Tabela de controles comuns de SGSI para as normas ISO 2001, PCI-DSS 3.2 e HIPAA usando a HIPAA como base

ISO 27001	PCI-DSS 3.2	HIPAA	Descrição	Coberto (total ou parcialmente) pela implementação do controle	Detalhes de implementação na camada do banco de dados	Detalhes de implementação na camada do aplicativo web	MS SQL Server 2016	.NET Core +2.0 (ASP.NET MVC C#)
		Controles basicos						
		§ 164.308 (a)(1)(i)	Exige implementação de politicas e procedimentos relacionados a detecção, prevenção e correção de violações de segurança	Audit Controls Standard – § 164 .312(b)				
		§164.308(a)(1)(ii)(D)	Exige que a solução implementada permita inspeção regular dos logs de auditoria, relatórios de acesso e registro de incidentes	Audit Controls Standard – § 164 .312(b)				
A.7.1.3 Uso aceitável dos ativos	Implement Strong Access Control Measures Requirement 7: Restrict access to cardholder data by business need	§164.308(a)(3)(ii)(B)	Exige que os procedimentos implementados garantam que o acesso do funcionário ao ePHI armazenado	Audit Controls Standard – § 164 .312(b)				

	to know		é apropriado					
A.7.1.3 Uso aceitável dos ativos A.8.3.3 Retirada de direitos de acesso A.11.2.1 Registro de usuário	Implement Strong Access Control Measures Requirement 7: Restrict access to cardholder data by business need to know	§164.308(a)(3)(ii)(C)	Exige que a solução implementada garanta que todo acesso do funcionário ao ePHI, que está definido no parágrafo (a)(3)(II)(B), quando este deixa a organização seja revogado		Implementar triggers de banco de dados na tabela de funcionários do banco ERP para baixa automática dos logins relacionados a funcionários desligados **OU** Utilizar a API do ERP para baixa automática dos logins relacionados a funcionários desligados	n/a	Table triggers (quando o acesso direto ao DB do ERP é possível) [101] **OU** Compiled Stored Procedures (para acesso a API do ERP) [102]	

		§164.308 (a)(4)(i)	Todo acesso ao ePHI deve ser autorizado e todas as politicas e procedimentos devem ser consistentes com os requerimentos aplicaveis definidos na CFR 45 parte 164, subsessão E	Access Control Standard – §164 .312(a)(1)				
		§164.308 (a)(4)(ii)(A)	Uma empresa que é subordinada de um conglomerado maior deve implementar políticas e procedimentos para proteger o acesso aos ePHI da sua organização controladora	Access Control Standard – §164 .312(a)(1)				
		§164.308(a)(4)(ii)(C)	Implementar políticas e procedimentos criados de acordo com políticas de autorização de acesso, e permite controle completo dos direitos de	Access Control Standard – §164 .312(a)(1)				

			usuário ao ePHI					
		§164.308(a)(5)(ii)(C)	Todas as tentativas de login devem sem registradas e procedimentos de relatório para detectar discrepâncias devem ser estabelecidos	Access Control Standard – §164 .312(a)(1)				
		§164.308(a)(5)(ii)(D)	Todos ao eventos de criação e troca de senhas devem ser auditados e revisados	Audit Controls Standard – § 164 .312(b)				
		§164.308(a)(6)(i)	Todos os incidentes de segurança devem ser registrados, revisados e endereçados	Audit Controls Standard – § 164 .312(b)				

A.5.1.1 Documento da política de segurança da informação A.5.1.2 Análise crítica da política de segurança da informação A.10.1.1 Documentação dos procedimentos de operação A.10.7.4 Segurança da documentação dos sistemas		§164.308(a)(6)(ii)	Estabelecer procedimentos que permitam identificar e apropriadamente responder a suspeitos/conhecidos incidentes de segurança incluindo documentar/revisar todos os incidentes e suas consequências	Audit Controls Standard – § 164 .312(b) Padrões de documentação física e eletrônica	Implementar documentação completa em meio fisico com acesso restrito **E** em formato digital em repósitório específico para políticas de segurança **REQUISITO** O meio físico deve ter acesso auditado e não conter senhas ou chaves E O meio digital deve ser auditado por política de acesso específica		(Externo ao SQL Server) Guarda de documentação em depósito com controles específicos ou datacenter em cofre separado do cofre do meio de backup magnético se houver **E** File Server com permíssões ACL estritas ao pessoal responsável pela operação do banco e aplicativo somente, com auditoria de acesso para leitura, criação, alteração e exclusão dos arquivos	
		§164.308(a)(7)(ii)(B)	Estabelecer e implementar procedimentos que permitam recuperar qualquer perda de informação do ePHI armazenado	Integrity Standard – § 164 .312(c)(1)				

		Controles principais						
		Controle de acesso						
A.10.4.1 Controle contra códigos maliciosos (ver implementação da camada do aplicativo) A.11.1.1 Política de controle de acesso A.11.2.3 Gerenciamento de senha do usuário A.11.2.4 Análise crítica dos direitos de acesso de usuário	Implement Strong Access Control Measures Requirement 8: Identify and authenticate access to system components Maintain a Vulnerability Management Program Requirement 6: Develop and maintain secure systems and applications (ver implementação da camada do aplicativo)	Access Control Standard – §164 .312(a)(1)	Política de identificação e autorização		Autorização do SQL Server: Papéis únicos por funcionário identificado unicamente com a tabela de funcionários do ERP **OU** Autorização integrada do Windows: Logins do AD em grupo auditado por GPO específico de acesso ao ePHI **REQUISITO** §164.308(a)(3)(ii)(C)	Implementar a autenticação de usuário baseada em forms ou integrada com AD **REQUISITO** Implementar salva de senhas de usuário em criptografia de mão única (SHA-512 mais SALT ou superior) **E** Implementar criptografia de dados de sessão (AES-256 ou superior) **E** Implementar dois fatores de segurança (certificado, sms ou token de aplicativo)	Windows Active Directory Authentication **OU** SQL Server Authentication and Authorization [103]	.NET Core Identity Framework (Este padrão de autenticação cobre todos os requisitos especificados em "plataforma") [104] **OU** Personificar o usuário de domínio do Windows na aplicação (AD sobre LAN ou VPN) [103]

A.11.2.2 Gerenciamento de privilégios	Implement Strong Access Control Measures Requirement 7: Restrict access to cardholder data by business need to know	Unique User Identification Specification – Required §164 .312(a)(2)(i)	Exige que todo login de acesso seja único para identificação e registro de identidade		Exigir a personificação do papel de usuário especifico do funcionário após a conexão com usuário padrão do aplicativo web com privilégio mínimo **OU** Implementar autenticação integrada (AD)	Exigir a personificação do papel de usuário especifico do funcionário após a conexão com usuário padrão do aplicativo web com privilégio mínimo **OU** Implementar autenticação integrada (AD)	Windows Active Directory Authentication **OU** SQL Server Authentication and Authorization **REQUISITO** implementar permissão mínima no usuário de conexão e permissões granulares nos usuários de funcionários	.NET Core Identity Framework **OU** Personificar o usuário de domínio do Windows na aplicação (AD sobre LAN ou VPN) **REQUISITO** O aplicativo deve conectar ao banco com privilégio mínimo e personificar o usuário específico do funcionário para operar o ePHI

		Emergency Access Procedure Specification – Required §164 .312(a)(2)(ii)	Política de acesso de emergência		Implementar meio de acesso de emergência ao mecanismo de dados	n/a	Emergency Access Policy (Pode ser usado o DAC ou Console de acesso direto administrativo) **E** SQL Server Audit **REQUISITO** As contas com acesso de emergência devem ser minimas para permitir redundância (ex: 2) e estarem sujeitas a política de auditoria padrão	n/a
		Automatic Logoff Specification – Addressable § 164 .312(a)(2)(iii)	Exige logoff automático de usuário		Implementar expiração de sessão	Implementar expiração de sessão no aplicativo	Windows Active Directory Group Policy Enforcement	Configure Session Timeout **REQUISITO** Essa política deve ser implementada independente do meio de autenticação

A.6.2.3 Identificando segurança da informação nos acordos com terceiros* A.12.5.4 Vazamento de informações* (*Always Encripted e o TDE funcionam em ambientes e nuvem) A.9.1.1 Perímetro de segurança física** (**TDE fornece data-at-rest encryption)	Protect Cardholder Data Requirement 3: Protect stored cardholder data	Encryption and Decryption Specification – Addressable § 164 .312(a)(2)(iv)	Política de criptografia e decriptografia		Implementar criptografia de colunas com chave externa ao mecanismo de banco de dados **OPCIONAL** Usar criptografia transparente no banco inteiro	Configurar aplicativo para utilizar chave externa na conexão para possibilitar leitura das colunas criptografadas	Always Encrypted[108] para criptografia de ponta-a-ponta em registros sensíveis; TDE[109] Para criptografia transparente	Configurar Connection String do aplicativo para usar chave externa de decriptografia[108]

	Protect Cardholder Data Requirement 4: Encrypt transmission of cardholder data across open, public networks	Person or Entity Authentication Standard – § 164 .312(d)	Política de identificação	Access Control Standard – §164 .312(a)(1)	Usar somente TLS1.2	Usar somente TLS1.2	SQL Server Password Policy **OU** Domain Password Policy Enforcement **REQUISITO** Transport Layer Security (TLS\SSL) Enforcement [106]	Configurar o servidor de aplicativo para recusar conexões que não satisfaçam requisitos mínimos de segurança [105] **REQUISITO** Transport Layer Security (TLS\SSL) Enforcement [105]
		Auditoria e conformidade						
A.10.10.1 Registros de auditoria A.10.10.2 Monitoramento do uso do sistema A.10.10.4 Registros (log) de administrador e operador A.10.10.5 Registros (logs) de falhas	Regularly Monitor and Test Networks Requirement 10: Track and monitor all access to network resources and cardholder data	Audit Controls Standard – § 164 .312(b)	Exige implementação de auditoria contínua do armazenamento de dados com mecanismos que registrem e reportem atividades nos armazens que contém ou usam dados do ePHI		Implementar auditoria e logins, alteração de privilégios e uso de dados **OPCIONAL** Habilitar a auditoria de alteração de registros	Implementar auditoria de uso de recursos e comportamentos não relacionados a dados (não cobertos pela auditoria de banco)	SQL Server Audit [112] **E** Policy-Based Management **OPCIONAL** Change Data Capture **OU** Table DML Triggers [101]	Entity Frramework Functions mapeando SQL Server Procedures criadas especificamente para auditoria

		Integridade de dados						
A.10.5.1 Cópias de segurança das informações A.10.4.1 Controle contra códigos maliciosos A.12.2.1 Validação dos dados de entrada A.12.2.2 Controle do processamento interno A.14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	Maintain a Vulnerability Management Program Requirement 6: Develop and maintain secure systems and applications	Integrity Standard – § 164 .312(c)(1)	Implementar auditoria contínua do armazenamento em todas as atividadesrelativas ao ePHI, para protegê-lo de tentativas impróprias de alteração ou deleção	Audit Controls Standard – § 164 .312(b)	Implementar auditoria de alteração de objetos e banco **E** Estabalecer designs consistentes de banco de dados aderentes a modelagem formal de R-DB's **E** Estabelecer baselines de performance e procedimentos de tunning **E** Estabelecer meios de backup automático encriptado e distribuído geograficamente	Isolar completamente a camada de interação do usuário da camada de acesso a dados por meio de modelos ou procedimentos de banco fortemente tipados	Database DDL Triggers **E** Database and Application Development Standards and Guidelines; Constraints, Triggers and Referential Integrity **E** Database Performance Collection **E** Database Backups **OU** Azure Encrypted Backup	Usar modelo Entity Framework **OU** Modelo Database-first/Code-First **REQUISITO** Usar modelos (classes) numa abordagem estrita MVC (Modelo-View-Controle) [111] **E** Usar somente LINQ [112] para todas as consultas (joins, searchs, order bys, etc) **OU** Encapsular as regras de negócio em procedimentos fortemente tipados e mapear em funções dentro do Entity Framework

A.9.2.3 Segurança do cabeamento A.12.2.3 Integridade de mensagens	Protect Cardholder Data Requirement 4: Encrypt transmission of cardholder data across open, public networks	Mechanism to authenticate ePHI Specification – Addressable § 164 .312(c)(2)	Mecanismo de autenticação		Criptografia de ponta-a-ponta para pacotes (Full over the wire encryption)	Criptografia de ponta-a-ponta para pacotes (Full over the wire encryption)	Enforce Minimun Transport Layer Security (TLS\SSL) Standard to TLS1.2 [106]	Enforce Minimun Transport Layer Security (TLS\SSL) Standard to TLS1.2 to SQL Server [106] & Enforce Minimun Transport Layer Security (TLS\SSL) Standard to TLS1.0 to Clients [105]
		Comunicações seguras						
A.10.8.4 Mensagens eletrônicas A.10.9.1 Comércio eletrônico A.10.9.2 Transações on-line	Protect Cardholder Data Requirement 4: Encrypt transmission of cardholder data across open, public networks	Transmission Security Standard – § 164 .312(e)(1)	Padrão de transmissão segura	Mechanism to authenticate ePHI Specification – Addressable § 164 .312(c)(2)	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para conexão	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para acesso a dados E Requerer criptografia de chave forte para acesso de cliente web	Use only TLS1.2 [106]	Use only TLS1.2 on data acess [106] **E** Enforce minimun SSL requiriments on IIS [105]

A.10.8.4 Mensagens eletrônicas A.10.9.1 Comércio eletrônico A.10.9.2 Transações on-line	Protect Cardholder Data Requirement 4: Encrypt transmission of cardholder data across open, public networks	Integrity Controls Specification – Addressable § 164 .312(e)(2)(i)	Padrão de integridade de controles	Mechanism to authenticate ePHI Specification – Addressable § 164 .312(c)(2)	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para conexão	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para acesso a dados E Requerer criptografia de chave forte para acesso de cliente web	Use only TLS1.2 [106]	Use only TLS1.2 on data acess [106] **E** Enforce minimun SSL requiriments on IIS [105]
A.12.3.1 Política para o uso de controles criptográficos	Protect Cardholder Data Requirement 4: Encrypt transmission of cardholder data across open, public networks	Encryption Specification – Addressable § 164 .312(e)(2)(ii	Padrão de criptografia	Mechanism to authenticate ePHI Specification – Addressable § 164 .312(c)(2)	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para conexão	Desabilitar todos os protocolos (TLS/SSL) exceto TLS1.2 para acesso a dados E Requerer criptografia de chave forte para acesso de cliente web	Use only TLS1.2 [106]	Use only TLS1.2 on data acess [106] **E** Enforce minimun SSL requiriments on IIS [105]
		Controles adicionais						
		§164.316(b)(1)(ii)	Manter um registro físico ou digital de quem, como e de onde audita o ePHI		Implementar grupo auditado de banco de dados para usuários com acesso a tabelas de auditoria	n/a	SQL Server Audit [113]	n/a

A.10.10.3 Proteção das informações dos registros (logs) A.15.3.2 Proteção de ferramentas de auditoria de sistemas de informação		§164.316(b)(2)(i), §164.316(b)(2)(ii), §164.528(a)	Garantir o arquivamento seguro dos registros de segurança por 6 anos apartir da sua data de criação e permitir que esses registros sejam disponíveis de maneira imediata		Provisionar hardware fisico OU Serviço de nuvem elástico para 6 anos de crescimento das tabelas de auditoria	n/a	Provisionar recursos para crescimento dos arquivos de dados específicos de auditoria no servidor local ou serviço do Azure por 6 anos **OPCIONAL** Habilitar recurso auto-growth para estes arquivos se não houverem métricas seguras para 6 anos	n/a
		Não enquadrados, mas potenciais controles baseados em						
		§164 .312(a)(1), §164 .312(a)(2)(i)			Desabilitar recurso "phone home" e telemetria do mecanismo de dados	Desabilitar telemetria do servidor	Configuração de registro [115]	Configuração de aplicativo
		§164 .312(a)(1), §164 .312(a)(2)(i)			Implementar superfície mínima de ataque na instalação		Procedimento de instalação da instância [114]	Procedimento de publicação

		§164 .312(a)(1), §164 .312(a)(2)(i)			Implementar permisões mínimas de usuário para as contas de serviço usadas na instalação		Procedimento de instalação da instância [114]	Procedimento de publicação