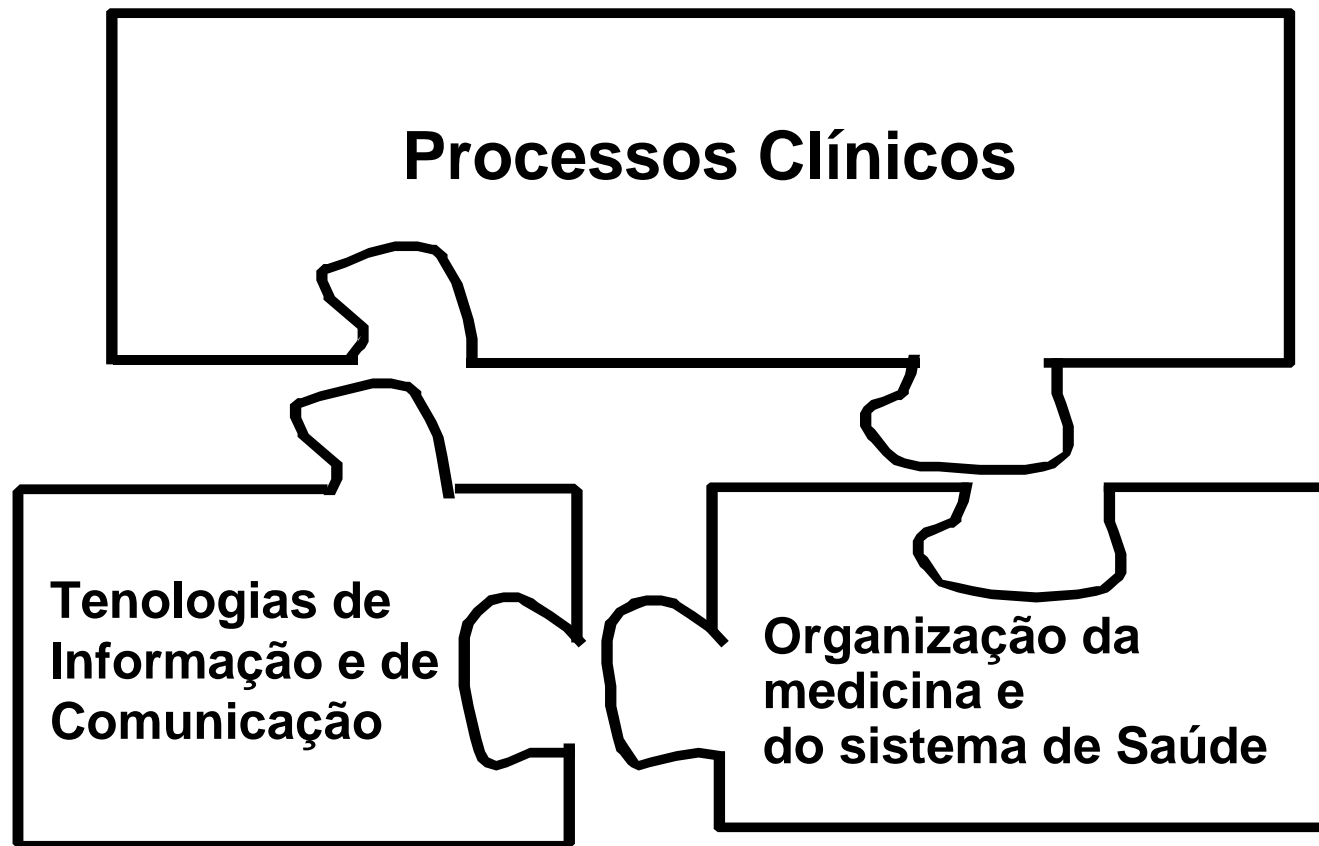
- INEXISTÊNCIA DE ESTRATÉGIA E DE ARQUITECTURAS ADEQUADAS
- “LEGACY SYSTEMS”
 - A existência de sistemas aplicacionais desactualizados e não padronizados.
- FALTA DE INTEGRAÇÃO E POUCA CONSISTÊNCIA DA INFORMAÇÃO
 - As aplicações não estão integradas por forma a garantir acesso à informação.
- POUCO CONHECIMENTO DAS APLICAÇÕES E GRANDE DEPENDÊNCIA DOS FORNECEDORES
 - O conhecimento das aplicações (e do modelo de dados) é um factor crítico.
- PROCESSOS E PROCEDIMENTOS POUCO DEFINIDOS
 - Existem problemas associados aos processos organizacionais.

**OS SISTEMAS DE SAÚDE NECESSITAM DE ENCONTRAR
UM EQUILÍBRIO EFICIENTE**



**PORQUE PRECISAMOS DE
INFORMAÇÃO
ATEMPADAMENTE
PARA A
GESTÃO**

OS VÁRIOS SISTEMAS NECESSITAM DE AJUSTE ATRAVÉS DAS TECNOLOGIAS DE INFORMAÇÃO



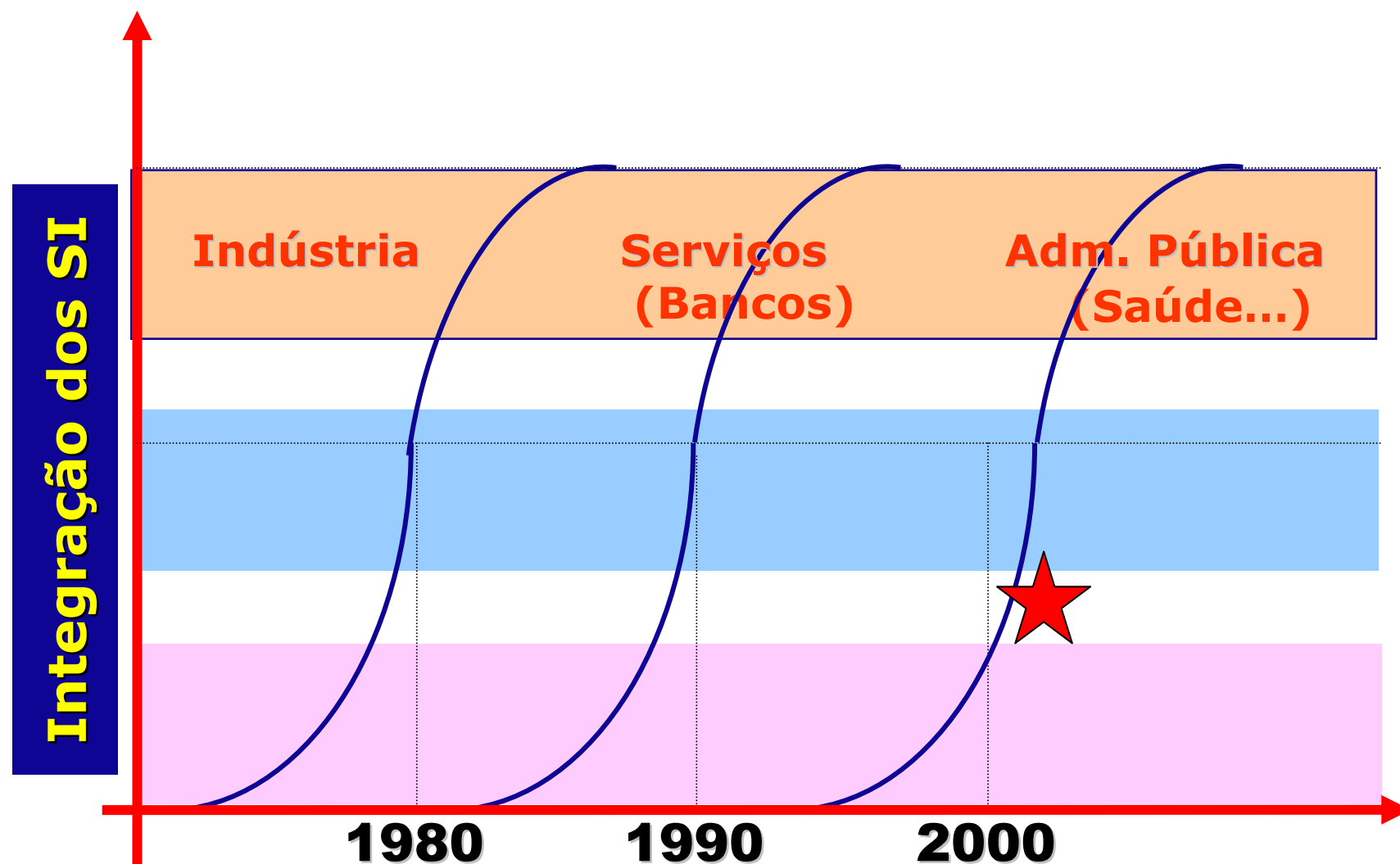
ERROS COMUNS ASSOCIADOS AO USO DE SI

- Informação inconsistente ou que não se encontra
- Identificação dos pacientes
 - Duplicação do ID implica perda das histórias,
 - Dois pacientes com o mesmo ID: inconsistência grave!!
- Atraso entre mensagens
 - Incompatibilidade semântica e de formatos...
- Meio diferente
 - Alteração de documentos em vários locais - inconsistência
- Código de barras errado
 - Utilização errada de códigos de barras “velhos”
- No casos do sistema falhar
 - Devem conhecer-se os processos convencionais

JG Anderson, MD Computing May/June 2000

A ONDA DE INTEGRAÇÃO ATINGE A SAÚDE

A Curva S Representa a Evolução de um “Tecnologia” num Ambiente “Selvagem”



IT como “novidade”

Constituem-se redes, ...

Integração dos SI no Negócio (Organizational, Legal, etc)

Jean-Claude Healy
May 2000

IMPORTÂNCIA DOS PROTOCOLOS “STANDARD” NUM SISTEMA DE INFORMAÇÃO HOSPITALAR

- **Existe a necessidade de partilhar dados entre várias aplicações no HIS**
 - Os dados existem em muitos formatos e tipos;
- **É preciso garantir a partilha de dados e conhecimento para se promover a melhoria dos cuidados de saúde e para se aumentar a eficiência económica;**
- **Procura da melhor qualidade**
 - A partilha só é economicamente possível se existir inter-operabilidade entre as aplicações;
- **A Inter-operabilidade existe sómente se se definir um conjunto de “standards” para o HIS.**
 - Exemplo: DICOM, HL7, XML, etc

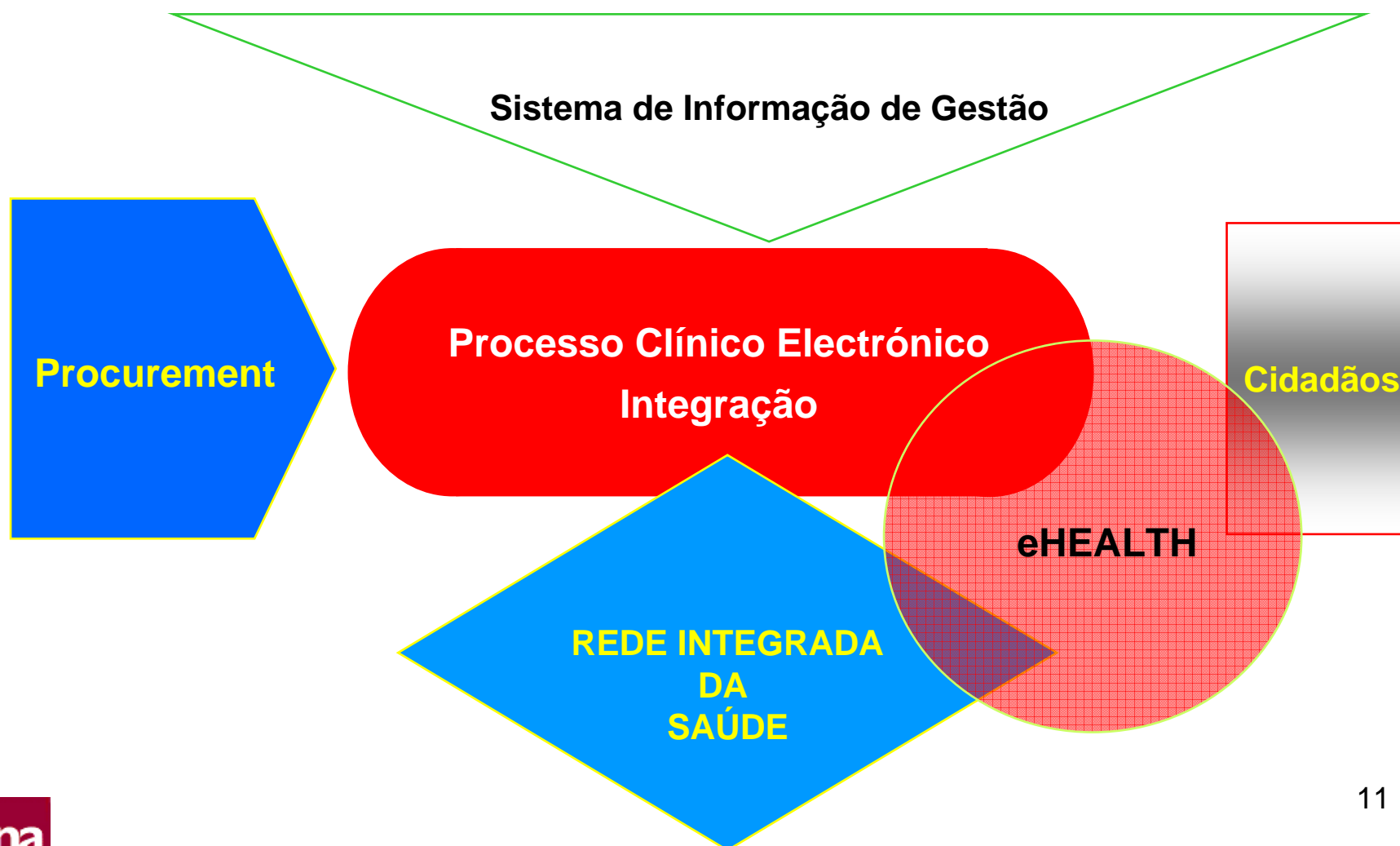


VISÃO DA SAÚDE COMO RESPOSTA À EVOLUÇÃO DA SOCIEDADE



eHEALTH NO *HOSPITAL INFORMATION SYSTEM*

Potenciar a Integração das Unidades de Saúde



- VISÃO - O CIDADÃO TORNA-SE O “OWNER” DA INFORMAÇÃO

Integração de Unidades de Saúde Aproxima o Cidadão



Observações Preliminares:

Lei de Bases da Saúde *

Base XII – Sistema de saúde

1 – O sistema de saúde é constituído pelo Serviço Nacional de Saúde e por todas as entidades públicas que desenvolvam actividades de promoção, prevenção e tratamento na área da saúde, bem como por todas as entidades privadas e por todos os profissionais livres que acordem com a primeira a prestação de todas ou de algumas daquelas actividades.

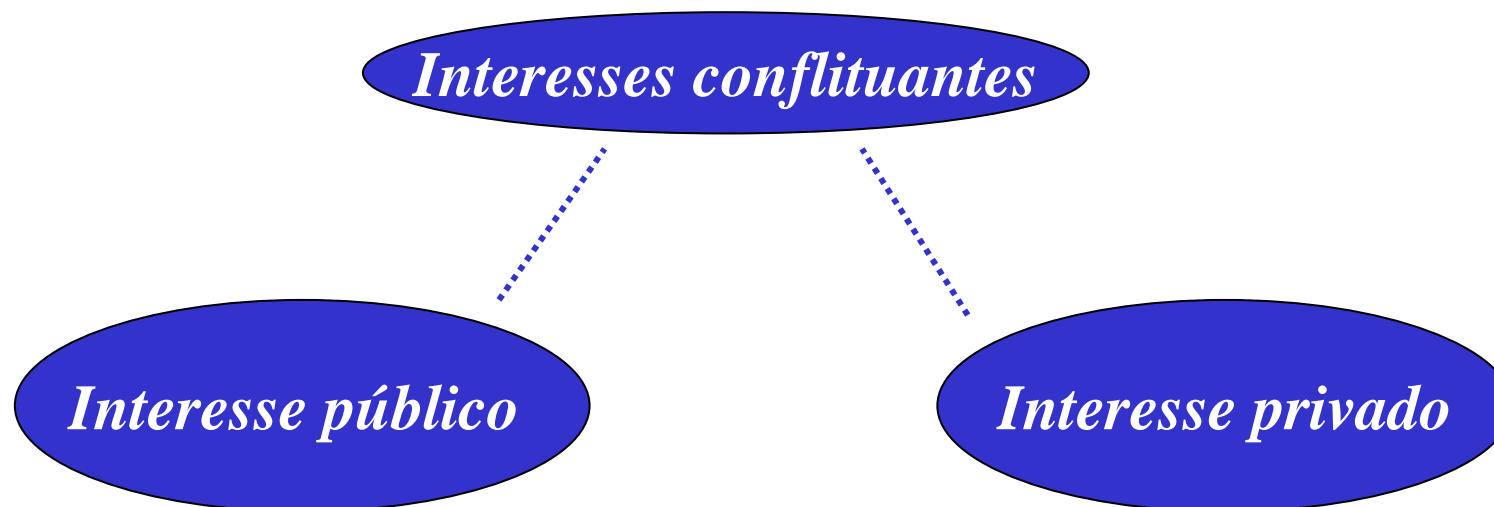
* Lei N.º 48/90, de 24 de Agosto, alterada pela Lei N.º 27/2002

Tal permite-nos a seguinte representação esquemática:



O EQUILÍBRIO POSSÍVEL DOS DISTINTOS INTERESSES EM CONFRONTO

Análise das vantagens e desvantagens de um sistema de informação em saúde, **geral** (cobrindo todas as unidades de saúde do sistema de saúde) **universal** (quanto à população abrangida) e **integrado** (no sentido de integrar e partilhar a informação de todos os doentes de todas as unidades de saúde).



O EQUILÍBRIO POSSÍVEL DOS DISTINTOS INTERESSES EM CONFRONTO



Interesse público

Reclama a partilha de informação:

- Aumento da eficácia do SNS (evitando ou minorando as “falsas patologias”, facilitando estudos epidemiológicos);
- Aumento da eficiência das unidades de saúde (mediante a redução de custos de arquivo e manuseamento de informação, a celeridade no atendimento, a partilha de informação entre distintas unidades de saúde e aumento das sinergias).
- Por outro lado, desde que dotado de elevados níveis de segurança poderia contribuir para uma maior protecção da informação (dado ser mais fácil desaparecer um documento em suporte de papel);

O EQUILÍBRIO POSSÍVEL DOS DISTINTOS INTERESSES EM CONFRONTO

Interesse privado

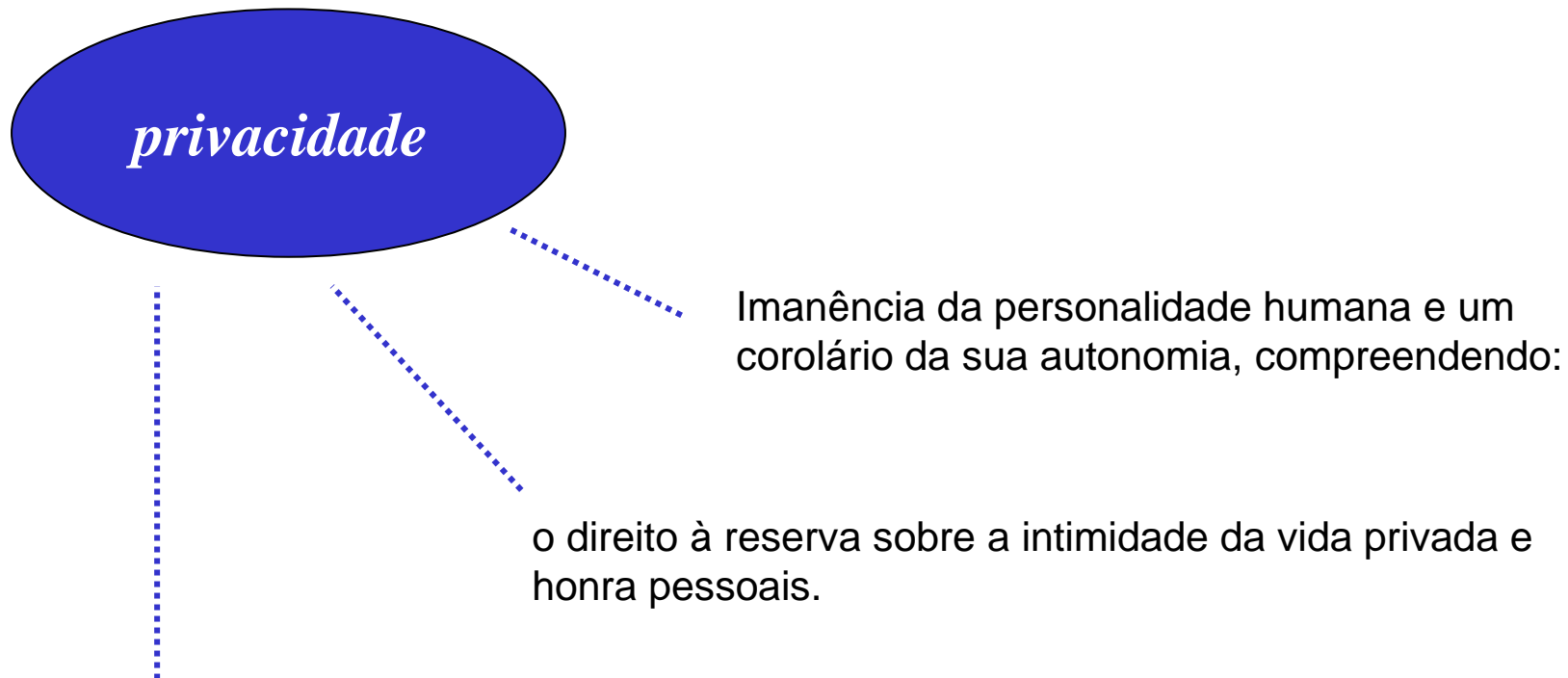
Reclama privacidade e segurança da informação

Uma base de dados informática possibilita o acesso a um maior número de pessoas do que um arquivo tradicional, dada a disponibilidade dessa informação em rede e a transmissão dos dados que sempre ocorre.

Riscos apontados, associados à fuga de informação:

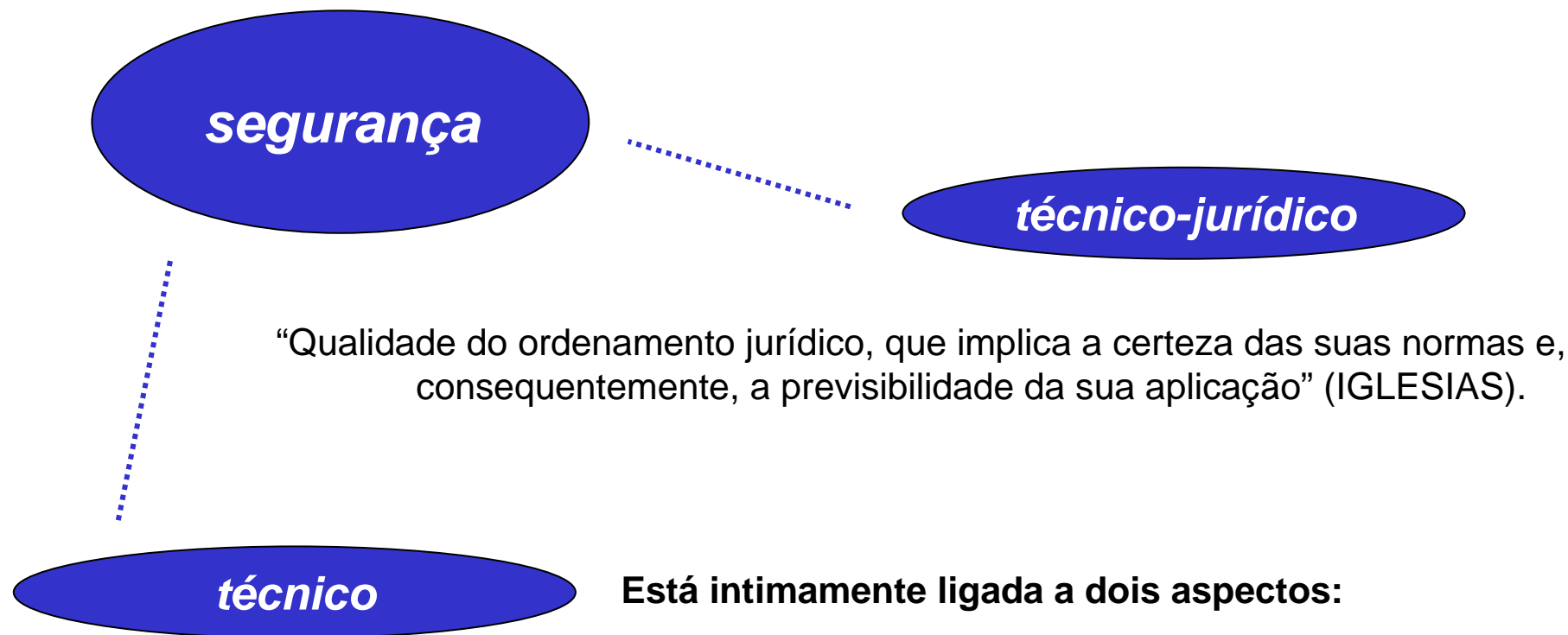
- São a recusa de celebração de contratos de seguros devido ao conhecimento de certas doenças,
- O possível conhecimento pelas entidades empregadoras poder condicionar a celebração de contratos de trabalho ou mesmo a progressão,
- O possível “assédio” de entidades privadas com propostas de fornecimento de serviços e produtos de saúde diversos,
- A devassa da intimidade da vida privada de entidades sujeitas a uma certa exposição pública (em particular políticos e desportistas).

O EQUILÍBRIO POSSÍVEL ENTRE PRIVACIDADE E SEGURANÇA



Consequentemente, é o “indivíduo que tem o direito de decidir que as suas informações pessoais sejam mantidas sob o seu exclusivo controlo, como tem o direito de comunicar a quem, quando, onde e em que condições as informações pessoais devem ser reveladas” (FORTES).

O EQUILÍBRIO POSSÍVEL ENTRE PRIVACIDADE E SEGURANÇA



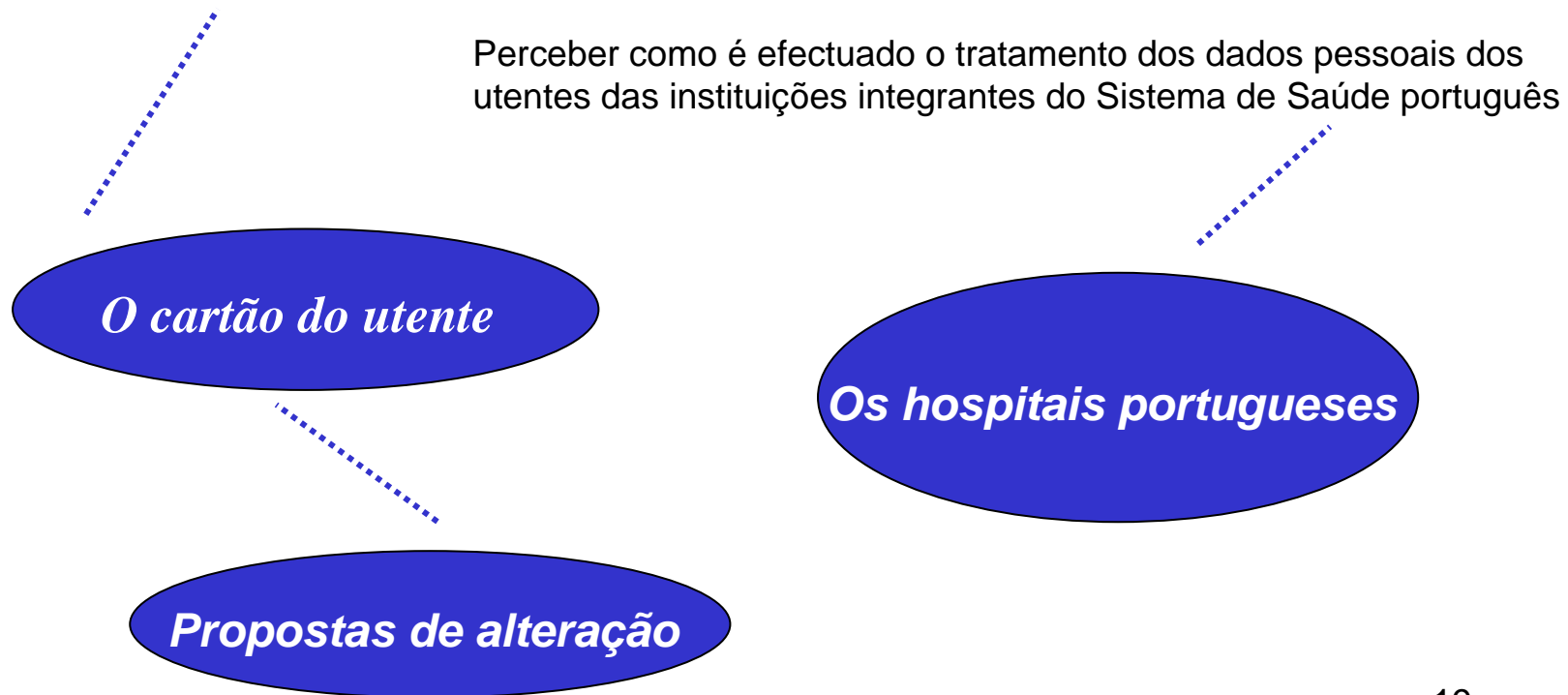
“Qualidade do ordenamento jurídico, que implica a certeza das suas normas e, consequentemente, a previsibilidade da sua aplicação” (IGLESIAS).

- À definição de níveis de acesso à informação (quem pode aceder a que informação e em que condições);
- À implementação e manutenção de um sistema de registo dos acessos à informação (quem acedeu a que informação e quando).

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

Aspectos a considerar:

Inexistência de um sistema de informação em saúde, susceptível de fornecer informação de forma universal em qualquer unidade prestadora de cuidados de saúde.



O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS



O cartão do utente

Decreto-Lei N.º 198/95, de 29 de Julho
criou o cartão do utente do Serviço Nacional de Saúde

Preâmbulo:

- “Diversidade de suportes de identificação”
- “Incorrecta definição da situação do utente, susceptível de comprometer o interesse público e, bem assim, de lesar a obtenção de benefícios directos pelos particulares.”
- Assegurar “a definição exacta da situação de cada um”.

Todavia resulta do art.º 13.º: nome, nacionalidade e naturalidade, sexo, data de nascimento, morada e telefone, o seu número de inscrição no centro de saúde, identificação da entidade responsável pelo pagamento ou comparticipação nas despesas com saúde e respectiva data limite de validade, informação sobre o direito a isenções ou benefícios e respectivas datas de validade, eventual isenção de taxa moderadora, regime especial de comparticipação de medicamentos e número de cédula profissional do médico de clínica geral.

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

Propostas de alteração - 1

Projectos de diploma – 2004 e 2005

Preâmbulo - pretendia:

A “automatização dos pagamentos”, a “operacionalidade na facturação, rigor no controlo dos actos praticados, combate à fraude e disponibilidade imediata de informação de gestão”.

Criação de “uma única base de dados acessível a todos os serviços prestadores de cuidados”, a qual deveria permitir “a correcta definição dos episódios de saúde de que o utente é sujeito”.

Parecer n.º 38/2004 da CNPD:

Graves deficiências quanto à recolha e processamento da informação, não sendo ainda especificados os dados pessoais que constariam do cartão do utente, em particular em matéria de rendimentos e dados de saúde, para além da necessidade de clarificação do acesso à informação (quem e como).

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

Propostas de alteração - 2

Projectos de diploma – 2004 e 2005

Preâmbulo - pretendia:

- Armazenar dados de saúde do utente, resultantes dos diversos actos clínicos, susceptíveis de acesso quando o mesmo fosse sujeito a situações de emergência médica.
- Saber-se em qualquer local (instituição prestadora de cuidados de saúde) que cuidados foram prestados a cada utente, respectivo diagnóstico, prescrições efectuadas e aquisição de medicamentos.
- Implicaria a centralização de informação a efectuar mediante a transmissão dos dados, recolhidos episodicamente, ao IGIF.

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

Propostas de alteração - 2

Projectos de diploma – 2004 e 2005

Preâmbulo - pretendia:

Parecer n.º 2/2005 da CNPD –

deficiências - Violação da Lei de Protecção de Dados Pessoais - a dois níveis:

- 1 - Não especificação da finalidade do tratamento de determinados dados
- 2 - A centralização de informação no IGIF, entidade sem qualquer função na prestação de cuidados de saúde.

“Só será legítimo o tratamento se (...) houver disposição legal ou consentimento do titular dos dados. (...) Esta disposição legal – porque estamos no domínio de dados sensíveis e que afecta direitos fundamentais dos titulares – terá que ser, necessariamente, uma Lei da Assembleia da República ou Decreto-lei autorizado (cf- artigo 165.º n.º 1 al. b) da CRP)”.

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

Análise efectuada pela CNPD - disponível no Relatório de Auditoria ao Tratamento da Informação de Saúde nos Hospitais, em resultado da visita de 38 hospitais. **Da mesma podemos concluir:**



*Os hospitais
portugueses*

- Cerca de 50% dos hospitais não procedem ao levantamento das situações de tratamento de dados pessoais, nem procedem à sua notificação à CNPD, como legalmente lhes é devido.
- Nenhum hospital – salvo alguns, nas situações de vídeovigilância - adoptou mecanismos concretos tendentes a assegurar o direito de informação dos titulares dos dados, tal como legalmente imposto.
- O incumprimento da lei é generalizado quando têm sido facultados dados pessoais para fins de investigação científica.
- Há falta de cumprimento dos prazos de conservação de dados de saúde.

O TRATAMENTO ACTUAL DOS DADOS PESSOAIS PELO SISTEMA DE SAÚDE PORTUGUÊS

*Os hospitais
portugueses*

Avultado número de processos clínicos em suporte de papel - “por mais esforços que sejam feitos, existe sempre o risco de a informação clínica ser acessível por terceiros não autorizados” dado que “o processo clínico em papel encontra-se, por natureza, exposto à curiosidade geral – quer no próprio arquivo, quer nos serviços onde circula – não havendo mecanismos eficazes que assegurem a impossibilidade de devassa”. Considerando que “só os suportes automatizados dotados das necessárias seguranças – *passwords* – com «perfis de utilizadores» bem definidos, separação lógica entre dados administrativos e de saúde – podem conferir a necessária confidencialidade à informação clínica dos doentes”.

CNPD - Relatório de Auditoria ao Tratamento da Informação de Saúde nos Hospitais

LIÇÕES QUE SE PODEM RETIRAR DO SISTEMA DE GARANTIA DE PRIVACIDADE E SEGURANÇA AMERICANO - HIPAA

A primeira lição resulta patente nos factos.

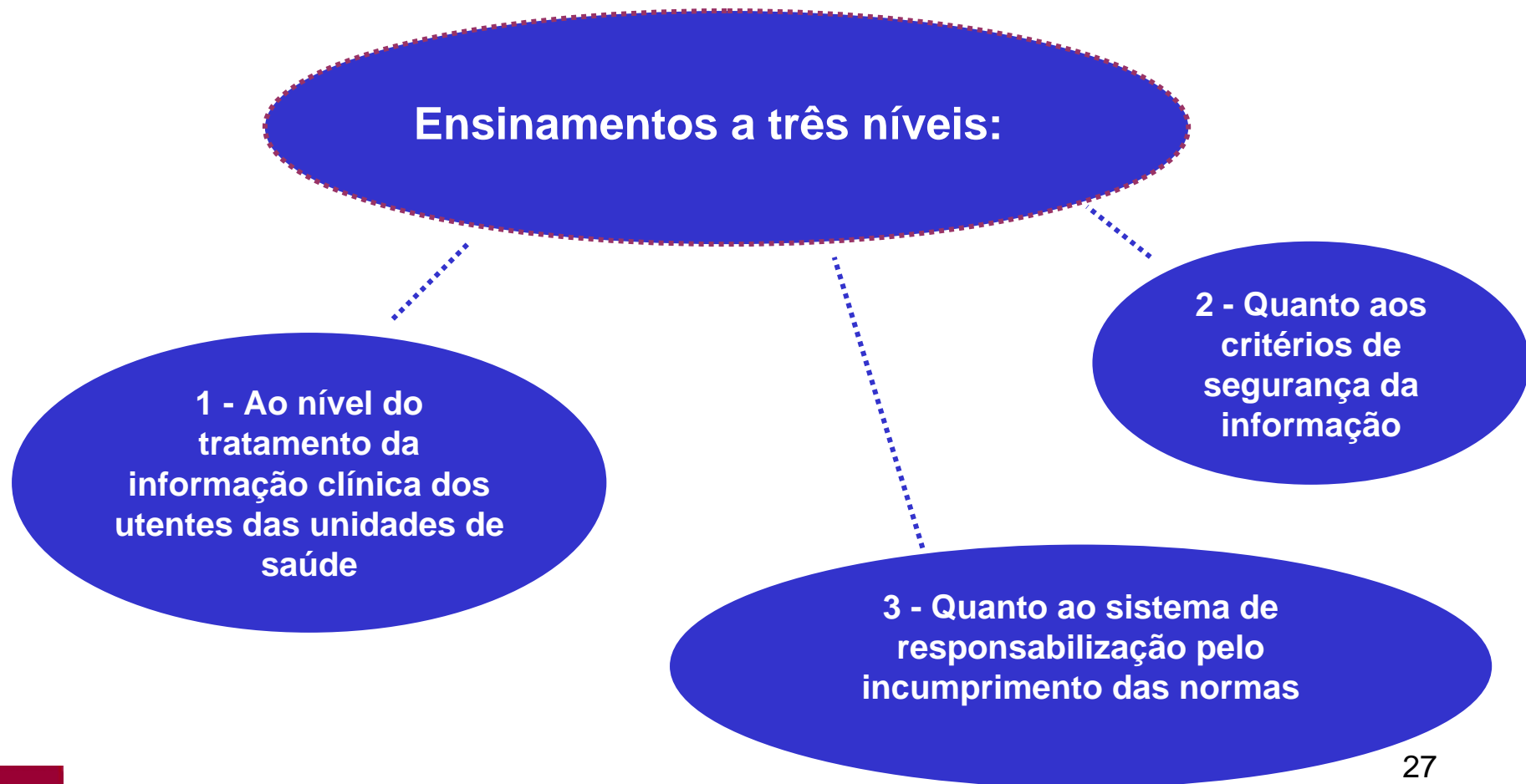
De facto, foi criado, em diploma próprio, um sistema de garantia da privacidade da informação clínica respeitante aos utentes de unidades de saúde,

O universo de destinatários é incomparável com o do sistema de saúde português.

Facto relevante porquanto a inexistência dum sistema similar em Portugal não resulta assim de dificuldades de dimensão.

Relevância do HIPPA: a portabilidade do sistema. Com efeito, são estabelecidos critérios de segurança face à gestão da informação e à sua transacção, salvaguardando-se a privacidade e o consentimento do interessado, devendo a protecção de dados de saúde ser garantida em qualquer tipo de suporte – escrito, falado, electrónico ou qualquer outro – atendendo à possibilidade da disponibilização da informação.

LIÇÕES QUE SE PODEM RETIRAR DO SISTEMA DE GARANTIA DE PRIVACIDADE E SEGURANÇA AMERICANO - HIPAA



HIPAA – 1. tratamento da informação clínica

Assenta em três pilares fundamentais:



Notificação

Enquanto obrigatoriedade de informação dos utentes mediante linguagem simples quanto à necessidade do seu consentimento e à possibilidade de os seus dados serem utilizados para diversos fins;



Consentimento

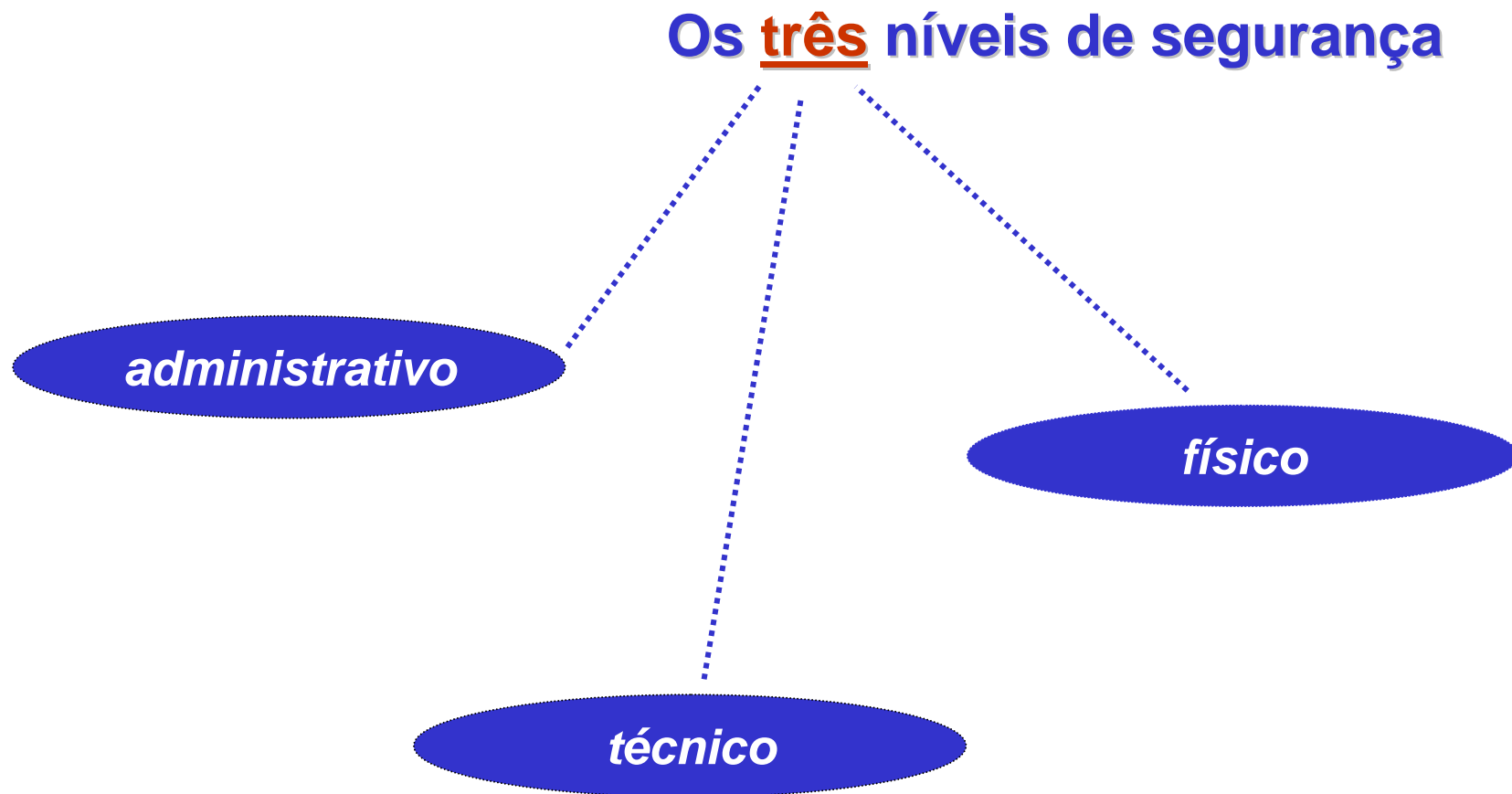
Enquanto anuência do utente para a recolha dos seus dados pessoais e uso dessa informação para efeitos de tratamento médico ou de pagamento de serviços médicos, ou outras necessidades de rotina, informação essa que tem uma duração ilimitada;



Autorização

Enquanto consentimento expresso do utente para a recolha dos seus dados pessoais e uso dessa informação para efeitos diversos dos anteriores, respeitante a procedimentos não rotineiros, informação essa que tem uma duração limitada.

HIPAA – 2.critérios de segurança da informação



HIPAA – 2.critérios de segurança da informação

Os três níveis de segurança



administrativo

Grosso modo, podemos dizer que implica:

- Procedimentos de prevenção, detecção, contenção e correcção de violações
- A identificação do responsável pelo controlo da gestão de informação
- A identificação de quem tem acesso à base de dados e a quem o mesmo está vedado
- Procedimentos para autorizar o acesso à informação clínica
- Procedimentos de rotina para garantir a segurança da informação (v.g., criação e alteração de *passwords*)
- Procedimentos a adoptar em situações de contingência (v.g., em casos de incêndio, vandalismo e outros)

HIPAA – 2.critérios de segurança da informação

Os três níveis de segurança



Grosso modo, podemos dizer que implica limitar:

- O acesso ao sistema electrónico que contém a informação clínica
- O acesso aos locais onde se encontram os terminais de acesso ao sistema electrónico.

HIPAA – 2.critérios de segurança da informação

Os três níveis de segurança

**Implica procedimentos
limitativos do acesso à
informação clínica,
tais como:**

técnico

- Nome ou número únicos para identificação do utilizador;
- Procedimentos electrónicos de protecção da informação em situações de emergência;
- Encerramento das sessões após um dado período de tempo ou de inactividade no acesso;
- Procedimentos de encriptação da informação;
- Sistemas de controlo que permitam verificar qual a actividade no sistema de informação e mecanismos que permitam garantir que a informação clínica não foi destruída ou alterada;
- Procedimentos de identificação do utilizador do sistema para que tenha acesso ao mesmo apenas quem esteja para tal autorizado;
- Medidas de segurança na transmissão de informação de modo a impossibilitar a sua apropriação ou alteração.

HIPAA – 3.responsabilização pelo incumprimento

Prevê a aplicação de sanções pecuniárias e sanções penais.

Respeitam às situações em que a violação dos direitos dos utentes resulta do desconhecimento ou negligência.

Serão aplicáveis em situações de violação intencional dos direitos dos utentes, com obtenção de benefícios pessoais pelo prevaricador.

Não contém disposições que prevejam a possibilidade de processar o infractor por danos, todavia, tal será sempre possível de acordo com a lei geral.

Conclusões

O interesse público reclama a partilha de um conjunto de informações, por razões diversas.

O ordenamento jurídico português contém disposições legais que permitem acautelar os interesses individuais em matéria de protecção de dados pessoais. Tal resulta da lei de protecção de dados pessoais, a Lei n.º 67/98, de 26 de Outubro.

Todavia, não existe legislação específica respeitante à recolha e centralização de informação clínica, com benefícios expectáveis na “melhoria dos cuidados prestados através da disponibilização de melhor e mais rápida informação, independentemente do local onde esta se encontre, por uma maior facilidade de acesso aos cuidados de saúde”, e ainda, “evitando a duplicação de alguns exames complementares” assim como “desnecessárias deslocações dos utentes” e “diminuindo a demora no atendimento dos doentes”(IGIF).

Em sede de recomendações do Relatório de Auditoria ao Tratamento da Informação de Saúde nos Hospitais a CNPD reflecte a necessidade de a Assembleia da República se pronunciar sobre as limitações ao *direito de acesso*, assim como sobre a disponibilização de dados clínicos para investigação científica.

Podemos pois concluir que, identificadas as vantagens e as dificuldades de implementação de um sistema de informação em saúde, mormente pela ausência de disposições legais susceptíveis de acautelar todos os interesses em presença, o Sistema de Garantia de Privacidade e Segurança Americano nos oferece elementos bastantes para a implementação, por via legislativa, de um sistema similar em Portugal, o que de facto vivamente se recomenda.