

1



• **Agenda**

- Housekeeping
- Agenda Overview & Meeting Introductions
- About HFS
- Development Status
- Security – Chuck Briggs
- Top Ten – Don Fry
- Training
- Fees & Contract Issues

- **CPE Plan**
- **Schedule**
- **Handouts**
- **Questions**

3

- Small Company in Elk Grove, CA.
- 39 years experience making MCR software.
- HFS makes Medicare Cost Reporting software for Hospitals, Skilled Nursing Facilities, Home Health Agencies, CMHC, RHC, FQHC, ESRD, Hospice, Home Office and OPO.
- SaFE Website, HCRIS Website, IRIS Database software and ProPapers
- Specialized Reporting for – CA, NY, MA and VA

12/2/2021

4

4

- So far this year we have issued 10 Updates and 34 Patches.
- All of our systems have been updated to our current developing language.
- We have started the conversion to upgrade to the latest version.

12/2/2021

5

5

- **SaFE**
 - Processed and Stored 27,979 provider submissions.
 - 19,750 or 71% were electronically signed
- **HCRIS**
 - 1,300,000 MCR reports
 - Upgrade in 2022
- **HFS Plus – Partnership Developing MCR Wokpaper Product**



12/2/2021

6

6



7



- 1 Background
- 2 HITRUST
- 3 Assessment Process
- 4 HFS Status
- 5 Questions



2010 - HFS adopted security policies designed to be compliant with the HIPAA Security Rule and related regulations.



12/2/2021

Health Financial Systems

9

9

- HFS expanded its security policies to include applicable controls from the NIST CSF. (NIST 800-53)



12/2/2021

Health Financial Systems

10

10

- HFS security policy requires and includes ongoing training.
- Sometimes the training consists of a live presentation on one or more security topics.
- Other times the training material is delivered online and is followed up by a quiz.
- We have security knowledge assessments.
- We subscribe to a service that allows us to send fake phishing emails to all employees. There are new emails each month. This really helps with awareness.

12/2/2021

Health Financial Systems

11

11

HFS started receiving lots of computer security questionnaires from clients. Vendor/Third Party Risk Management was becoming a very prevalent issue for clients.



12/2/2021

Health Financial Systems

12

12

HFS wanted to undergo a formal assessment and obtain a report we could share with clients that would confirm our security posture.

HFS considered ISO 27001, SOC1, SOC2 and several other assessments/certifications.

HFS chose HITRUST.

- **HITRUST Cybersecurity Framework (CSF)**



- Designed for healthcare organizations and their business associates, HITRUST offers organizations a flexible way to meet Health Insurance Portability and Accountability Act (HIPAA) compliance standards.

- HITRUST CSF was originally created as a set of safeguards for protecting the security and privacy of protected health information (PHI) and electronic PHI (ePHI).
- HITRUST CSF was originally based on the ISO 27001. It has evolved to include almost all major cybersecurity laws, regulations and CSFs.

The CSF v9.4.2 integrates 44 major security and privacy related standards, regulations, and frameworks:

- 16 CFR Part 681 – Identity Theft Rules [16 CFR 681]
- 201 CMR 17.00 – State of Massachusetts Data Protection Act [201 CMR 17.00]
- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, 2017 [AICPA TSP 100]

- Asia-Pacific Economic Cooperation (APEC) Privacy Framework, 2005 [APEC]
- California Consumer Privacy Act (CCPA) [CCPA 1798]
- CAQH CORE Phase 1 [CAQH Core Phase 1]
- CAQH CORE Phase 2 [CAQH Core Phase 2]
- Center for Internet Security (CIS) Critical Security Controls (CSC) [CIS Controls v7.1]

- Cloud Security Alliance (CSA) Cloud Controls Matrix Version 3.0.1 [CSA CCM v3.0.1]
- CMS Information Security ARS 2013 v3.1: CMS Minimum Security Requirements for High Impact Data [CMS ARS v3.1]
- COBIT 5: Deliver and Support Section 5 – Ensure Systems Security [COBIT 5]
- Department of Defense (DoD) Cybersecurity Maturity Model Certification [CMMC v1.0]
- Department of Homeland Security (DHS) Critical Resilience Review (CRR) v1.1 [DHS CISA CRR (2016)]

- Electronic Health Network Accreditation Commission (EHNAC) [EHNAC]
- Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures, 2003 [21 CFR 11]
- General Data Protection Regulation (GDPR)
- OCR Guidance for Unsecured PHI
- Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook, September 2016 [FFIECIS]

- Federal Risk and Authorization Management Program [FedRAMP]
- Health Information Trust Alliance (HITRUST): [HITRUST De-ID Framework v. 1]
- HIPAA – Federal Register 45 CFR Part 164, Subpart C (Security Rule) [45 CFR HIPAA.SR]
- HIPAA – Federal Register 45 CFR Part 164, Subpart D (Breach Notification Rule) [45 CFR HIPAA.BN]
- HIPAA – Federal Register 45 CFR Part 164, Subpart E (Privacy Rule) [45 CFR HIPAA.PR]

- IRS Publication 1075 v2016: Tax Information Security Guidelines [IRS Pub 1075 (2016)]
- ISO/IEC 27001:2013: Information Technology – Information Security Management Systems [ISO/IEC 27001:2013]
- ISO/IEC 27002:2013: Information Technology Security Techniques Code of Practice for Information Security Controls [ISO/IEC 27002:2013]
- ISO/IEC 27799:2016: Health Informatics – Information Security Management in Health using ISO/IEC 27002 [ISO/IEC 27799:2016]

- ISO/IEC 29100:2011: Information Technology – Privacy Framework [ISO/IEC 29100:2011]
- ISO/IEC 29151:2017: Information Technology – Code of Practice for PII [ISO/IEC 29151:2017]
- Minimum Acceptable Risk Standards for Exchanges: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges [MARS-E v2]
- New York State Department of Financial Services – [23 NYCRR 500]

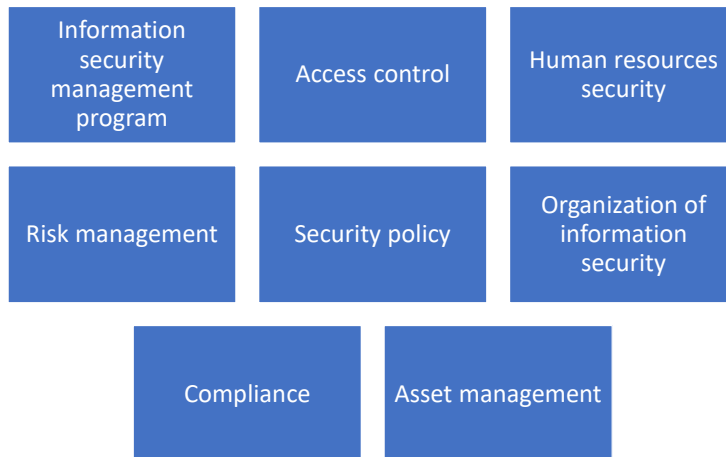
- NIST Cybersecurity Framework v1.1
- NIST Special Publication 800-53 Revision 4 (Final), Security Controls for Federal Information Systems and Organizations [NIST SP 800-53 R4]
- NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [NIST SP 800-171 R2]
- State of Nevada: Security and Privacy of Personal Information [NRS 603A]
- NY DOH Office of Health Insurance Programs [NYS DOH SSP v3.1]

- Office of Civil Rights (OCR) [OCR Audit Protocol (2016)]
- Payment Card Industry (PCI) Data Security Standard Version 3.2.1[PCI DSS v3.2.1]
- Personal Data Protection Act 2012 [PDPA]
- South Carolina Insurance Data Security Act [SCIDSA 4655]
- Title 1 Texas Administrative Code § 390.2 – State of Texas: Standards Relating to the Electronic Exchange of Health Information [1 TAC 15 390.2]

- Each assessment is based on a scoping questionnaire – determines which laws and regulatory schemes are applicable.
- Assessments only include security controls based on each entities relevant characteristics.
- HFS current validated assessment includes 200+ distinct security controls based on a handful of applicable laws and regulations.



- The HITRUST CSF consists of 49 control objectives across 156 control specifications, all of which fall into one of the following 14 control categories:



12/2/2021

Health Financial Systems

27

27



12/2/2021

Health Financial Systems

28

28

HFS HITRUST Certifications

- Validated Assessment Completed – certification issued March 20, 2019



Letter of Certification

March 20, 2019

Health Financial Systems
8109 Laguna Blvd,
Elk Grove CA 95758

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF® Assessor to validate such information, and HITRUST®'s independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following systems and applications of the organization meet the HITRUST CSF v9.1 Certification Criteria:


12/2/2021

Health Financial Systems

29

29

Interim Assessment in 2020 – certification issued March 20, 2020



6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

March 20, 2020

Health Financial Systems
8109 Laguna Blvd
Elk Grove, CA 95758

Based upon the procedures performed by an Authorized External Assessor which indicated that there were no material changes to the control environment that would result in Health Financial Systems ("the Organization") no longer meeting certification criteria of the HITRUST® CSF Assurance Program, the following systems and supporting infrastructure of the Organization ("Scope") continue to meet the HITRUST CSF® v9.1 certification criteria:

12/2/2021

Health Financial Systems

30

30

- HFS is currently completing its validated assessment for 2021.
- Should be complete 30-60 days from now.

Questions & Comments

Chuck Briggs
chuckbriggs@hfssoft.com

Don Fry's Famous Top 10 List!

33

 Health Financial Systems

Fees & Contracts

- **Contract Issues**
- **Fee Increase as of 1/1/2022**

34

- **Continued WebEx Training on HFS software features – 10 Sessions – Offered twice per year.**
- **Transmittal Updates**
- **Guest Speakers**
- **Provider User Meeting**
- **Individual Meetings/Training/Presentations**
- **Next year Live**
- **Suggestions**

35

35

- **HFS Employees**
- **Our Fantastic Guest Speakers**
- **Our Users/Attendees**

36