**Sample Terms for Third Parties Providing Remote Processing Services**

**I BACKGROUND AND DEFINITIONS**

1. **Background:** Health System has become increasingly dependent upon other organizations to provide services where the organization or its subcontractors, agents, representatives, and the like (“Third Party”) provide Remote Processing Services to Health System (as defined in section 3.f. below). These Remote Processing Services take many forms and names, including “Application Service Provider”, “Software as a Service”, “Cloud-based”, etc.

Remote Processing Services may also include situations where Third Party remotely processes or stores Health System Data in order for Third Party to provide a Professional Service to Health System. In such cases, typically only section I, II, III and IV are applicable.

To ensure that Remote Processing Services can be reliably and effectively delivered, that Health System Data is appropriately safeguarded, and that Health System complies with relevant laws and regulations, the following terms have been established by Health System.

1. **Application:** These terms apply to situations where a Third Party provides Remote Processing Services to Health System. For clarity, these situations may arise when the Third Party is not paid for providing Remote Processing Services to Health System.
2. **Definitions**:
3. *Authorized Party* is a party that acts for or on behalf of Third Party in delivering Remote Processing Services, and include subcontractors, agents, representatives, auditors, and the like.
4. *HITRUST® Certification* means a letter of certification issued by HITRUST, based on the completion of a Validated Assessment of the HITRUST Cyber Security Framework (CSF) performed according to the then-current HITRUST Assurance Program Standards and version of the HITRUST CSF® found at <https://hitrustalliance.net>.
5. *Personally Identifiable Information (PII)* means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. Non-PII can become PII whenever additional information is made available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.
6. *Professional Services* means services provided by an individual, often as a representative of a Third Party, that involves expertise that an organization either does not possess, does not have sufficient capacity to perform itself or chooses not to do itself.
7. *Protected Health Information (PHI)* **-** As defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub.L. 104–191).
8. *Remote Processing Service(s)* means all products and services supplied by the Third Party that are remotely delivered that involve access, processing, receipt, storage, transmission, and/or destruction of personal information, including PHI, electronic versions of PHI, and PII. Remote Processing Services also include Professional Services where the Professional Services include the Third Party receiving, storing, processing, transmitting, and/or remotely destroying PHI or PII of Health System. Remote Processing Services include any new versions or revisions of Remote Processing Service and any new products that Third Party delivers to Health System that replace the Remote Processing Services originally acquired by Health System. For clarity, the following are examples of Remote Processing Services:
   * 1. Providing “cloud” based services that allow Health System to access computer program or service on Third Party’s computers (including computer capacity contracted for by Third Party – such as AWS or Azure).
     2. Performing remote processing or storage of Health System Data in order for Third Party to provide a Professional Service to Health System. Health System would not have access to Third Party computer programs or services (as set for (i)).
     3. Providing remote computing capacity to Health System. This includes IaaS, PaaS and SaaS services provided by Third Party.
9. *Security Breach* means (i) any act or omission by Third Party or any other part retained by or engaged by Third Party that compromises either the security, availability, confidentiality or integrity of Health System Data or the physical, technical, administrative or organizational safeguards put in place by Third Party that relate to the security, confidentiality or integrity of Health System Data, or (ii) a loss or unauthorized access, exfiltration or disclosure of (a) Health System Data caused by Third Party or (b) Health System Data in Third Party’s possession. For clarity, the following are examples of a Security Breach:

* Third Party experiences a ransomware attack involving Health System Data;
* Health System data is exposed to access by non-authorized party, and Third Party cannot verify that such information was not accessed; or
* Health System Data was actually accessed or exfiltrated by an unauthorized party.

1. *Third Party* means the organization hereunder that is providing Remote Processing Service(s) to Health System. Third Party also includes Authorized Parties.
2. *Tracking Technologies* mean a script or code on a website or mobile app used to gather information, including PHI, PII and non-identifying information (e.g., aggregate usage information) about users, their activity, and the device used as they interact with the website or mobile app (“Usage Data”).

Tracking technologies, such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts, can be used to track and collect this Usage Data. Mobile apps can include/embed tracking code within the app to enable the app to collect information directly provided by the user or the activities of the user on the website, and mobile apps may also capture the user’s mobile device-related information. For example, mobile apps may use a unique identifier from the app user’s mobile device, such as a device or advertising ID.

Tracking technologies developed by third parties (e.g., tracking technology vendors) may collect and/or send information directly to the third parties who developed such technologies, and may continue to track users and gather information about them even after they navigate away from the original website to other websites.

1. *Health System Data means a*ll data created by, entered into, collected through, made in conjunction with or contained in files specifically associated with performing the Remote Processing Service for Health System or contained in the software or on the equipment used to provide the Remote Processing Service to Health System, including Usage Data PII and PHI collected or processed through the use of Tracking Technologies. Health System Data includes information in de-identified, aggregate, or summary form.

**II. GENERAL TERMS**

1. **Standard of Care.** Third Party acknowledges and agrees that, in the course of its engagement by Health System, Third Party may receive or have access to Health System Data. Third Party shall comply with the terms and conditions set forth herein in its collection, receipt, transmission, access, processing, storage, disposal, use and disclosure of such Health System Data and be responsible for the unauthorized collection, receipt, transmission, access, processing, storage, disposal, use and disclosure of Health System Data under its control or in its possession.
2. **Material Breach.** Third Party’s failure to comply with any of the provisions of this Agreement is a material breach of this Agreement. In the event of a material breach, Health System may terminate this Agreement immediately upon written notice to the Third Party without further liability or obligation to Health System, subject to a Transition Period as set forth herein. In the event that Health System has prepaid any fees, Third Party shall proportionally refund any prepaid fees.
3. **Criminal Background Check**.  Third Party shall complete a criminal background check and drug testing on every individual, not employed by Health System that provides Remote Processing Services involving access to Health System Data.  In the event an individual fails a drug test or has a criminal record or history which consists of a felony or misdemeanor conviction, Third Party shall not allow the individual with access to Health System Data without Health System’s prior written consent.  This provision is in addition to such other Health System terms associated with criminal background checks, drug testing and infectious disease testing that Health System may require for resources coming on to Health System premises.
4. **Employee Training.** Third Party shall annually provide appropriate privacy and information security training to Third Party’s staff and others that assist in providing Remote Processing Services
5. **Employee Acts.** Third Party shall at all times cause its staff to abide strictly by Third Party’s obligations under this Agreement and Health System’s policies and procedures, a copy of which shall be provided to Third Party. Third Party further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of Health System Data by any of Third Party’s staff.
6. **Indemnification**. Third Party shall defend, indemnify, and hold harmless Health System, and Health System’s subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors and permitted assigns (each, a “Health System Indemnitee”) from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys’ fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim against any Health System Indemnitee arising out of or resulting from a claim of intellectual property infringement, Security Breach, or from Third Party’s failure to comply with any of its obligations under this Agreement.
7. **No Limits on Liability.** Regardless of any limitation of liability terms otherwise agreed to by the parties, with respect to a claim of intellectual property infringement or Security Breaches caused by Third Party, there shall be no limitation on the liability that Third Party has to Health System.
8. **Equitable Relief.** Third Party acknowledges that any breach of its covenants or obligations set forth in this Agreement may cause Health System irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Health System is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which Health System may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Agreement to the contrary.
9. **Cybersecurity Risk Insurance.**  Third Party shall maintain a Cybersecurity Risk Insurance policy that covers all risks and associated costs resulting from a Security Breach. Such policy shall extend to including those risks and cost incurred by Health System as a result of Third Party’s Security Breach.
10. **Authorized Parties.** Third Party is responsible for and remains liable to Health System for the actions and omissions of all Authorized Parties. Where Third Party is identified in these terms, such terms shall also apply to Authorized Parties. Third Party shall require all Authorized Parties to execute a written agreement agreeing to comply with the terms and conditions set forth herein.

**III. Health System DATA CONFIDENTIALITY, OWNERSHIP AND ACCESS STANDARDS**

1. **Data Ownership**. All Health System Data is solely owned by Health System. Third Party has a limited license to use Health System Data solely for and only to the extent necessary to provide the Remote Processing Services.
2. **Confidentiality**. All Health System Data is Confidential Information of Health System. In recognition of the foregoing, Third Party agrees that it shall:
   1. Keep and maintain all Health System Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure.
   2. Not, directly, or indirectly, disclose or allow access to Health System Data by any person other than its staff, without express written consent from Health System, unless and to the extent expressly required by law, in which case, Third Party shall notify Health System before such disclosure with sufficient time to allow Health System to seek to prevent or limit such disclosure.
3. **Data Use and Disclosure.** Third Party has no right to use or disclose Health System Data for any purpose other than to provide the Remote Processing Services to Health System without Health System’s prior written consent, regardless of whether the Health System Data is aggregated or de-identified. For clarity, Third Party shall not use, sell, rent, transfer, distribute, or otherwise disclose or make available Health System Data for Third Party’s own purposes or for the benefit of anyone other than Health System without Health System prior written permission and in a manner that complies with applicable laws.
4. **Data Access and User Accounts.**
   1. Third Party shall only access and/or use Health System Data for the purpose of meeting its commitments to Health System set forth this Agreement.
   2. Third Party shall issue unique user accounts to each member of its staff requiring access to Health System Data. Such access shall be based on a need to know.
   3. Third Party is responsible for the appropriate safeguarding of user accounts and passwords used to access Health System Data.
   4. To the extent that Third Party’s staff requires access to Health System information systems and infrastructure, Third Party shall execute the “Health System Third Party Computer System Access Agreement” and have its staff who access Health System information systems or infrastructure sign the “Health System Confidentiality Agreement for Third Party Staff / Students Accessing Health System Information Systems”. These agreements shall be submitted by Third Party to the Health System staff member who establishes the user accounts.
   5. All user accounts issued by Third Party to its staff shall be accounted for by Third Party and Third Party shall make such records available to Health System.
   6. Third Party staff is not permitted to share or use another staff member’s user account(s).
   7. If a Third Party staff member no longer requires access to Health System Data, Third Party shall notify Health System to revoke the staff member’s user account(s).
   8. Third Party shall maintain a log of all access to Health System Data. Third Party shall regularly monitor the access log to ensure that the Third Party’s staff access was appropriate.
   9. Third Party shall inform Third Party’s staff of its responsibilities under this Agreement.
5. **Management of Health System Data.** The parties shall establish a data management plan to address how data will be managed by the Third Party both during the time that Remote Processing Services are being provided and at the cessation of Remote Processing Services. This will include, but is not limited to:
6. Management of Health System Data During Processing. In situations where Third Party requires the use of Health System Data for a limited period of time in order to deliver a Remote Processing Service, immediately following the time when such use is required, Third Party shall provide a copy of such Health System Data to Health System in a mutually agreed upon electronic format (if requested), then destroy unneeded copies of such Health System Data in its possession [in manner consistent with applicable industry standards] [or] [in compliance with NIST Special Publication 800-88, Revision 1] such that the Health System Data can never be retrieved, undeleted, or reconstituted in any way.
7. Encryption. Third Party shall encrypt and appropriately secure all Health System Data while Health System Data is in Third Party’s possession.
8. Management of Health System Data at Cessation of Remote Processing Services.
9. Based on milestones established in the Transition Schedule and instructions established by the parties, Third Party shall provide to Health System copies of Health System Data in Third Party’s possession in a mutually agreed upon electronic format.
10. Following the provision of Health System Data as set forth in subsection (i), Third Party shall destroy all Health System Data in its possession and provide Health System with written notice of destruction.
11. In the absence of any instructions from Health System for the return of Health System Data, Third Party shall notify Health System in writing of the existence of Health System Data, and provide Health System thirty (30) days from the receipt of such notice to arrange for the return of the Health System Data in a mutually acceptable electronic format, after which, in the absence of other directions by Health System, Third Party shall destroy all Health System Data in its possession and provide Health System with written notice of destruction.
12. **Location of Health System Data and Services**. All Health System Data shall be stored in data centers located within the United States. All Remote Processing Services involving access or use of Health System Data shall be performed by Third Party’s staff located within the United States.
13. **Domestic Remote Processing Services Processing Requirement**.Third Party shall ensure that Remote Processing Services delivered by Third Party and its suppliers to Health System are performed using information systems physically located in the United States of America (USA). Processing includes the transmission, storage, and destruction of Health System Data.
14. **Comingling of Health System Data.** Third Party shall not co-mingle Health System Data with data from other of Third Party’s customers. For clarity, “co-mingle” means to include Health System Data with data from other of Third Party’s customers in a single database or file structure.
15. **Ownership of Domain Names.** In the event that Third Party establishes or registers web domain names, non-fungible token and other crypto domain names, or other digital accounts on behalf of Health System (“Domain Names and Accounts”), all such Domain Names and Accounts shall be solely owned by Health System for which Third Party has no rights to use except for the purpose of providing Remote Processing Services, provided that Third Party shall not establish or register domain names and accounts on behalf of Health System without Health System’s prior written permission. Health System may also provide Third Party with its own Domain Names and Accounts for Third Party to use in conjunction with the Remote Processing Services. Health System agrees that it shall bear all responsibility, maintenance and costs for the registration and renewal of any such domain names and accounts-related certificates.
16. **Use of Tracking Technologies.** Tracking Technologies shall not be utilized or required for the Remote Processing Service to operate and shall only be utilized with Health System’s prior written approval. Any such Tracking Technology shall be configured to comply with all applicable laws and regulations.

**IV. INFORMATION SECURITY**

1. **Information Security - Generally**. Without limiting Third Party’s obligations hereunder, Third Party shall implement administrative, physical, and technical safeguards necessary to secure its computers, applications, IT infrastructure, premises and Health System Data that are no less rigorous than accepted industry practices, including current and ongoing HITRUST Certification, and shall ensure that all such safeguards, including the manner in which Health System Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with the terms and conditions of this Agreement. Third Party’s safeguards for the protection of Health System Data shall include, but are not limited to:
2. Limiting access of Health System Data to authorized persons.
3. Securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, thumb drives, mobile devices, and other equipment with information storage capability.
4. Implementing network, device, application, database, and platform security - securing information transmission, storage, and disposal.
5. Implementing authentication and access controls within media, applications, operating systems, and equipment.
6. Encrypting Health System Data stored on any PC, laptop, server, storage device, mobile device, removable media, backup storage media, etc.
7. Encrypting Health System Data transmitted over public or wireless networks.
8. **Compliance with Laws, Rules and Regulations.** Third Party shall provide the Remote Processing Services hereunder in full compliance with all applicable federal, state, and local laws, industry rules and generally accepted industry standards at its own expense and within the mandated time frames. For example, to the extent that Third Party has access to or will collect, access, store, process, dispose of or disclose credit, debit or other payment cardholder information, Third Party shall comply on an ongoing basis with relevant PCI requirements at its own expense within the mandated time frames. All such compliance shall be at Third Party’s expense.
9. **HIPAA.** To the extent that Third Party has access or possession of identifiable Health System patient data, Third Party shall comply with Health System’s HIPAA Business Associate terms and conditions, including any future modifications thereto, that are found at:

*[Insert Health Systems URL link for about/partners/supply-chain/guidelines-for-associates]*

The Health System’s Business Associate terms and conditions supplement and do not replace this Agreement. In the event of a conflict between this Agreement and such Business Associate terms and conditions, the Business Associate terms and conditions will control with respect to identifiable Health System patient data.

1. **Security Assessment Requirements.**
   1. Generally. Health System employs a tiered security assessment process to evaluate its third parties’ information security capabilities. Security assessments are performed during the initial evaluation of a third party (prior to the formation of a relationship) and typically annually thereafter. Which tier of the assessment process a Third Party must comply with is based on criteria set forth in subsection 4.b. below and is measured at the time of the security assessment.
   2. Security Assessment.
      1. HITRUST Certification. HITRUST offers a tiered certification program. Where Third Party has access to or has in its possession Health System patient or Member information, that Third Party shall maintain HITRUST Certification as more fully described below, or
      2. HITRUST Assessment Xchange (HAX). Third Party shall participate in the **e1 Self - Assessment** process as described below – or such other assessment process that Health System determines.
   3. Other Assessment and Reporting Requirement. Where relevant to the Remote Processing Services provided, Third Party’s handling of specific forms of regulated data may be required to adhere to additional specific standards (such as Payment Card Industry (PCI) Security Standards). Effective oversight of other specific compliance functions by Third Party is required by Health System and shall be met through provision of additional “Report” documentation and the use of applicable regulatory and other additional factors offered by HITRUST.
2. **Requirement for HITRUST® HAX e1 Self - Assessment.**
3. Generally. As required by Health System hereunder, prior to the initiation of Remote Processing Services and at least annually thereafter, Third Party provide information as necessary to complete the **e1 Self - Assessment** .
4. Reassessment Requirements. Third Party shall complete a **e1 Self - Assessment** (i) at least annually, (ii) if additional Remote Processing Services are contracted for, or (iii) when such Remote Processing Services are renewed. Third Party agrees to register with and conform to rules governing use of HAX found at https://hitrustax.com/ for the purpose of providing HITRUST assessment reports and related information to Health System.
5. Failure to Receive an Adequate **e1 Self - Assessment** Score Prior to Initiation of Remote Processing Services. In the event that Third Party’s does not achieve a **e1 Self - Assessment** score of 90 prior to initiation of Remote Processing Services by Health System or as agreed to:
6. Health System reserves the right to terminate this Agreement without cause or penalty for cause. Upon such termination, Third Party shall refund Health System all amounts paid hereunder; and/or,
7. Health System may conduct a security audit at Third Party’s expense of Third Party’s security controls and infrastructure that are used by Third Party to provide the Remote Processing Services.  Such audit may be performed by Health System or by a subcontractor selected by Health System and shall include the right to inspect Third Party’s site and to evaluate Third Party’s information security program, policies, and procedures.  Such audit may also include performing unannounced penetration testing of Third Party’s network and systems.  Health System shall provide notice to Third Party following such penetration testing; and/or,
8. Health System may agree to provide Third Party with an extension in order for Third Party to achieve a **e1 Self - Assessment** score of 90, provided that should Third Party not achieve a **e1 Self – Assessment** score of 90 within six (6) months of the effective date of these terms, Third Party shall pay the penalties set forth in Subsection d (titled “Penalties”).
9. **Failure to Maintain e1 Self - Assessment.** In the event Third Party fails to maintain a **e1 Self - Assessment** score of 90 for any reason:
10. Health System reserves the right to terminate this agreement without cause or penalty. Upon such termination, Third Party shall refund Health System a prorate amount of all amounts paid hereunder for the remaining unused term of the agreement; and/or,
11. Third Party agrees to develop and submit a remediation plan demonstrating restoration of controls found to be deficient, restoring such control practices to the point which re-assessment may occur. Updates on remediation plans should be submitted at least every three (3) months until completed. Third Party agrees to perform such remediation and re-assessment within a commercially reasonable period of time to achieve a **e1 Self - Assessment** score of 90; and/or.
12. Health System may conduct a security audit at Third Party’s expense of Third Party’s security controls and infrastructure that are used by Third Party to provide the Remote Processing Services.  Such audit may be performed by Health System or by a subcontractor selected by Health System and shall include the right to inspect Third Party’s site and to evaluate Third Party’s information security program, policies, and procedures.  Such audit may also include performing unannounced penetration testing of Third Party’s network and systems.  Health System shall provide notice to Third Party following such penetration testing.
13. Third Party shall reduce all fees incurred by Health System for all Remote Processing Services and related Professional Services, according to the following below table.

|  |  |
| --- | --- |
| Requirement | Penalty |
| Out of compliance for <= 30 days | 2% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for 31-60 days | 10% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for 61-90 days | 25% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for more than 90 days | 30% of all fees payable by Health System for the period of non-compliance, payable monthly. Grounds for Termination for Cause at the sole determination of Health System. |

1. **Requirement for HITRUST® Certification.**
2. Generally. HITRUST offers a tiered certification program. Where Third Party has access to or has in its possession Health System patient or Member information, prior to the initiation of Remote Processing Services and continuously thereafter, Third Party shall maintain (a) HITRUST Certification for all Remote Processing Services being subscribed to by Health System, and (b) a summary of any Corrective Action Plans (“CAPs”), including a timeframe for addressing the CAPs, produced during the production of the most recent report, and issued with the report. The level (tier) of HITRUST Certification required shall be at Health System’s sole discretion and based on the amount of patient / member information that it accesses or possesses.
3. Reporting Requirements. Third Party shall provide to Health System its HITRUST Certification and Reports and related CAPs for all Remote Processing Services prior to the initiation of Remote Processing Services and thereafter (i) at least annually, (ii) if HITRUST Certification status changes, (iii) when additional Remote Processing Services are contracted for, or (iv) when such Remote Processing Services are renewed. Third Party agrees to register with and conform to rules governing use of the HITRUST Assessment Xchange (HAX) found at https://hitrustax.com/ for the purpose of providing HITRUST Certification Reports and related information to Health System.
4. Commitment to Accept HITRUST Certification. Health System agrees that it will accept HITRUST Certification in lieu of the requirement to perform or provide other audits or assessments related to the Remote Processing Services.
5. Failure to Receive HITRUST Certification Prior to Initiation of Remote Processing Services. In the event that Third Party’s does not achieve HITRUST Certification prior to initiation of Remote Processing Services by Health System or as agreed to by Health System:
6. Health System reserves the right to terminate this agreement without cause or penalty. Upon such termination, Third Party shall refund Health System all amounts paid hereunder; and/or,
7. Third Party must participate in the **e1 Self – Assessment** as set forth above until officially certified; and/or,
8. Health System may conduct a security audit at Third Party’s expense of Third Party’s security controls and infrastructure that are used by Third Party to provide the Remote Processing Services.  Such audit may be performed by Health System or by a subcontractor selected by Health System and shall include the right to inspect Third Party’s site and to evaluate Third Party’s information security program, policies, and procedures.  Such audit may also include performing unannounced penetration testing of Third Party’s network and systems.  Health System shall provide notice to Third Party following such penetration testing; and/or,
9. Health System may agree to provide Third Party with an extension in order for Third Party to achieve HITRUST Certification, provided that should Third Party not achieve HITRUST Certification within eighteen (18) months of the effective date of these terms, Third Party shall pay the penalties set forth in Subsection e (titled “Penalties”).
10. **Failure to Maintain HITRUST Certification.** In the event Third Party fails to maintain HITRUST Certification following its original issuance, for any reason:
11. Health System reserves the right to terminate this agreement without cause or penalty. Upon such termination, Third Party shall refund Health System a prorate amount of all amounts paid hereunder for the remaining unused term of the agreement; and/or,
12. Third Party agrees to develop and submit a remediation plan demonstrating restoration of controls found to be deficient, restoring such control practices to the point which re-Certification may occur. Updates on remediation plans should be submitted at least every three (3) months until completed. Third Party agrees to perform related re-Certification activities within a commercially reasonable period of time to achieve HITRUST Certification; and/or,
13. Health System may conduct a security audit at Third Party’s expense of Third Party’s security controls and infrastructure that are used by Third Party to provide the Remote Processing Services.  Such audit may be performed by Health System or by a subcontractor selected by Health System and shall include the right to inspect Third Party’s site and to evaluate Third Party’s information security program, policies, and procedures.  Such audit may also include performing unannounced penetration testing of Third Party’s network and systems.  Health System shall provide notice to Third Party following such penetration testing.
14. Third Party shall reduce all fees incurred by Health System for all Remote Processing Services and related Professional Services, according to the following below table.

|  |  |
| --- | --- |
| Requirement | Penalty |
| Out of compliance for <= 30 days | 2% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for 31-60 days | 10% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for 61-90 days | 25% of all fees payable by Health System for the period of non-compliance, payable monthly. |
| Out of compliance for more than 90 days | 30% of all fees payable by Health System for the period of non-compliance, payable monthly. Grounds for Termination for Cause at the sole determination of Health System. |

1. Use of Subcontractors. Third Party agrees to require any subcontractor and/or service provider(s) it uses to deliver Remote Processing Services which require the use, access, disclosure, transmission, or storage of PHI and PII to comply with these terms. Third Party agrees to provide evidence of service provider’s HITRUST Certification to Health System upon request.
2. **Integration with Health System Security Tools.**
3. Identity Management. At Health System’s request and Third Party’s expense, Third Party shall allow for the automated management of user accounts through the integration of its system(s) with Health System’s identity management system and framework (including federation). If Health System’s identity management system is utilized, accounts will not be independently created without Health System’s approval. Where Health System approves the independent creation of user accounts, any accounts created independently shall be entered into Health System’s identity management system within five (5) business days.
4. Patient Privacy Monitoring. At Health System’s request and Third Party’s expense, In the event that the Third Party’s system will house Health System patient information, at least weekly, Third Party shall provide user access information in the format provided by Health System for inclusion in Health System’s patient privacy monitoring system.
5. Security Incident and Event Management system. At Health System’s request and Third Party’s expense, Third Party shall provide security related logs on a daily basis to Health System for inclusion in Health System’s Security Incident and Event Management system.
6. Enterprise Key Management. Where technically feasible, at Health System’s request, and at Third Party’s expense, Third Party shall utilize encryption keys provided by Health System for securing Health System Data kept in its system(s). Such keys shall be managed through the use of a commercial key management system that is either approved and/or managed by Health System.
7. Multifactor Authentication. At Health System’s request and Third Party’s expense, Third Party shall integrate its systems into Health System’s Multifactor Authentication environment.
8. **New Releases.** Third Party shall implement all New Releases of software used to deliver the Remote Processing Services within a commercially reasonable period time, which must in all cases be agreed to by Health System, but shall be no longer than is required so that the software remains fully supported by the Third Party. A “New Release” is defined as any update, upgrade, or new version of the software. Health System reserves the right to request a security assessment or application code assessment (including any remediation) of any New Release prior to deployment.
9. **Patches**. Should the software used to deliver the Remote Processing Services (including any related Third Party software, operating systems, layered software, etc.) require a software patch to correct an issue (including, but not limited to, security issues, incorrect operation of the software that materially impact the safe or correct operation of the software, software performance, data integrity, etc.), Third Party shall create and/or install the software patch within seven (7) days that the patch was made available. Health System reserves the right to request a security assessment or application code assessment (including any remediation) of any patch prior to deployment.
10. **Introduction of Viruses**. In providing Remote Processing Services, Third Party shall not introduce, and will implement technical, operational and administrative measures to manage the risk of introducing into Health System’s computer systems, operating systems, applications or other equipment or software any program routine, device or other undisclosed feature, comprising a trap door, time bomb, trojan horse, worm, spyware, bot, cookie, malicious logic, viruses, usage locks, physical or electronic license keys or disabling mechanisms or other routine, device, file or feature, whether such disabling mechanisms are based on calendar date or elapsed time, that is designed to track, monitor or capture computer or user files, information or data, or to delete, disable, deactivate or otherwise render the software or any other of Health System’s software, hardware or network inoperable. Third Party shall reimburse Health System for its costs incurred as a result of Third Party not performing its obligations as set forth in this section.
11. **Anti-Virus and Encryption Software.** Third Party shall install anti-virus / anti-malware software on the servers used to process and/or store Health System Data. Third Party shall regularly update anti-virus software, based on the anti-virus Third Party’s update schedules. Third Party shall employ encryption within its environment to protect Health System Data. This includes encryption of all endpoints (PCs, laptops, tables, smartphones, etc), all servers, all removable storage (including CDs, thumb drives, external hard drives, etc.), networks / communication protocols and infrastructure, e-mail services, etc.
12. **Security Breaches**.
    1. Third Party shall:
13. Provide Health System with the contact information for a primary security point of contact and shall be available to assist Health System twenty-four (24) hours per day, seven (7) days per week to address Security Breaches.
14. Notify Health System of a Security Breach as soon as practicable, but no later than four (4) hours after Third Party becomes aware of it. Such notice shall include the scope of any possible or actual breach or Loss of Health System Data.
15. Notify Health System of any Security Breaches by e-mailing Health System with a read receipt at [isgsoc@XXXXX.edu and with a copy by e-mail to Third Party’s primary business contact within Health System.
    1. Immediately following Third Party’s notification to Health System of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Third Party agrees to fully cooperate with Health System in Health System’s handling of the Security Breach, including, without limitation:
    2. Assisting with any investigation.
    3. Providing Health System with physical access to the facilities and operations affected.
    4. Facilitating interviews with Third Party’s employees and others involved in the matter.
    5. Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Health System.
    6. Third Party shall use its commercial best efforts to immediately remedy and mitigate any harmful effects of a Security Breach. Third Party shall reimburse Health System for actual costs incurred by Health System in responding to, and mitigating damages caused by any Security Breach, including all costs of notice and/or remediation.
    7. Third Party agrees that it shall not inform any third party or the public of a Security Breach without first obtaining Health System’s prior written consent, other than to inform a complainant that the matter has been forwarded to Health System’s legal counsel. Further, Third Party agrees that Health System shall have the sole right to determine:
    8. Whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Health System’s discretion.
    9. The contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.
    10. Third Party agrees to fully cooperate at its own expense with Health System in any litigation or other formal action deemed reasonably necessary by Health System to protect its rights relating to the use, disclosure, protection, availability, and maintenance of Health System Data.
    11. In the event of any Security Breach, Third Party shall promptly use its reasonable efforts to prevent a recurrence of such Security Breach. Third Party shall provide Health System with information regarding the steps that it has taken to prevent a recurrence of a Security Breach, provided that if Health System determines that such steps are not adequate, Health System may terminate this Agreement as a material breach.
    12. In the event that Third Party does not truthfully answer any assessment required hereunder, Health System reserves the right to terminate this agreement without cause or penalty. Upon such termination, Third Party shall refund Health System a prorate amount of all amounts paid hereunder for the remaining unused term of the agreement.