Indiana University Health

Information Security

Third Party Information Security Practices Due Diligence

Service Organization Control Reports, HITRUST Common Security Framework (CSF) certification, or Annual Risk Assessments.

Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate and associated subservice providers to deliver Services to or on behalf of Covered Entity, Business Associate agrees to provide to CE an attestation of its and its applicable subservice providers that handle IU Health Confidential Information security risk assessments via an IT Risk Assessment (ITRA), ISO 27001/27017/27018 certifications, or Data Protection Impact Analyses and associated documentation, and Service Organizations Control Level 2 (SOC2) reports every year. A Health Information Trust (HITRUST) Common Security Framework (CSF) certification to the current framework will be accepted for every other year. For the purposes of this BAA, IU Health Confidential Information shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

i. *Health Information Trust (HITRUST) Common Security Framework (CSF) Certification.* If Vendor has provided proof of HITRUST certification, allow IU Health the right to review their HITRUST assessment certification letter in lieu of an IT Risk Assessment and SOC2 report.
    a. The HITRUST certification must be kept current within 1 year of review and be conducted by a certified assessor.
    b. The version of the CSF attested to must be current within 1 year of review.
    c. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the version of the HITRUST Common Security Framework (CSF) that has been attested to and certified.
    d. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

ii. *Service Organization Control Reports.* Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate to deliver Services to or on behalf of Covered Entity, Business Associate agrees to annually provide a Service Organization Control 2 (SOC 2) Type 2 report to Covered Entity if (1) it provides Service Organization services to Covered Entity involving IU Health Confidential Information that Covered Entity would otherwise perform such as medical record services, data centers, IT managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses, or (2) it is required as more particularly described in Exhibit A attached hereto. For the purposes of this, "IU Health Confidential Information" shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

iii. *ISO 27001/27017/27018 Certification.* If Vendor has provided proof of ISO 27001/27017/27018 certification, allow IU Health the right to review their ISO certification in lieu of an IT Risk Assessment and SOC2 report.
    a. The ISO certification must be kept current within 1 year of review and be conducted by an accredited certification body (e.g. ANSI-ASQ National Accreditation Board [ANAB]) or a certified accountancy.
    b. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the ISO standards that have been attested to and certified.
    c. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

Information Security

iv. *European Union General Data Protection Regulation (GDPR) or similar governmental level privacy regulations.* If Vendor has provided proof of compliance with the below, IU Health will review in lieu of an IT Risk Assessment and SOC2 Report. The deliverables need to be in the form of:
    a. A completed Data Protection Impact Assessment (DPIA) or equivalent, including risk assessment and risk management plan.
    b. An assigned Data Protection Officer who has oversight and responsibility for execution of the DPIA, and the review and remediation processes.
    c. Evidence of communication with supervisory authorities about the DPIA, risk assessment, and risk management plan.

v. *Manufacturer Disclosure Statement for Medical Device Security (MDS2) – 2019 revision.* If vendor has provided a completed MDS2 statement for their medical device (not supporting hardware or software), and the MDS2 form submitted is using the 2019 revision of it or later, IU Health will accept this in lieu of an IT Risk Assessment. Older versions do not address current and emerging risks.

vi. *Information Technology Risk Assessment (ITRA).* If the Business Associate cannot provide evidence of HITRUST or ISO certification, sufficient evidence of compliance with GDPR or similar applicable regulations, or a valid MDS2 2019 form for their medical device, the Business Associate needs to Provide IU Health responses to the provided Vendor Risk Assessment and Security Questionnaire.

Any misrepresentation on any of these documents may result in contract termination.