



UNIVERSIDADE FEDERAL DE SÃO PAULO
1933 - 2008

Departamento de Informática em Saúde Universidade Federal de São Paulo – UNIFESP

Sessão Oral #28– Auditório VAIL - 3/12

Revisão sobre Normas e Padrões de Segurança da Informação para o Registro Eletrônico em Saúde

Heitor Gottberg¹, Thiago Martini da Costa², Beatriz de Faria Leão³, Ivan Torres Pisa⁴

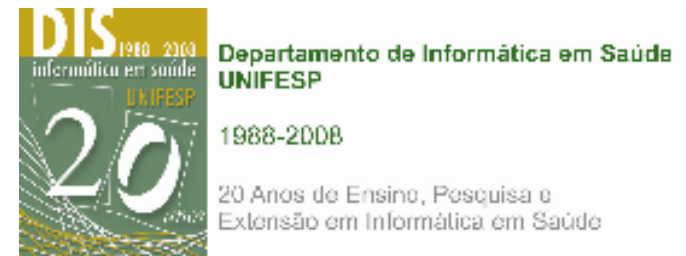
¹ Programa de Pós-graduação em Saúde Coletiva, Universidade Federal de São Paulo (UNIFESP)

² Programa de Pós-graduação em Informática em Saúde, UNIFESP

³ Zilics Sistemas de Informação em Saúde, Brasil

⁴ Departamento de Informática em Saúde, UNIFESP

E-mail: heitor@cisco.com



Introdução

- ✓ Em Novembro de 2007, foi publicado no Diário Oficial da Resolução 1821/07 que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde¹.

Mais um passo na viabilização do aumento do uso dos Sistemas de Registro Eletrônico em Saúde

- ✓ Em Agosto de 2002, o Centro Médico de Administração dos Veteranos dos EUA, em Indianópolis, vendeu ou doou 139 computadores sem remover dados confidenciais, incluindo nomes de pacientes de AIDS e doenças mentais².
- ✓ Em Maio de 2006 um artigo de jornal denunciou que uma falha nos computadores pode ter levado ao roubo de dados referentes a 60.000 pacientes que visitaram o Centro Médico da Universidade de Ohio².

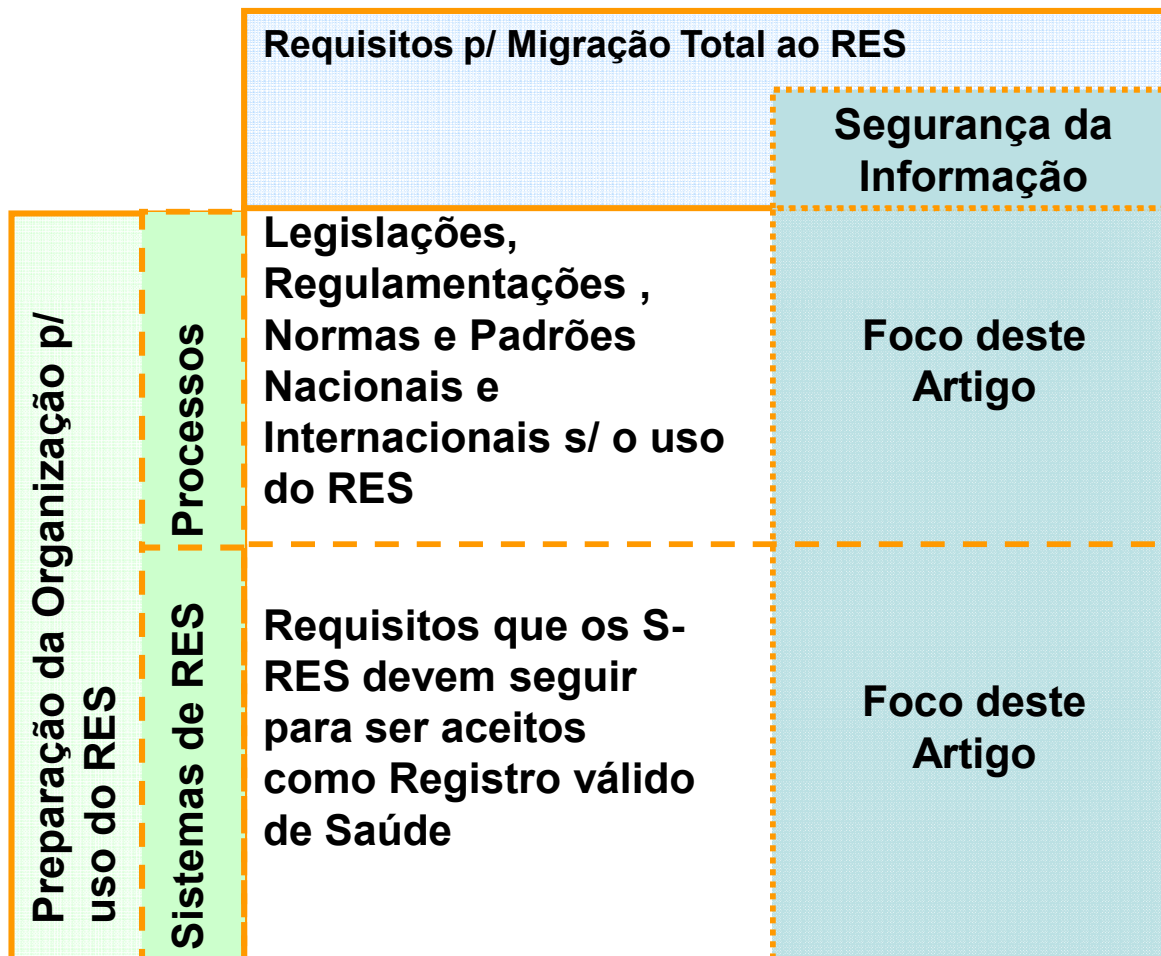
Os dados nos S-RES e nas instituições que os utilizam estão seguros?
Quais as Normas, Padrões e Legislações Nacionais e Internacionais que guiam a segurança da informação em Saúde?

1. Conselho Federal de Medicina (CFM), Resolução CFM Nº 1.821, Diário Oficial da União; Poder Executivo, Brasília, DF, 23 nov. 2007. Seção I p. 252. (cerca de 6 páginas) disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.htm.2007.

2. Hoffman S, Podgurski A, "In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information"; disponível em: <http://ssrn.com/abstract=931069>. 2006.

Método

✓ A Segurança da Informação tem que contemplar Processos em um Sistema de Gestão da Segurança da Informação e a Segurança dos Sistemas de RES.



- ✓ Para atingir o mapeamento estudou-se as normas o que há de Segurança da Informação em:
- Conselho Federal de Medicina (CFM),
 - Sociedade Brasileira de Informática em Saúde (SBIS).
 - United States Department of Health and Human Services (US-HHS).
 - International Organization for Standardization (ISO).
 - Associação Brasileira de Normas Técnicas (ABNT).
 - Instituto Health Level 7 (HL7).

Resultado

✓ International Organization for Standardization (ISO) e Associação Brasileira de Normas Técnicas (ABNT).

✓ Para suportar a definição dos controles de segurança em TI, a ISO desenvolveu a norma ISO/IEC 27002^{1]} – hoje já com sua versão brasileira a NBR ISO/IEC 27002:2005^{2]}

✓ A ISO formou o comitê técnico TC 215 Health Informatics – para debater as especificidades das demandas do segmento de saúde, propondo padrões específicos que atendam às características da prestação de serviços em saúde. Este publicou a ISO-DIS 27799 – Health informatics - Information security management in health using ISO/IEC 17799.

Passos p/ implementação de um SGSI

- 1) Criação de um plano de tratamento de risco
- 2) Alocação de Recursos

3) Selecionar e implementar controles de Segurança

- Controles podem ser encontrados em:

ISO 27002
Requisitos de
Segurança p/ o
mercado em geral

ISO 27799
Requisitos de
Segurança p/ o
Segmento de Saúde

- 4) Treinamento e Educação
- 5) Gerenciamento das operações
- 6) Gerenciamento dos recursos
- 7) Gerenciamento dos incidentes de segurança

1. ISO/IEC 27.002; Information technology - Security techniques -- Code of practice for information security management. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue-e_tc/catalogue_detail.htm?csnumber=50297. 2005

2. ABNT NBR ISO/IEC 27.002; Código de Prática para a Gestão da Segurança da Informação. Disponível em: <http://www.abntnet.com.br/ecommerce/default.asp>. 2005.

Resultado

- ✓ **Health Level 7 (HL7)**
- ✓ O HL7 é uma organização certificadas pelo ANSI (sigla para Institutos Nacionais Americanos de Padronização) operando na área de saúde em normas para dados clínicos e administrativos¹.
- ✓ Em Fevereiro de 2007 o Instituto HL7 editou o Modelo Funcional para S-RES (que fornece uma lista com mais de 160 funções que devem estar presentes em um S-RES¹).

Atendimento direto	<ol style="list-style-type: none"> 1. Gerenciamento do Atendimento 2. Suporte à Decisão 3. Gerenciamento das operações e comunicação
Suporte	<ol style="list-style-type: none"> 1. Suporte Clínico 2. Medição, Análise, Pesquisa e Relatórios 3. Administrativo e financeiro
Infra-estrutura de Informação	<ol style="list-style-type: none"> 1. Segurança 2. Registro de informação em saúde e gerenciamento 3. Registros e serviços de diretório 4. Terminologias padrão e serviços de terminologia 5. Interoperabilidade baseada em padrões 6. Gerenciamento das regras de negócio 7. Gerenciamento do fluxo de trabalho

Subitem da Subseção Segurança	Nr Critérios
Autenticação de Entidade	4
Autorização de Entidade	7
Controle de Acesso de Entidade	4
Gestão do Acesso do Paciente	1
Não-repudição	4
Intercâmbio Seguro de Dados	5
Roteamento Seguro de Dados	3
Validação da Informação	7
Privacidade e Confidencialidade do Paciente	10

1. HL7 Institute; 2007; HL7 - EHR-S Functional Model; disponível em: <http://www.hl7.org>

Resultado

✓ EEUU - HIPAA: Health Insurance Portability and Accountability Act

- ✓ Determina a padronização nas transações de dados entre provedores e pagadores dos serviços de saúde.
- ✓ Determina a existência de políticas para proteger e manter o acesso aos dados de pacientes e que também forneça aos clientes o direito de ter acesso à informação de como e por quem seus dados pessoais serão usados, permitindo aos mesmos inspecionar e possivelmente adicionar informações¹.

✓ A parte da HIPAA referente à privacidade e segurança (parte no. 164) estabelece os requisitos que a organização em saúde deve implementar e envolvem proteções nos âmbitos **administrativo, físico e técnico**.

✓ Na parte de segurança, uma atenção especial é dada à privacidade da informação identificada em saúde².

Proteções demandadas pela HIPAA	Nr. de Requisitos
Proteções administrativas	23
Proteções físicas	10
Proteções técnicas	9

1. Shortliffe E, Cimino J; Biomedical Informatics: Computer Applications in Health Care and Bio-medicine, 3rd Ed.; Springer Science+Business Media, LLC. 2006

2. US-HHS, HIPAA Administrative Simplification Regulation Text; United States Dept. of Health and Human Services disponível em: <http://www.hhs.gov/ocr/AdminSimpRegText.pdf>; .2006.

Resultado

- ✓ **Brasil – Resolução 1821/2007 / CFM – SBIS : Manual de Certificação de S-RES.**
- ✓ Resolução 1821/2007 regula o uso de métodos de digitalização de dados de pacientes e ou uso de S-RES com registro de informações de saúde de modo informatizado. Esta resolução aprovou o “Manual de Certificação para Sistemas de Registro Eletrônico em Saúde”, elaborado em convênio com a Sociedade Brasileira de Informática em Saúde (SBIS)¹.

Requisitos p/ os
S-RES

1. Segurança

- Requisitos para Nível de Garantia de Segurança 1 (NGS1)
- Requisitos para Nível de Garantia de Segurança 2 (NGS2)

- 2.1 Requisitos de Estrutura e Conteúdo
- 2.2. Requisitos de Funcionalidades
- 3. Requisitos TISS (ANS)

S-RES certificados no **NGS1** estão autorizados a serem usados para prestação de serviços de saúde.

S-RES certificados no **NGS2** permitem às organizações em saúde a manter e usar os dados médicos e de pacientes exclusivamente em formato eletrônico.

1. Leão B, Costa C, Forman J, Silva M, Galvão D (ed); Manual de Certificação para Sistemas de Registro Eletrônico em Saúde Manual versão 3.1; disponível em: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS_CFM_Fase2_v3.1_Consulta_Publica.pdf.; 2008

Resultado

✓ **Brasil – Resolução 1821/2007 – Manual de Certificação de S-RES¹.**

Nível de Gestão Segurança 1

Categoria	No. de Requis.
Controle da Versão do Software	4
Identificação e Autenticação de Usuário	5
Controle de Sessão de Usuário	2
Autorização e Controle de Acesso	9
Disponibilidade do RES	2
Comunicação Remota	6
Segurança de Dados	8
Auditoria	4
Documentação	8
Tempo	2
Notificação de Ocorrências	1

Nível de Gestão Segurança 2

Categoria	No. de Requisitos
Certificação Digital	4
Assinatura Digital	8
Autenticação de Usuário Utilizando Certificado Digital	4
Digitalização de Documentos (apenas para S-RES da categoria GED-Gestão Eletrônica de Documentos)	9

1. Leão B, Costa C, Forman J, Silva M, Galvão D (ed); Manual de Certificação para Sistemas de Registro Eletrônico em Saúde Manual versão 3.1; disponível em: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS_CFM_Fase2_v3.1_Consulta_Publica.pdf; 2008

Conclusões

- 1. Há material e conhecimento desenvolvido para suportar a migração para a saúde digital no que diz respeito à segurança da informação. As principais normas brasileiras e internacionais, como ISO, HL7, SBIS/CFM e ANS, dedicam um foco especial ao tema.**
- 2. A preparação para a eliminação do papel na atenção à saúde passa pela escolha de S-RESs que sejam certificados, mas também por uma preparação organizacional com o estabelecimento de um SGSI que faça com que os processos da organização sejam também seguros o suficiente para a prestação de serviços em saúde.**

Pergunta para Debate

“Quão preparadas estão nossas instituições de saúde para garantir a segurança da informação digital?”

Revisão sobre Normas e Padrões de Segurança da Informação para o Registro Eletrônico em Saúde

Heitor Gottberg¹, Thiago Martini da Costa², Beatriz de Faria Leão³, Ivan Torres Pisa⁴

¹ Programa de Pós-graduação em Saúde Coletiva, Universidade Federal de São Paulo (UNIFESP)

² Programa de Pós-graduação em Informática em Saúde, UNIFESP

³ Zilics Sistemas de Informação em Saúde, Brasil

⁴ Departamento de Informática em Saúde, UNIFESP

E-mail: heitor@cisco.com

Agradecimentos:

Luiz Kiatake : ABNT – CEE em Informática em Saúde – GT 4 – Segurança
UNIFESP – Dept. de Informática em Saúde – Setor de Tecnologia da Informação

