CASE STUDY: IT CONTROLS AND COMPLIANCE

HAPPY LIFE INSURANCE

ASSIGNMENT OVERVIEW

Summary:	As a team, present the proposed solution to the case. The presentation should lay out clear recommendations for how management should address the problem. This case study is divided into two parts: 1. define, implement and test three organizational processes in a way that meets IT General Controls defined in Exhibit One, Two and Three, and 2. create a phased HIPAA compliance strategy and roadmap (and define two safeguard processes), with clearly defined projects to meet the safeguards defined in Exhibit Four, Five and Six. Each team should analyze both parts of the case but only one team will present each part. You only need to turn in the deliverables for your assigned part of the case.
Presentation Deliverable:	Case study presentation (in Microsoft PowerPoint format)**.**
Executive Briefing Deliverable:	Single page case study executive briefing (in Microsoft PowerPoint format).

BACKGROUND

Happy Life Insurance is a large, private insurance company based in New York and currently has 34 offices across the country. In the past decade Happy Life has grown exponentially. In the early 2000s Happy Life had two million members. This number now stands at over 40 million members. Happy Life's growth is primarily driven by deep, trusted relationships with their customers. Happy Life has a reputation for being an organization that truly cares about its members and is present during their time of need primarily driven by its regional offices that ensure a strong connection to the community and resident families.

Happy Life provides many different kinds of health insurance services:

1. *Individual and family plans* **–** Happy Life allows individuals or families to select one of three plans:

    - *Tier 3 plan* – In a tier 3 plan, Happy Life covers 50% of health care costs over a year. Monthly premiums are lower than other plans; families are encouraged to select this plan if they anticipate their healthcare needs to be very low.

- *Tier 2 plan* – In a tier 2 plan, Happy Life covers 75% of health care costs over a year. Monthly premiums are higher than a tier 3 plan, but still low enough for this to be affordable to most families. Year after year, this has proved the most popular package for Happy Life's members.
- *Tier 1 plan* – In a tier 1 plan, Happy Life covers 95% of health insurance costs over a year. Monthly premiums are high and very few members opt for this plan. However, Happy Life provides this plan for members that have high medical needs each year.

2. *Medicare solutions* – Happy Life is a private provider for Medicare insurance on behalf of the United States Government. About 20% of Happy Life's current members are over the age of 65, and enrolled in the Medicare package. Year on year loyalty is highest among this customer demographic due to the community connections that Happy Life representatives maintain.
3. *Dental and vision plans* – Happy Life provides dental and vision coverage as add-ons to individual and family plans. Happy Life covers the following percentages of cost for services (only for doctors within Happy Life's network):

    - *Cleanings, exams, x-rays* – Happy Life pays 100% of cost for one of each per year.
    - *Fillings* – Happy Life pays for 50% of the cost for one per year.
    - *Crowns, root canals, oral surgery* – Happy Life pays for 60% of the cost for one per year.
    - *Orthodontia* – Happy Life pays for 60% of the cost.
    - *Eye exams* – Happy Life pays for one eye exam per year.
    - *New frames* – Happy Life fully covers one new frame every two years. One additional frame is covered at 40% of cost.
    - *Standard lenses and contact lenses* – Happy Life fully covers one set of lenses every two years. One additional set of lenses is covered at 40% of cost.

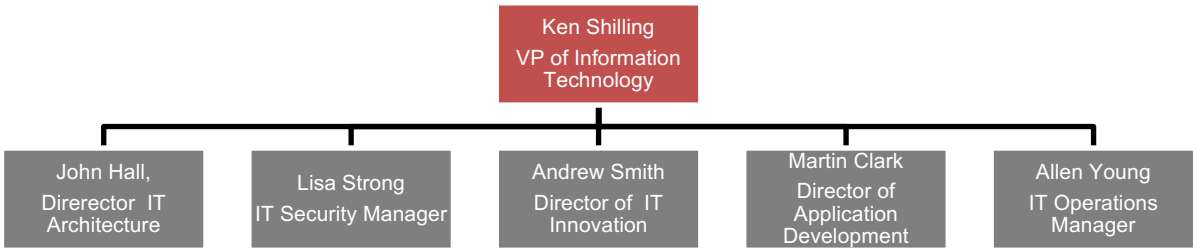
Happy Life provides members with the option to renew insurance coverage each year. Local representatives have a comprehensive database of their members, and launch campaigns every year so they can have personal conversations with each member prior to renewal. Such personalized service ensures a very low "drop-out" rate among Happy Life members. In fact, recent statistics show Happy Life has the lowest "drop-out" rate of any major health insurance provider.

Happy Life executives feel the company's tremendous, decade-long growth has reached its peak within USA and time is right for international expansion. To encourage an infusion of money to enable this international growth, Happy Life executives have decided to take the company public.

HAPPY LIFE'S IT ENVIRONMENT

Happy Life's IT organization consists of 150 employees primarily focused on supporting the growth Happy Life Insurance has experienced in the past decade. Systems and applications are all developed and supported with this growth in mind. Information security and compliance are, and have always been, secondary to growth. There is a general culture of ignoring security and compliance primarily due to funding constraints. Below is an organization chart of the Information Technology department:

Copyright © Justin Greis



Happy Life is an SAP-driven organization with some applications developed by the internal IT group that interface with the SAP system. All applications allow employees to connect via Windows workstations and laptops. Happy Life Insurance also has an external facing website where members can sign up for insurance coverage, change insurance coverage and obtain general information about Happy Life. This external website connects to a back-end Oracle database that stores information about all customers.

APPLICATION DEVELOPMENT

Happy Life has an internal application development group. This group specifically focusses on developing internal solutions and customizing existing applications, based on requirements defined by the business. Each application team is comprised of various developers and testers, and is led by a manager:

- *Developers* – Application developers respond to any new development requests or application changes requested by end users and/or managers. Once these requests have gone through an approval process from the respective application manager, developers act to develop the application or customize an already existing application. There are separate development environments and end user environments. Developers work in the development environment, which is an exact replica of the end user environment. Once an application is developed, the IT Operations team works to move it to the end user environment. Only a few developers have access to the end user environment to be able to make changes in the event of an emergency. However, there is no approval process for developers to make emergency changes, nor is there any documentation requirement for emergency changes.
- *Testers* – Testers are focused purely on testing the application from a usability perspective. Testers test the application in the development environment prior to it being migrated to the end user environment. There is no consideration for application security or secure coding in the test phase.
- *Managers* – Managers lead a team of developers. Generally, the teams are organized based on application. New application requests may be given to an existing development team, based on availability of the team. This is decided in an ad-hoc fashion. Minor system and application changes are made by the respective system and application teams. Managers are responsible for approving minor changes. Major changes need two levels of approval – first by the manager, and then by Martin, who is the Director of the Application Development group. Martin also approves new application requests. New application requests also need a second level of approval from Ken Shilling, the VP of Information Technology. There have been multiple instances in the past of development team rolling out a major application change without appropriate approvals, all in the interest of “helping the business”.

Copyright © Justin Greis

IT SECURITY

Happy Life's IT Security group is primarily focused on provisioning and de-provisioning access and monitoring access rights. Access to any new system or application is managed through Active Directory. Happy Life allows all users to select their own password; however, the password policy enforced is not strong enough as per industry standards. There are various roles that are part of the access provisioning and de-provisioning process at Happy Life Insurance:

- *End User* – End users request access through a centralized web-based system that lists out all applications. They can select the application, provide basic credential information and hit submit.
- *Supervisor* – All employees within Happy Life have a supervisor. When an employee requests access to a system, it is sent to their direct supervisor who can approve or deny. Once the supervisor approves, a second level of approval is required from the IT Security Manager.
- *IT Security Manager* – Once a supervisor approves the request for an application, the IT Security Manager receives this request for approval. If the IT Security Manager approves, they will also assign the user to the appropriate security groups within the application. When the user is assigned to the appropriate security groups and access is provisioned, the user and their supervisor receive an email confirmation.
- *HR Representatives* – When an employee leaves the organization the HR representative sends an email to the employee's supervisor. The supervisor can forward that email to the IT Security Manager who is responsible for de-provisioning access.

For role changes within the organization, Happy Life relies on a manual notification from the employee's supervisor to de-provision and re-provision access to the correct systems.

Administrator access to systems and applications follows the same process as regular access, and there are no specific considerations for administrator access to systems.

IT OPERATIONS

The IT Operations group primarily focusses on data backups, IT job scheduling and processing, and IT incident response via the helpdesk function.

Database operations – All critical data, such as financial data is backed up each night. Backups are stored in the primary data center. The system administrator verifies backups are done appropriately each day. In the recent years, there have been several issues with data backups. There have been multiple instances of failed backups and purging of backup logs. The system administrator has tried numerous times to resolve data backup issues, but with no success.

IT Helpdesk – Users can call a helpdesk number and open a ticket for any IT issue they encounter. When a user opens a ticket, they are directed to Level 1 IT support. Most tickets are resolved by level 1 support. Tickets that cannot be resolved by Level 1 support are forwarded to Level 2 IT support. The user receives an email from the IT helpdesk once the ticket is resolved.

Copyright © Justin Greis

CURRENT IT GENERAL CONTROLS ENVIRONMENT

The general culture within the IT department is to be extremely responsive to the business. Systems and applications do not have a heavy emphasis on IT security and IT general controls primarily due to Happy Life being a private company and was not required to meet SOX compliance requirements.

All of that is about to change.

Happy Life executives and senior employees have found that there are significant factors to consider as part of going public. One of the many important factors includes getting their IT General Controls implemented to meet Sarbanes Oxley (SOX) requirements.

Happy Life hired a Director of Compliance to build an internal compliance team that will report up to the VP of Information Technology. This team developed a compliance roadmap with an end goal to implement specific IT general controls. However, the IT controls this team identified were not mapped to relevant process flows. Moreover, the projects defined in their roadmap were extremely high level. As a result, executives did not feel comfortable that the team will be able to meet compliance by themselves. They decided at that moment time was right to call for external help and start from scratch. Happy Life executives hired you so they can hit the re-start button on their compliance journey. They want you to help them meet compliance with IT General Controls. They want you to define a detailed compliance roadmap which is clearly aligned with all IT General Controls (outlined in Exhibits One, Two and Three). They also want to ensure all controls are mapped to appropriate process flows, with clear definition of roles and responsibilities in the process flows.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Recently, a major competitor to Happy Life Insurance suffered a data breach. This breach made headlines nationwide and had severe financial and reputational impact on the competitor. Over 20 million customer records were stolen and industry estimates say the company will lose about 5% of its members as a result of this breach.

Seeing this breach so close to an Initial Public Offering (IPO) has concerned Happy Life executives. They don't want an IPO to be accompanied by news of a healthcare data breach. HIPAA recommends safeguards and industry-leading best practices for information protection of covered entities. This means HIPAA controls are specifically aimed to protect customer healthcare information. Happy Life executives want to ensure compliance to HIPAA security rule safeguards in addition to IT general controls. While being compliant with these safeguards does not mean absolute protection of information against breaches, it does provide Happy Life executives, employees and customers with an additional level of comfort that their information is less likely to be breached.

This also alleviates Happy Life executives' concerns of a potentially failed IPO. Happy Life executives have outlined the safeguards they want to be in compliance with in Exhibits Four, Five and Six. Happy Life executives are expecting a project plan to implement all HIPAA security safeguards. Happy life executives also want you to develop process flows for six safeguards (two from each exhibit noted above).

Copyright © Justin Greis

YOUR TASK FOR THIS CASE – PRESENTING TEAMS

Happy Life's executives want you and your team to help them with the following:

PART 1: IT GENERAL CONTROLS

The team assigned to present Part 1 for the case should address only the bullets below:

- *Draft control implementation plan* – Provide a detailed plan to implement each control objective in each process. Please include specific activities, timelines, cost and roles and responsibilities for performance of those activities in the project plan. A single project may be aligned to more than one control; however, make sure you show very clearly how the project helps Happy Life implement the control.
- *Draft a test plan to test each control objective* – Draft a test plan with detailed testing scenarios to test that the controls have been implemented. Please outline the test cases including any specific considerations for testing. A single test may be able to test more than one control; however, make sure you show very clearly how a test scenario helps Happy Life appropriately test the effectiveness of a control.
- *Design application change process* – Design a change control process to meet the control objectives outlined in Exhibit One. The process diagram should include swim lanes to outline responsibilities and clearly defined process steps. The process diagram should also clearly show how the process meets each control and helps Happy Life meet compliance requirements.
- *Design logical access process* – Provide a detailed access provisioning, de-provisioning and access change process to meet the control objectives outlined in Exhibit Two. The process diagram should include swim lanes to outline responsibilities, and clearly define all process steps. You may divide access provisioning, access de-provisioning and access changes into three different sub-processes if you wish. The process diagram should also clearly show how the process meets each control and helps Happy Life meet compliance requirements.
- *Design the IT operations processes* – Provide detailed IT operations processes to meet the controls objectives outlines in Exhibit Three. Please include swim lanes to outline responsibilities and clearly defined process steps. The process diagram should also clearly show how the process meets each control and helps Happy Life meet compliance requirements.
- *Outline control objective risks* – For all control objectives outlined in Exhibits One, Two and Three, please describe the risk to Happy Life in case they don't meet a specific control objective.

PART 2: THE ROAD TO HIPAA COMPLIANCE

The team assigned to present Part 2 for the case should address only the bullets below:

- *Draft security safeguard implementation plan* – Provide a detailed plan to implement all HIPAA safeguards. Please include specific activities, timelines, cost and roles and responsibilities for performance of those activities in the project plan. A single project may be aligned to more than one control; however, make sure you show very clearly how the project helps Happy Life satisfy the control.
- *Develop detailed process flow* – Select any two physical, five administrative and five technical safeguards from all HIPPA safeguards (defined in Exhibit Four, Five and Six) and develop a detailed process flow. The process flow should include swim lanes to outline responsibilities and

Copyright © Justin Greis

clearly define all process steps. Please also ensure process flows do not conflict with IT General Control process flows.

- *Outline HIPAA safeguard risks* – For all HIPAA safeguards please outline the risk to Happy Life in case they don't meet a specific safeguard.
- *Develop breach notification process* – Please develop a detailed breach notification process as per HIPAA breach notification requirements outlined in Exhibit Seven. The notification process should account for notifications to all parties as required by HIPAA. This process should take into account the various roles and responsibilities within Happy Life through swim lanes and not be in conflict with any other processes that you develop as part of this case study.

WORKING TOGETHER

The groups working on parts 1 and 2 may, but do not have to, work together to solve this case. Because there are two separate presentations, each team's solutions are not required to be coordinated; however, you may decide to do so if you choose.

YOUR TASK FOR THIS CASE – ALL OTHER TEAMS

CASE STUDY EXECUTIVE BRIEFING

Due to the importance of having a well-defined IT controls environment, the VP of Information Technology (Ken Shilling) is requesting an overview of defining a sustainable/manageable IT controls program. As such, leveraging *Exhibit One through to Exhibit Three* (inclusive) in the "Appendix" below, you will need to develop a single page placemat in Microsoft PowerPoint providing this overview and showing how the IT general controls components help manage the IT environment.

GENERAL CASE STUDY GUIDANCE

At a minimum, the solution to your case study should include the criteria below. Though not mandatory, you may use this as a format and general flow for your case study.

- A clear and concise background of the facts of the case.
- Key issues, observations and complicating factors that contribute to the root cause business problem at hand.
- A clear statement of the business problem to be solved.
- An overview of the solution and its components. The solution should address the key tasks outlined for you in the case.
- Demonstration of sufficient analysis that led you arrived at your solution.
- Clear recommendations for how the solution should be implemented or deployed.
- A timeline for execution of your recommendations.
- A budget or cost model for implementing your solutions. Be sure to include the cost to build and deploy your solution and the cost to run and operate your solution after it is built.
- An analysis of the risks, issues, key assumptions and any mitigating factors you will employ to minimize the likelihood and/or impact.

You have been asked for a lot of detailed information to solve this case. The trick will be to package this up into a digestible executive presentation your audience can understand. Detailed supporting information can be included in an exhibit in the appendix of your presentation.

Copyright © Justin Greis

Your case study solution should also include:

- Citation of key sources in the form of end notes cited in your appendix.
- Application of standards and leading practices that help to inform your solution.

A few tips and tricks for solving this case:

- Company financials have intentionally not been provided to you for this case. To build your model about sizing of the company, please conduct your own independent research and find similar peer companies.
- Feel free to make assumptions that support your conclusions. Be sure to state your assumptions in an exhibit in your appendix. Your assumptions should not significantly alter the facts of the case; rather, they should support the recommendations by filling in the missing pieces of information in the case.
- You should NOT simply copy/paste from COBIT or any of the other standards. The key is to use the standards to help you solve the case. Remember: standards are NEVER the answer on their own; they must be applied to the business problem.

Copyright © Justin Greis

APPENDIX

EXHIBIT ONE: IT GENERAL CONTROLS – MANAGE SYSTEM AND APPLICATION CHANGES

#	Control Name	Control Objective
1	Changes are authorized.	• Obtain a complete list of changes to the relevant components of the IT environment. • Select an appropriate sample of changes from the list and determine that the change was appropriately authorized.
2	Changes are tested.	• Obtain a complete list of changes to the relevant components of the IT environment. • Select an appropriate sample of changes from the list and determine that the change was appropriately tested.
3	Changes are approved.	• Obtain a complete list of changes to the relevant components of the IT environment. • Select an appropriate sample of changes from the list and determine that the change was appropriately approved.
4	Changes are monitored.	• Obtain sufficient evidence to determine that the change process is monitored on a regular basis (e.g., steering committee, management review of changes to production).
5	Segregation of incompatible duties exists within the manage change environment.	• Determine, both organizationally and logically, that different individuals within the organization perform the following duties: o Request/approve program development or program change. o Program the development or change. o Move programs in and out of production. o Monitor program development and changes.

Copyright © Justin Greis

EXHIBIT TWO: IT GENERAL CONTROLS – MANAGE LOGICAL ACCESS

#	Control Name	Control Objective
1	General system security settings are appropriate	• Determine that general system security settings are appropriate based on minimum security guidelines.
2	Password settings are appropriate	• For each relevant technical component of the logical access process, test the organization's settings for the following security configurations: o Minimum password length. o Initial log-on uses a one-time password. o Password composition (e.g., alpha/numeric characters, not words in dictionary). o Frequency of forced password changes. o The number of unsuccessful log on attempts allowed before lockout. o Ability of users to assign their own passwords. o Number of passwords that must be used prior to using a password again. o Idle session time out. o Logging of unsuccessful login attempts.
3	Access to privileged IT functions is limited to appropriate individuals	• Obtain a list of privileged user rights for relevant technical components of the logical access path that support the key controls (e.g., users with full system access or access to security administration functionality). • Determine that it is complete. • Review the lists of users with privileged rights and determine if the number of users appears appropriate. Based on the volume of users and the critical nature of this control, develop a test to determine if the users' privileged access is appropriate based on their job description/function (this listing should include the review of sensitive system accounts).
4	Access to system resources and utilities is limited to appropriate individuals	• Identify and obtain a list of resources (e.g., datasets, security, accounting schema, master files, transactional data), including utilities (e.g., SQL Plus) associated with the relevant applications that could affect the accuracy of the financial statements if not appropriately secured. • Determine that access to the resource(s) is appropriate.

Copyright © Justin Greis

#	Control Name	Control Objective
5	User access is authorized and appropriately established	• *New User Setup* – Obtain a list of new users added during the period under audit and determine that it is complete. • Select an appropriate sample and determine that there was appropriate approval granting the new user access and that the user's access was appropriately established based on his/her job function and the new user request form.
		• *Periodic User Validation* – Obtain the periodic validation report(s) and select an appropriate sample to determine that the users' access had been appropriately validated (are they a current employee, is their access appropriate based on job function, etc.).
		• *Monitoring of User Access* – Identify relevant monitoring controls and test that the controls functioned as expected over the audit period. These controls might include: o Violation or violation attempts reporting and review. o Review of logs (i.e., surrounding privileged user access).
6	Physical access to computer hardware is limited to appropriate individuals	• Obtain a list of employees with access to data centers, determine it is complete, and review for appropriateness. • Confirm that controls are in place to restrict access to only those individuals.
7	Logical access process is monitored	• Obtain sufficient evidence to determine that the logical access process is monitored on a regular basis (e.g., monitoring compliance with established logical access control procedures, periodic review of logical access policies and procedures, security risk assessments, etc.).
8	Segregation of incompatible duties exists within the logical access environment.	• Determine, both organizationally and logically, that different individuals/system resources perform the following duties related to granting user access: o Requesting access, approving access, setting up access, and monitoring access violations/violation attempts. o Performing rights of a "privileged" user and monitoring use of a "privileged" user IDs.

EXHIBIT THREE: IT GENERAL CONTROLS – IT OPERATIONS

#	Control Name	Control Objective
1	Financial data has been backed-up and is recoverable	• Determine process for identifying data to be backed up. • Determine that individuals who perform backups are not also responsible for monitoring them. • Select an appropriate sample of back-up activity and test that the IT General Controls over back-ups are operating as expected. • Review the procedures for periodically testing that backups can be restored.
2	Deviations from scheduled processing are identified and resolved in a timely manner	• Determine that only appropriate users have the ability to make changes to the job schedule and only approved changes are made. • Determine that individuals who program/implement/monitor scheduling do not have conflicting duties. • Test a sample of errors from production processing. For each, determine that an appropriate level of follow-up and resolution occurred.
3	IT operations problems or incidents are identified, resolved, reviewed, and analyzed in a timely manner	• Obtain sufficient evidence to determine that IT operations problems or incidents are identified, resolved, reviewed and analyzed in a timely manner.

Copyright © Justin Greis

EXHIBIT FOUR: HIPAA COMPLIANCE – ADMINISTRATIVE SAFEGUARDS

#	Safeguard Name	Required or Addressable	Safeguard Summary
1	Security management process — §164.308(a)(1)(i)	-	Implement policies and procedures to prevent, detect, contain, and correct security violations.
1.1	Security management process implementation specifications — Risk analysis — §164.308(a)(1)(ii)(A)	R	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (PHI) held by the covered entity.
1.2	Security management process implementation specifications — Risk management — §164.308(a)(1)(ii)(B)	R	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
1.3	Security management process implementation specifications — Sanction policies and procedures — §164.308(a)(1)(ii)(C)	R	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Covered Entity.
1.4	Security management process implementation specifications — Information system activity review — §164.308(a)(1)(ii)(D)	R	Procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking records.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
1.5	Assigned security responsibility — §164.308(a)(2)	R	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
2	Workforce security — §164.308(a)(3)(i)	-	Implement policies and procedures to ensure that all members of its workforce have appropriate access to Electronic Protected Health Information, as provided under §164.308(a)(4), and to prevent those workforce members who do not have access under §164.308(a)(4) from obtaining access to Electronic Protected Health Information.
2.1	Workforce security implementation specifications — Authorization and/or supervision — §164.308(a)(3)(ii)(A)	A	Implement procedures for the authorization and/or supervision of workforce members who work with Electronic Protected Health Information or in locations where it might be accessed.
2.2	Workforce security implementation specifications — Workforce clearance procedure — §164.308(a)(3)(ii)(B)	A	Implement procedures to determine that the access of a workforce member to Electronic Protected Health Information is appropriate.
2.3	Workforce security implementation specifications — Termination procedures — §164.308(a)(3)(ii)(C)	A	Implement procedures for terminating access to Electronic Protected Health Information when the employment of a workforce member ends or as required by determinations made in §164.308(a)(3)(ii)(B).

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
3	Information access management — §164.308(a)(4)	-	Implement policies and procedures for authorizing access to Electronic Protected Health Information that are consistent with the applicable requirements (of the privacy rule).
3.1	Information access management implementation specifications — Isolating health care clearinghouse functions - §164.308(a)(4)(ii)(A)	R	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement the policies and procedures that protect the Electronic Protected Health Information of the clearinghouse from unauthorized access by the larger organization.
3.2	Information access management implementation specifications — Access authorization §164.308(a)(4)(ii)(B)	A	Implement policies and procedures for granting access to Electronic Protected Health Information, for example, through access to a workstation, transaction, program, process, or other mechanism.
3.3	Information access management implementation specifications — Access establishment and modification §164.308(a)(4)(ii)(C)	A	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
4	Security awareness and training — §164.308(a)(5)	-	Implement a security awareness and training program for all members of its workforce (including management).

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
4.1	Security awareness and training implementation specifications — Security reminders §164.308(a)(5)(ii)(A)	A	Periodic security updates.
4.2	Security awareness and training implementation specifications — Protection from malicious software §164.308(a)(5)(ii)(B)	A	Procedures for guarding against, detecting, and reporting malicious software.
4.3	Security awareness and training implementation specifications — Log—in monitoring §164.308(a)(5)(ii)(C)	A	Procedures for monitoring log—in attempts and reporting discrepancies.
4.4	Security awareness and training implementation specifications — Password management §164.308(a)(5)(ii)(D)	A	Procedures for creating, changing, and safeguarding passwords.
5	Security incident procedures — §164.308(a)(6)	-	Implement policies and procedures to address security incidents.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
5.1	Security incident procedures implementation specifications — Response and reporting §164.308(a)(6)(ii)	R	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Covered Entity; and document security incidents and their outcomes.
6	Contingency plan — §164.308(a)(7)	-	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain Electronic Protected Health Information.
6.1	Contingency plan implementation specifications — Data backup plan §164.308(a)(7)(ii)(A)	R	Establish and implement procedures to create and maintain retrievable exact copies of Electronic Protected Health Information.
6.2	Contingency plan implementation specifications — Disaster recovery plan §164.308(a)(7)(ii)(B)	R	Establish (and implement as needed) procedures to restore any loss of data.
6.3	Contingency plan implementation specifications — Emergency mode operation plan §164.308(a)(7)(ii)(C)	R	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of Electronic Protected Health Information while operating in emergency mode.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
6.4	Contingency plan implementation specifications — Testing and revision procedures §164.308(a)(7)(ii)(D)	A	Implement procedures for periodic testing and revision of contingency plans
6.5	Contingency plan implementation specifications — Applications and data criticality analysis §164.308(a)(7)(ii)(E)	A	Assess the relative criticality of specific applications and data in support of other contingency plan components.
6.6	Evaluation – §164.308(a)(8)	R	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of Electronic Protected Health Information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
7	Business associate contracts and other arrangements — 164.308(b)(1)	-	A Covered Entity, in accordance with 164.306, may permit a Business Associate to create, receive, maintain, or transmit Electronic Protected Health Information on the Covered Entity's behalf only if the Covered Entity obtains satisfactory assurances, in accordance with 164.314(a) that the Business Associate will appropriately safeguard the information.
7.1	Business associate contracts and other arrangements implementation specifications —	R	Document the satisfactory assurances required by 164.308(b)(1) though written contract or other arrangement with the Business Associate that meets the applicable requirements of 164.314(a).

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
	Written contract or other arrangement §164.308(b)(4)		

EXHIBIT FIVE: HIPAA COMPLIANCE – PHYSICAL SAFEGUARDS

#	Safeguard Name	Required or Addressable	Safeguard Summary
1	Facility access controls — §164.310(a)(1)	-	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
1.1	Facility access controls implementation specifications — Contingency operations §164.310(a)(2)(i)	A	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
1.2	Facility access controls implementation specifications — Facility security plan §164.310(a)(2)(ii)	A	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
1.3	Facility access controls implementation specifications — Access control and validation procedures §164.310(a)(2)(iii)	A	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
1.4	Facility access controls implementation specifications — Maintenance records §164.310(a)(2)(iv)	A	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
1.5	Workstation use — §164.310(b)	R	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.
1.6	Workstation security — §164.310(c)	R	Implement physical safeguards for all workstations that access Electronic Protected Health Information, to restrict access to authorized users.
2	Device and media controls — §164.310(d)(1)	-	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.
2.1	Device and media controls implementation specifications — Disposal §164.310(d)(2)(i)	R	Implement policies and procedures to address the final disposition of Electronic Protected Health Information, and/or the hardware or electronic media on which it is stored.
2.2	Device and media controls implementation specifications — Media re—use §164.310(d)(2)(ii)	R	Implement procedures for removal of Electronic Protected Health Information from electronic media before the media are made available for re—use.
2.3	Device and media controls implementation specifications —	A	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
	Accountability §164.310(d)(2)(iii)		
2.4	Device and media controls implementation specifications — Data backup and storage §164.310(d)(2)(iv)	A	Create a retrievable, exact copy of Electronic Protected Health Information, when needed, before movement of equipment.

EXHIBIT SIX: HIPAA COMPLIANCE – TECHNICAL SAFEGUARDS

#	Safeguard Name	Required or Addressable	Safeguard Summary
1	Access controls — §164.312(a)(1)	-	Implement technical policies and procedures for electronic information systems that maintain Electronic Protected Health Information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).
1.1	Access controls implementation specifications — Unique user identification (required) §164.312(a)(2)(i)	R	Assign a unique name and/or number for identifying and tracking user identity.
1.2	Access controls implementation specifications — Emergency access procedure (required) §164.312(a)(2)(ii)	R	Establish (and implement as needed) procedures for obtaining necessary Electronic Protected Health Information during an emergency.
1.3	Access controls implementation specifications — Automatic logoff (addressable) §164.312(a)(2)(iii)	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
1.4	Access controls implementation specifications — Encryption and decryption	A	Implement a mechanism to encrypt and decrypt electronic protected health information.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
	(addressable) §164.312(a)(2)(iv)		
1.5	Audit controls (required) — §164.312(b) –	R	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic Protected Health Information.
2	Integrity — §164.312(c)(1)	-	Implement policies and procedures to protect Electronic Protected Health Information from improper alteration or destruction.
2.1	Integrity implementation specifications — Mechanism to authenticate electronic protected health information (addressable) §164.312(c)(2)	A	Implement electronic mechanisms to corroborate that Electronic Protected Health Information has not been altered or destroyed in an unauthorized manner.
2.2	Person or entity authentication (required) — §164.312(d) –	R	Implement procedures to verify that a person or entity seeking access to Electronic Protected Health Information is the one claimed.
3	Transmission security — §164.312(e)(1)	-	Implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network.

Copyright © Justin Greis

#	Safeguard Name	Required or Addressable	Safeguard Summary
3.1	Transmission security implementation specifications — Integrity controls (addressable) §164.312(e)(2)(i)	A	Implement security measures to ensure that electronically transmitted Electronic Protected Health Information is not improperly modified without detection until disposed of.
3.2	Transmission security implementation specifications — Encryption (addressable) §164.312(e)(2)(ii)	A	Implement security measures to ensure that electronically transmitted Electronic Protected Health Information is not improperly modified without detection until disposed of.

EXHIBIT SEVEN: HIPAA BREACH NOTIFICATION RULE[1]

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Definition of Breach – A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Breach Notification Requirements – Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Individual Notice – Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more

[1] Source: U.S. Department of Health and Human Services

individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

Media Notice – Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary – In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Notification by Business Associates - If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.