UIDP Contract Accord 9: Confidential Disclosure Agreements

The Contract Accord provided below has been developed on behalf of the UIDP by a university / industry working group and was approved for publication in its current form by the UIDP board of directors.

The Accord is a UIDP work product that is not to be copied or used for commercial purposes. It is presented 'as is' and subject to change without notice.

The Accord aims to help parties who are new to university / industry collaboration to better understand the process, opportunities and potential pitfalls of putting a mutually beneficial research agreement in place.

UIDP Contract Accords do not present legal advice or claim accuracy or completeness. Any user should not rely solely on the information presented here and consult their attorney for legal matters.

Individuals interested in participating in the development of new accords can contact the UIDP office at uidp@nas.edu.

Contract Accord 9: Confidential Disclosure Agreements

Overview

Industry and Academia diverge sharply with respect to their perspectives on disclosing and sharing information with individuals and organizations. Industry wishes to generate market value and be profitable; therefore, it needs to maintain the secrecy of certain information. Universities (and the researchers and students that pursue scholarly activities) create and disseminate knowledge; therefore the ability to publish and share information is critically important to a University's academic research mission. The parties may hold differing views and interpretations of certain provisions of a confidential disclosure agreement (CDA). Thus the basic assumptions and practical implications regarding a confidentiality agreement should be discussed to ensure that all parties' expectations, both short term and long term, are addressed. CDAs should not restrict publication but may allow a party to delete its own confidential information.

Not all interactions between Industry and university may require a CDA. However the contractual mechanisms by which Industry and Academia share confidential information are commonly referred to as a Confidential Disclosure Agreement (CDA), a Non-Disclosure Agreement (NDA), or a Proprietary Information Agreement (PIA). For the purposes of this contract accord, only the term CDA will be used.

Industry Perspective

- Industry seeks to keep information confidential to protect essential proprietary information and thereby ensure a competitive advantage in the marketplace for as long as possible or as needed. In order to maintain a competitive advantage, Industry often seeks technologies or expert advice available at Universities. Pursuit of these relationships may require Industry to disclose its proprietary information.
- Industry faces a conundrum in that it must disclose its own confidential information in sufficient detail for University researchers to understand that information, while at the same time the confidential nature of the information must be preserved. Once the information is disclosed, Industry is at risk that its confidential information may be shared with others and its valued competitive advantage may be lost.
- Thus Industry needs to ensure that certain core information will remain confidential for a sufficient length of time – perhaps indefinitely – in order to preserve the value of the information in the market place. An agreement ensuring confidentiality of proprietary information may be the only means available to Industry to protect that information in situations when it must be disclosed.

University Perspective

- Universities have a culture of openness and shared knowledge, as their mission includes educating students and publishing research results for the public good. However, Universities may benefit from receiving confidential information from an Industry partner as well as by keeping their own discoveries in confidence for some period of time.
- Universities typically avoid CDAs in which shared information must be maintained as confidential in perpetuity because of efforts and costs associated with ongoing monitoring and compliance or a lack of mechanisms to do so, and because they have no ability to control students after graduation or employees who leave the University.
- Universities are experienced in maintaining the secrecy of certain types of information related to patients and students and are required to do so by law. They may also have the need to maintain confidentiality of other types of information, such as unpublished data or inventions not yet covered by a patent, as discussed above. A faculty member who is engaged in research may want to disclose his or her research results to Industry in hopes of having Industry sponsor all or a part of a research project or with the hope that Industry may license and commercialize a University-based invention.
- A CDA allows Universities to manage the receipt or disclosure of confidential information. Each CDA should be tailored to match the requirements of a specific situation.

Principles

CDAs enable the sharing of confidential information for the purpose of exploring potential interactions between two prospective partners while protecting the information from uncontrolled dissemination and possible subsequent disclosure. A CDA follows non-confidential interaction and typically precedes other agreements (e.g., sponsored research, membership, licensing). This means:

1. Confidential information should not be exchanged unless and until a CDA has been executed, and it should always be limited to the scope of the CDA. Information shared outside of the scope is not protected.
2. The CDA should define the scope and permitted uses of the information as well as duration and obligations of the parties. The scope of the CDA must be sufficiently narrow and clear to meet the purpose(s) of the exchange of confidential information. If necessary, the scope should be updated as necessary to reflect any potential change in the interaction between the partners.
3. Trade secret information, or other information that should be kept confidential in perpetuity, should never be disclosed.
4. Confidentiality in perpetuity would be inconsistent with the University's fundamental research exemption.

5. No work or research that could result in invention and the creation of intellectual property should be performed under a CDA. Such work or research should only be performed under a separate, formal agreement.
6. Discussions or brainstorming sessions that may lead to the creation of intellectual property (IP) should be avoided, but if such discussions are anticipated, then the CDA should include provisions for protecting such IP.
7. Any exchange of confidential information under consulting arrangements involving individual faculty members are not covered by CDAs that have the University as a party.
8. The agreement must be enforceable and meaningful. It is good practice to designate a Disclosure Coordinator for each party who is responsible to ensure proper procedure by and thus protection for the participants in a CDA.
9. Termination terms may not be appropriate in a CDA: neither party should be able to terminate any of the obligations, and the disclosure period can be terminated at any time by either party refusing to talk or listen. In the event that termination terms are applicable, the parties need to insure that the confidentiality obligations survive throughout the Protection Period.

Common Considerations in CDAs

1) Purpose of the CDA. In many jurisdictions the disclosure of information from one party to another without specifying and limiting the purposes for which the receiving party may use the information constitutes a license to use the information for whatever purpose the receiving party desires, even though the recipient must preserve the confidentiality of the information.

It is therefore generally recommended that the CDA specify the reason why the parties are exchanging information, the ways in which the receiving party may use the information, and clearly state that the receiving party may not use the information for any other purpose.

2) Scope of Disclosure. In many cases neither party intends to disclose all of its confidential information, nor does it wish to undertake obligations to ensure the confidential handling of more information than is necessary. Moreover, it is often impractical to compile an exhaustive list of the information to be shared that will be subject to the obligations of confidentiality.

Two useful techniques are (a) to specify the range of subject matter that the parties to the agreement anticipate being received and held in confidence and (b) to specify that information is only subject to the terms of the agreement if either (i) it is provided in writing suitably marked as confidential or (ii) if it is disclosed other than in writing, it is designated as confidential at the time of disclosure (some organizations do not require this), subsequently reduced to writing, marked as confidential, and delivered to the other party within a specified period of time, e.g., 30 days.

It is important to keep in mind that the Scope of Disclosure cannot limit what is disclosed, but only what is legally protected if disclosed. If a party chooses to share confidential information that is outside the Scope, then the receiving party legally has no obligation to protect that information and could use the information for any purpose. In the interest of preserving a positive collaborative relationship, the receiving party should therefore verify with the disclosing party whether the scope of the CDA should be changed to cover this information, or whether the information should be returned or destroyed.

3) Duration of the Confidentiality Agreement and Confidentiality Period. Generally, the duration of confidentiality is understood as the period of time information must be kept in confidence. However, two time periods are frequently involved in a confidentiality agreement.

One is the disclosure period, i.e., the period during which information subject to the obligation of confidentiality will be disclosed. The disclosure period begins on the effective date of the agreement and ends when the agreement expires.

The other is the protection period, i.e., the period of time information must be kept confidential. The protection period usually begins with actual disclosure of confidential information and ends as specified in the agreement (typically 3-7 years).

The protection period should reflect the actual useful life of the confidential information. Industry may desire longer protection periods, at least long enough to evaluate and file for IP protection. In contrast, Universities typically prefer shorter time periods, primarily because they often do not have mechanisms in place to ensure campus-wide compliance with such an agreement and because they prefer to have a cut-off date after which they are free to use and publish any information related to the project.

4) Individuals Covered by the CDA. Confidential information should be provided to individuals on a "need to know" basis. Universities usually see the CDA as being specific to a particular researcher or project, e.g., evaluating specific information in contemplation of a collaborative research project or technology licensing opportunity. But since the disclosing party will expect all individuals who receive its confidential information to be covered by the obligations of confidentiality, care should be given as to who actually receives this information.

This is particularly true if students or others are involved who are not employees of the University or parties to the agreement. CDAs should require all individuals receiving confidential information to acknowledge and agree to be bound by the confidentiality obligations defined in a CDA, even if they are not University employees or parties to the CDA.

It is best practice to name the individuals who are authorized or present to receive information in the agreement and have them sign an acknowledgment that they have read and understood the CDA. Individuals who are not employees of the University can agree to be bound by the agreement on their own behalf. An addendum may be required to update both the scope (i.e. the definition of the confidential information) and the list of individuals who receive confidential information as necessary as the discussions or the project may progress).

The parties should consider a single point of contact for the exchange of confidential information, i.e. a Disclosure Coordinator responsible for each party, and they should refrain from exchanging confidential information directly with unauthorized individuals. This practice

is very valuable in order to keep any disclosures clear in terms of maintaining adherence to the intended scope and ensuring proper follow-up documentation, storage etc. It is common to see behavior - from both Industry & University participants - that assumes that a CDA provides the protection when it really just provides the *framework* for the participants to ensure protection. In other words the important part is not getting a CDA signed but being disciplined in defining & reinforcing what is or is not confidential during any project-based interaction.

The parties may reserve the right to refuse acceptance of confidential information, for instance if they believe this could compromise their IP position or put them into an untenable situation with regards to export control.

5) Exceptions. Exceptions are typically made for the confidentiality obligations and for potential charge of liability in case of disclosure where the information was:

a) within the public domain prior to disclosure by the disclosing party to the receiving party or thereafter becomes part of the public domain other than as a result of breach of the CDA by the receiving party;

b) in the possession of the receiving party on or before the date of disclosure, as evidenced by competent written records;

c) acquired by the receiving party from a third party not under an obligation of confidentiality, as evidenced by competent written records;

d) independently developed by the receiving party without reference to the confidential information of the disclosing party, as evidenced by competent written records;

e) disclosed pursuant to operation of the law or a legal process.

6) Export Control. Export control laws apply to everyone, including Universities. Confidential information transferred under a CDA is not covered by the fundamental research exclusion as defined in 22 CFR 120.11(8). Loss of this exclusion could require the University to obtain export licenses to allow certain foreign students or employees to receive confidential information. Failure to comply exposes the employees of the parties to personal criminal liability. See Contract Accord #7 EC.

7) Copy Retention. CDAs often state that upon expiration of the term of the agreement, or at the disclosing party's written request, the receiving party will either return all confidential information to the disclosing party or destroy all copies of the confidential information in their possession. The receiving party is generally allowed to retain one archival copy in its records, but in order to prevent unauthorized use of the confidential information, these copies are generally kept in offices other than those of the individuals who initially received the information (for example, the archival copy may be kept in the office of the receiving party's legal counsel). [1]

8) Trade Secrets. A trade secret is information that provides a key economic advantage to its owner and for which reasonable measures of secrecy are maintained, typically in

[1] *The parties should bear in mind that universities frequently have obligations to maintain laboratory notebooks in order to verify the integrity of work performed and results published. For this reason it is good practice to avoid including confidential information obtained from another party in a laboratory notebook.*

perpetuity. The parties should avoid providing or accepting trade secret information under a CDA. Universities do not generally have mechanisms in place to implement extensive security provisions or keep information confidential indefinitely and have virtually no control over students after graduation or employees who leave the University.

9) Delegated Signature Authority. Industry employees generally understand that they are unable to sign documents that are legally binding upon their employers. University faculty members are not always cognizant that the documents they sign may purport to bind the University but that they personally lack the capacity to sign such agreements. Industry should consult with the University's relevant office, e.g., office of sponsored programs or technology transfer, to determine who has the authority to sign a CDA on behalf of the University.

10) "Open Record Laws" and State Universities. State-supported Universities may be subject to a state's "open record" or "public record" laws. These laws require a University to make information in its possession available under "freedom of information" requests filed by third parties. These requests can be used to compel a University to disclose information unless that information meets specific criteria set forth in the law. In such situations, it is good practice to indicate that the University has a duty to inform the company so that the company has an opportunity to request some form of protection from whatever body that is requesting the information.

Such laws override the obligations of confidentiality in CDA between the University and Industry even if the CDA does not specifically call out the applicability of the law (since contracts requiring parties to break a law are not enforceable,) so care must be taken in drafting CDAs to ensure that they comport with those laws. In these situations the University should provide specific reference to any such laws that are applicable so that Industry can properly evaluate the risk of disclosure of its confidential information.

11) Controlling Law and Jurisdiction. Generally both parties to a CDA will be most knowledgeable about the laws of their home state and therefore prefer that agreements be governed by those laws. State Universities may be prevented from entering into agreements that are subject to the laws of other states or of foreign countries. Similar prohibitions may apply to agreements specifying or allowing jurisdiction in courts outside of the University's home state. Many agreements do not specify the legal venue even if controlling law is specified.

It should be noted that jurisdiction and venue are most important to the parties in the event of a breach of a CDA but do not generally affect the terms or performance other than as noted above. The parties to a CDA may agree to remain silent as to controlling law or specify the laws of a neutral jurisdiction. Companies that do business nationally may be more willing to specify venue in a state other than their home state, while Universities are reluctant to be subject to the venue of a state in which they do not do business.

12) Arbitration or Mediation. In many cases arbitration or mediation may be more desirable than trying to assert a party's rights through litigation in a dispute. Some universities are prohibited from participating in binding arbitration either because of policies, legislation or principles of state sovereignty. Also, some companies are averse to engaging in binding arbitration. In such cases it may be advisable to require representatives of each party to

participate in non-binding mediation prior to initiating litigation. Many states court rules require mediation in cases meeting a certain monetary threshold.

13) Limitation of Liability. The disclosing party has valid concerns about the possible consequences of the recipient party violating its obligations under a CDA. To address these concerns, language in a CDA may seek to place financial obligations on the party violating the terms of that agreement. In some circumstances, particularly when dealing with a state University, the liability of one party may be controlled by statute[2] limiting the liability of any state agency, including its Universities. Any such limitation of liability should be clearly stated in the CDA.

14) Injunctive Relief. Industry may wish to include language in a CDA to ensure adequate remedy for breach or threatened breach of the confidentiality obligations including the right to injunctive relief or specific performance, as is customary in the commercial environment. Such language may include wording to the effect that all parties agree that monetary damages would not be sufficient to remedy a breach.

Universities may find such wording unacceptable, as it may constitute a violation of principles of state sovereignty or be construed as an open door to additional litigation or contractual admission of fault. If this is the case, any such limitation by a state University should be brought to the attention of the prospective industry partner.

Industry should be aware that the inclusion of language specifying that the parties may *seek* injunctive relief - rather than language stating that the parties are *entitled* to injunctive relief - may be misleading because the actual ability of Industry to successfully obtain injunctive relief when dealing with a State University may not really exist.

Additional Considerations

1. Inclusion of confidential information and potential embargo of Student Publications, particularly works that are required for obtaining a degree, are a particular concern as Universities have an obligation to ensure that they do not enter into agreements that prevent or impede students from graduating. Such work should never require the use of another party's confidential information unless it is clear to everyone that the student will be able to complete publication of the work without violating a CDA.
2. Many Universities allow their researchers to enter into **Consulting Agreements** with industry. In these situations the researchers are allowed to work as private contractors rather than as employees of the University. The researchers have an obligation to ensure that they abide by the terms of any CDA into which they enter as private contractors and to realize that disclosure in the course of their academic work of the information gained under such agreements may be a violation of those agreements.
3. **Control over Authorship on Scholarly Articles lies** solely with the principal investigators rather than with the University. The content of a publication, at least to the extent that it contains any confidential information, may, however, be subject to

[2] *Example: "Tort Claims Act"*

the terms of the CDA between the University and the Company. The University would be expected to compel its employees to abide by the terms of the CDA.

4. In some cases it may be possible to provide a receiving party with protected or **Trade-Secret information embedded in a Product or Service** with a prohibition on reverse engineering of materials. The advantage of this arrangement is that it allows the receiving party to publish its research results in compliance with the terms of the CDA.
5. The parties should avoid language concerning **Residual Information** - i.e. information that is kept in non-written form in a person's unaided memory - or at least carefully consider the use of a Residual term in a specific circumstance because of the inability to protect ambiguous or undefined information and control its later use. This pertains in particular to company confidential or trade secret information that another individual may learn as a result of a collaboration or a visit to the other party's facilities. Residuals terms are typically contentious. If one side values and insists on them, the best advice for the other party is to very carefully consider the motivation for and the potentially very significant consequences of including such terms.
6. For both Industry and Universities, the disclosing party may want to avoid **"Contamination" through Inadvertent Exposure** to confidential information that it does not own or have rights to use. For example, a party disclosing a confidential new product may not wish to be informed about the receiving party's ideas for improving that product for fear of "contaminating" the disclosing party's own planned improvements for that product. Thus the parties should consider whether the situation warrants explicitly specifying certain types of information that, if possible, should not be disclosed in order to avoid such contamination, and whether a one-way or a two-way agreement may be more adequate for the situation.

Summary

The goal of a CDA is to protect the information from uncontrolled dissemination. Confidential information provides its holder with a competitive advantage, be it academic or economic, that may be lost if the information is disclosed.

Procedures of working with Industry and obligations on the part of academic researchers to keep information confidential are often unclear or non-existent in an academic environment. Industry may request specific safeguards which might be unusual in agreements between business entities. Such safeguards may include spelling out specific measures that need to be observed, for instance how confidential information is received and controlled and secured by the University and how the initial disclosure as well as any subsequent sharing of the information with others should be tracked to properly protect it.

The reputations of University researchers depend upon them being the first to publish significant findings from their work; therefore, it is important for University researchers to ensure that confidentiality agreements with Industry will not compromise their ability to be the first to publish, whether via a patent application or a peer-reviewed journal.

An incremental exchange of information is often a better way to proceed by allowing the parties to become familiar with each other's norms and potential incompatibilities while minimizing risks associated with sharing proprietary information. This approach may be prudent if the parties are not certain that they share similar perspectives on the identification, sharing and handling of sensitive information.